UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE DIREITO

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

KELVIANE DE ASSUNÇÃO FERREIRA BARROS

SOB VIGILÂNCIA: O EQUILÍBRIO ENTRE SEGURANÇA E PRIVACIDADE NA GESTÃO DE DADOS PELO ESTADO BRASILEIRO

FORTALEZA-CE

2023

KELVIANE DE ASSUNÇÃO FERREIRA BARROS

SOB VIGILÂNCIA: O EQUILÍBRIO ENTRE SEGURANÇA E PRIVACIDADE NA GESTÃO DE DADOS PELO ESTADO BRASILEIRO

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal do Ceará como requisito parcial à obtenção do título de Mestre em Direito. Área de Concentração: Constituição, sociedade e pensamento jurídico.

Orientador: Prof. Dr. Hugo de Brito Machado Segundo.

FORTALEZA-CE

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

B278s Barros, Kelviane.
Sob Vigilância: : O equilíbrio entre segurança e privacidade na gestão de dados pelo Estado brasileiro / Kelviane Barros. – 2024.
124 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Faculdade de Direito, Programa de Pós-Graduação em Direito, Fortaleza, 2024.
Orientação: Prof. Dr. Hugo de Brito Machado Segundo.

1. Proteção de Dados. 2. Privacidade. 3. Administração Pública. 4. Segurança Pública. 5. Segurança Pública, Direitos Fundamentais. I. Título.

CDD 340

SOB VIGILÂNCIA: O EQUILÍBRIO ENTRE SEGURANÇA E PRIVACIDADE NA GESTÃO DE DADOS PELO ESTADO BRASILEIRO

Esta Dissertação foi julgada _____para obtenção do Título de Mestre, e _____ em sua forma final pelo Programa de Mestrado em Direito da Universidade Federal do Ceará.

Fortaleza/CE, 24 de novembro de 2023.

BANCA EXAMINADORA

_____
Prof.ª Raquel Cavalcanti Ramos Machado, Dr.ª
Universidade Federal do Ceará

_____
Prof. George Marmelstein Lima, Dr.
Universidade Federal do Ceará

_____
Prof.ª Fernanda de Carvalho Laje, Dr.ª.
Universidade de Brasília

RESUMO

Este estudo explora a coleta, armazenamento, tratamento e uso de dados pessoais pelo Poder Público no Brasil no âmbito da segurança pública, enfatizando as implicações dessas práticas no cenário dos direitos fundamentais. Através de uma análise histórica e do estudo de casos contemporâneos, esta dissertação investiga a evolução da gestão de dados pessoais pela administração pública, destacando a necessidade de uma abordagem cuidadosa na manipulação desses dados. Examinando o regime jurídico atual sob a Lei Geral de Proteção de Dados, o trabalho avalia criticamente a eficácia das normas existentes e sua aplicação nas esferas administrativas e judiciais.

São discutidos, ainda, casos práticos que ilustram a aplicação das normas de proteção de dados no Brasil, proporcionando uma visão crítica da legislação e de sua execução. A partir destes estudos, a dissertação propõe melhorias na administração de informações pessoais, sugerindo métodos técnicos e procedimentos para uma proteção de dados mais eficaz e respeitosa dos direitos fundamentais.

Ao final, o estudo visa estabelecer recomendações para o aprimoramento da regulamentação do uso de dados pessoais pelo Poder Público no âmbito da segurança pública, assegurando a preservação dos direitos fundamentais dos cidadãos no território nacional.

Palavras-chave: Proteção de Dados, Privacidade, Administração Pública, Segurança Pública, Direitos Fundamentais, Lei Geral de Proteção de Dados.

ABSTRACT

This study explores personal data collection, storage, processing and use by Public Authorities in Brazil in the context of public security, emphasizing the implications of these practices in the scenario of fundamental rights. Through a historical analysis and contemporary cases study, this dissertation investigates the evolution of personal data management by public administration, highlighting the need for a careful approach when handling this data. Examining the current legal regime under the General Data Protection Law, the work critically evaluates the effectiveness of existing regulations and their application in the administrative and judicial spheres.

Practical cases that illustrate the application of data protection standards in Brazil are also discussed, providing a critical view of the legislation and its execution. Based on these studies, the dissertation proposes improvements in the management of personal information, suggesting technical methods and procedures for more effective data protection that respects fundamental rights.

In the end, the study aims to establish recommendations for improving the regulation of the use of personal data by the Public Authorities within public security scope, ensuring the preservation of the fundamental rights of citizens in the national territory.

Keywords: Data Protection, Privacy, Public Administration, Public Security, Fundamental Rights, General Data Protection Law.

Todo produto humano que entendemos e desfrutamos instantaneamente se torna nosso, onde quer que ele se tenha originado. Orgulho-me de minha condição humana quando posso reconhecer os poetas e artistas de outros países como meus semelhantes. Permitam-me sentir com alegria genuína que todas as grandes glórias do homem são minhas.

Amartya Sen, Desenvolvimento como Liberdade.

AGRADECIMENTOS

Estar na Academia é um prazer e uma grande responsabilidade. A produção científica é, antes de tudo, um escudo social contra o vazio, o falso, o demagógico.

Este trabalho encerra um ciclo iniciado e largamente vivido em tempos de pandemia e que somente foi possível ser experienciado graças à força humana que nos permitiu enfrentar tudo com um pouco mais de esperança.

O esforço aqui empenhado e todos os futuros serão sempre uma homenagem ao conhecimento, aos seus instrumentalizadores e àquilo de bom que ele possa trazer para o mundo e para as pessoas.

Represento tudo isso agradecendo a meus mestres, que me encorajaram no caminho bonito da descoberta.

SUMÁRIO

1 INTRODUÇÃO

Informações pessoais sempre foram ativo importante para atividades exercidas nas esferas privada e pública, vez que permitem o direcionamento de ações que alcancem resultados mais eficientes e satisfatórios. A coleta daquelas, porém, passou a intervir em searas cada vez mais íntimas do indivíduo, provocando como reação uma busca de tutela da privacidade, em especial diante de investidas ilegais ou maliciosas no recôndito mais particular de seus titulares.

A captação desses recursos pessoais foi significativamente incrementada com o progresso tecnológico, que permitiu uma coleta e tratamento de dados em volume, velocidade e variedade antes não imaginadas. Esse potencial não passou despercebido pelo Poder Público, que, sob o discurso da busca do interesse da coletividade, utilizou sua ascendência sobre os cidadãos para coletar destes informações cada vez mais detalhadas e sensíveis. É certo, nesse contexto, que o conhecimento detalhado de informações, hábitos, relações dos cidadãos os põe em posição de extrema vulnerabilidade, sujeitando-os a uma vigilância que pode comprometer, em definitivo, o comportamento social.

Visando a trazer parametrização mínima para o procedimento de coleta, tratamento e uso de dados pessoais, foi aprovada a Lei Geral de Proteção de Dados Pessoais (LGPD), a qual, apesar de trazer importantes princípios e diretrizes para a ação estatal, apresenta uma significativa limitação: não se aplica quando o Estado atua na segurança pública, defesa nacional, segurança do Estado ou em atividades de investigação e repressão de infrações penais.

Apesar de não haver regulamentação precisa para essas hipóteses, o Estado amplamente utiliza tratamento de dados pessoais para prevenção e repressão de delitos, como uso de inteligência artificial para manuseio de sistemas de reconhecimento facial e monitoramento de placas de veículos, em sistema de cruzamento de dados entre diversos órgãos que compõem as forças policiais e de inteligência do Estado.

Essa postura parece causar sérios prejuízos a indivíduos e a grupos identitários, seja em razão de limitação técnica no desenho dos sistemas utilizados, seja mesmo em função da vigilância sem controle a que os cidadãos vêm sendo submetidos. Esta é a hipótese a ser pesquisada.

O tema é palpitante dado que, após testes iniciais ocorridos no final da última década no Brasil, o uso de dados pessoais vem sendo amplamente difundido, com incentivos governamentais para implantação de soluções de tecnologia na seara da segurança pública em todo o país. Por outro lado, observa-se literatura estrangeira e nacional a respeito da indevida

restrição de direitos em razão de falhas nas ferramentas tecnológicas utilizadas, de forma que se deve perquirir as causas mais ou menos aparentes que contribuem para essa problemática. Nesse campo, destaca-se que alguns grupos sociais restam ainda mais expostos às falhas tecnológicas.

De outra senda, ainda que as limitações técnicas sejam superadas, insta perquirir-se acerca da razoabilidade de uso contínuo de sistemas de monitoramento e vigilância em massa para satisfação da busca de defesa e paz sociais.

Tendo em vista, porém, a importância dos modernos recursos tecnológicos para atuação eficiente do Estado, procura-se, a par de problematizar as suscetibilidades a direitos, pensar-se em modelos de regulamentação que mitiguem os riscos enumerados após a exposição dos principais problemas observados. Esse é o escopo do último capítulo.

A metodologia usada no trabalho é hipotético dedutiva, buscando-se como fontes para a análise documentos e bibliografia nacional e estrangeira a respeito do tema.

No Capítulo I será realizada uma contextualização do uso de informações pessoais dos indivíduos pela administração pública, mostrando-se, por meio de referências históricas, a necessidade de atenção à forma como os dados são manipulados no exercício da ação estatal. Será feita, ainda, uma abordagem histórica por meio de pesquisa de legislação e jurisprudência para análise da evolução da ideia de privacidade até se chegar ao conceito de proteção de dados pessoais, hoje disseminado.

No capítulo II, será apresentado o regime jurídico do tratamento de dados pessoais pelo Poder Público no Brasil. Serão apontados os princípios regentes da matéria, os quais são confrontados com outros também aplicáveis à esfera pública fora da LGPD. Também serão indicadas as bases legais em que o Poder Público está autorizado a realizar tratamento de dados pessoais, finalizando-se o capítulo com indicação dos limites aplicáveis ao uso secundário e compartilhamento de dados com outros órgãos públicos ou privados.

A seguir, serão analisados casos concretos de uso dos sistemas de inteligência artificial na seara da segurança pública, visando à prevenção e à repressão de delitos. Aqui, serão analisadas as principais falhas e os grupos que a esta são mais expostos. Por fim, diante da análise dos casos concretos, subsumidos com a normatização aplicada à matéria – ou sua insuficiência – serão feitas propostas de regulamentação a fim de que o uso de sistemas tecnológicos ocorra com o menor custo possível aos direitos fundamentais.

2 USO PÚBLICO DE DADOS

As informações pessoais sempre foram ativo importante para o Poder Público, que as coleta e utiliza com o fito de melhor promover políticas voltadas ao atendimento de direitos fundamentais. Contudo, ao longo da história, diversos exemplos demonstram os riscos associados a essa coleta e uso, demandando atenção para as possíveis consequência do acesso a um elevado manancial de dados dos administrados.

Diante desses desafios, foi revisto o próprio conceito de privacidade, que se transformou, evoluiu e desmembrou em outros que visam a melhor atender aos interesses público e privado.

2.1 Contextualizando a proteção de dados no setor público

A questão referente à proteção de dados tradicionalmente foi atrelada à ideia de privacidade. Tipicamente a privacidade é vista como um espaço dentro do qual o indivíduo pode desenvolver-se livremente, sem interferência do meio social mais amplo. A identificação do que se entende como expressão da privacidade e a sua importância para os indivíduos variou, porém, conforme o tempo.

Abercrombie, Hill e Turner[1] mencionam que, em civilizações antigas, não se via o privado como um espaço social enobrecedor, mas como um enfraquecimento das relações sociais genuínas e racionais. Assim, destacam que, em sociedades pré-modernas, a vida privada era sistematicamente escrutinada para livrar a comunidade do mal pessoal. A defesa das crenças, tradições e práticas coletivas servia como meio de proteção contra inimigos externos. Nesse contexto, a religião, a moral social e as instituições desempenharam papel relevante de vigilância e controle sobre a vida pública e o ambiente doméstico dos indivíduos.

Somente na sociedade industrial ocidental contemporânea, com o avanço da divisão social do trabalho, a condição individual foi valorizada, percebendo-se o indivíduo como parte de um todo, mas também um organismo relevante por si mesmo. Nesse contexto, a privacidade foi elevada a uma condição necessária para o bom desenvolvimento pessoal.

---

[1] ABERCROMBIE, N.; HILL, S.; TURNER, B.S. **Sovereign individuals of capitalism**. London: Allen & Unwin, 1986.

Émile Durkheim[2] ressalta o caráter moral atribuído ao dever com o coletivo e a ausência da pessoalidade existente em especial em sociedades menos avançadas, com o fim de garantir a persistência de uma "consciência comum" e da solidariedade social. Esse comunitarismo gerou a ideia de uma coesão coletiva, a qual se viu abalada a partir da divisão social do trabalho, fenômeno que se generalizou e apresentou repercussões em diversos níveis da vida comunitária, não apenas no interior das fábricas ou no campo econômico. Sua influência atingiu setores sociais diversos, como as funções políticas, administrativas, científicas, artísticas e mesmo as relações pessoais.

Observa-se, portanto, que, ao longo do tempo, a valorização da individualidade e da privacidade variou consideravelmente, havendo, porém, em qualquer tempo, flexibilização de acesso a esta esfera pessoal. O ponto diferencial entre os contextos passado e atual de intervenção na vida privada consiste na forma de exercício dessa vigilância, pessoal e íntima no passado e ampla e anônima em tempos atuais, com enorme coleta de informações (dados) sobre os cidadãos. Em tempos hodiernos, ressalta-se, ainda, a intervenção do Estado via tecnologias de vigilância e comunicação.

No que tange ao Poder Público, é preciso que se perceba que, embora em razão da revolução tecnológica ocorrida a partir da segunda metade do século XX tenha-se observado o aumento da coleta e utilização de dados pessoais, produzidos agora em larga escala, a ideia de seu uso como ativo para a gestão pública é antiga. Esta prática tornou-se mais assente com o desenvolvimento da ideia de Estado Social, no qual o ente estatal adquire o caráter de patrocinador de setores econômicos e sociais[3].

Essa nova concepção do papel do Estado atribui-lhe a responsabilidade de atuar ativamente na realização de serviços públicos e de promoção de bem-estar da população. Para atingimento dessa finalidade, é necessário que o Estado conheça bem seus cidadãos, buscando informações a fim de traçar um quadro pessoal e social que permita ação direcionada e estratégica. Assim, a investigação do indivíduo advém em parte como resultado da ação estatal advinda de uma luta por direitos sociais e igualdade de tratamento entre cidadãos, o que leva ao crescimento de material censitário e de pesquisas sociais[4].

Ainda nesse contexto, deve ser ressaltado que as políticas públicas amparadas em evidências garantem não somente o cumprimento das funções estatais, mas o controle político

---

[2] DURKHEIM, Émile. Da Divisão do Trabalho Social. Tradução Eduardo Brandão. – 2. ed. – São Paulo: Martins Fontes, 1999.
[3] BONAVIDES, Paulo. **Teoria Geral do Estado.** 11. ed., rev. e aum. – São Paulo: Malheiros, 2018.
[4] ABERCOMBRIE, N.; HILL, S.; TURNER, B.S. **Sovereign individuals of capitalism**. London: Allen & Unwin, 1986.

dos Poderes pelos cidadãos, dado que a análise racional dos dados permite avaliação da correção e adequação das ações desenvolvidas e o escrutínio público sobre o direcionamento da atividade pública.

A intervenção estatal para busca de informações dos cidadãos pode decorrer, portanto, de uma luta por realização de direitos sociais, de direcionamento para adoção de políticas públicas mais efetivas e melhor gerenciamento de ações e recursos públicos. Esse fato vem associado, porém, ao risco da construção de um sistema de dominação por meio de vigilância próxima e generalizada da população. Este se torna, então, um processo contraditório, em que, na medida em que é necessária a identificação dos indivíduos a fim de reconhecer-lhes cidadania e acesso a direitos, estes são postos em posição de vulnerabilidade frente ao controle de informações e à vigilância que é exercida pelo Estado sobre sua vida particular e privada.

Exemplos históricos podem demonstrar o quadro desafiador para equilíbrio entre vantagens e prejuízos do uso de dados pessoais e para pretensões regulatórias do tema.

Durante os regimes nazista e fascista, a utilização de bases de dados produzidas pelo Estado permitiram a identificação de grupos sociais perseguidos e uma ação concentrada contra estes antes e durante a Segunda Guerra Mundial[5]. Registra-se que, nos países invadidos por tropas nazistas que tinham armazenados dados pessoais minuciosos sobre os cidadãos, em especial dados sensíveis[6], houve uma mais clara identificação dos grupos perseguidos, que foram dizimados em maior parcela do que em outros em que não existia tal detalhamento. Neste caso, o plexo de informações foi utilizado de modo abusivo e criminoso, demonstrando o risco da concentração de grande volume de informações dos cidadãos pelo aparato estatal.

Por outro lado, em tempos mais recentes, reportam-se os problemas advindos da menor vigilância exercida sobre a população. No contexto do ataque ocorrido em solo americano em 11 de setembro de 2001, Shoshana Zuboff[7] destaca que existia uma tendência neoliberal da máquina governamental americana que impediu vigilância e regulações profundas em setores sensíveis como as redes de comunicação, em especial canais da internet, o que teria dificultado a antecipação e a prevenção da ação terrorista naquele ano. Segundo essa visão

---

[5] WORLD JEWISH CONGRESS e UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION (UNESCO). Como os alemães sabiam quem era judeu? Disponível em: https://abouttholocaust.org/pt/facts/como-os-alemaes-sabiam-quem-era-judeu . Acesso: 27 de outubro de 2022.

[6] A Lei Geral de Proteção de Dados considera como sensível o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

[7] ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução George Schleinger. – 1. ed. – Rio de Janeiro: Intrínseca, 2020.

neoliberal, toda regulamentação estatal seria opressiva e favoreceria autoritarismo, discurso que sobressaía mesmo ao lado de análises de custo e eficiência.

O cenário americano foi, porém, modificado após o atentado de 2001, quando o foco passou de privacidade para segurança. O Congresso americano aprovou o *Patriot Act*, criou o *Terrorist Screening Program* e instituiu uma série de outras medidas que aumentaram drasticamente a coleta de informação pessoal sem necessidade de mandado. Ademais, agências foram autorizadas a compartilhar informações e a cruzar bases de dados para análises mais abrangentes de perfis pessoais.

Dos exemplos expostos, observa-se que a coleta, armazenamento, tratamento e uso de dados pessoais dos cidadãos pelo Poder Público é questão sensível, que pode igualmente levar à proteção e realização de direitos individuais e coletivos, e à opressão e perseguições a partir da identificação de indivíduos e grupos.

Esta não é uma questão exclusiva de governos, porém. A ampla disponibilidade e maior flexibilidade da tecnologia causa uma mudança profunda na atitude em relação às informações e seu uso também em setores comerciais, industriais e acadêmicos. Em tempos recentes, acompanhou-se sua influência sobre o campo político e democrático, com a coleta e tratamento de dados pessoais de milhões de cidadãos com o objetivo de direcionar seu comportamento em decisões políticas relevantes[8]. O realce feito em relação aos governos que se faz neste trabalho decorre do desequilíbrio de posições que se observa entre cidadão administrado e Poder Público, dado o condicionamento da entrega de informações para usufruto de direitos legalmente reconhecidos e a possibilidade de aplicação de sanções em caso de recusa do titular dos dados[9].

Reconhece-se a importância que os dados, que geram estatísticas, representam para a política governamental, permitindo que se identifique uma base de ação para que a política estatal possa alcançar os fins visados. Ademais, questões relacionadas à segurança pública podem justificar uma intervenção estatal na esfera eminentemente privada, resguardando-se a coletividade de maiores perigos. A questão a ser levantada é em que medida esse poder estatal deve ser exercido e quais os riscos que o tratamento de dados pessoais nessa esfera gera para os indivíduos e para sociedade como um todo. Visando a dar respostas a estas questões, construções de caráter doutrinário, legislativo e jurisprudencial foram realizadas.

---

[8] Caso Cambridge Analytica, empresa de consultoria política que usou dados pessoais de milhões de usuários da rede social Facebook para influir na campanha presidencial americana de 2016 e no movimento do Brexit.
[9] A Lei 5.534/68, que dispõe sobre a obrigatoriedade de prestação de informações estatísticas, indica como infração a não prestação de informações e a prestação de informações falsas, ambas sujeitas a multa que pode chegar a até 20 (vinte) salários-mínimos.

A disciplina de proteção de dados pessoais foi fomentada em razão desses avanços sobre a privacidade promovidos dentro da administração pública em especial no pós-guerra e com o impulsionamento da informática a partir da década de 1960. Esse contexto de avanço tecnológico e busca de controle de dados, destaca Danilo Donedo[10], inspirou projetos como o *National Data Center* e o SAFARI, bem como o Censo alemão. A reflexão doutrinária surge como reação a estes projetos, sendo seguida das primeiras normas para tratamento da matéria.

O *National Data Center* surge em 1965 como recomendação de cientistas sociais para que o governo federal americano desenvolvesse uma central que armazenasse e disponibilizasse aos pesquisadores e realizadores de políticas públicas dados coletados por diversas agências estatísticas. Essa central armazenaria as informações pessoais de todos os norte-americanos coletadas pelos órgãos da administração federal, começando com a unificação dos dados do censo americano, do fisco, de registros trabalhistas e de previdência social. A ideia subjacente ao projeto era garantir a maior eficiência na administração pública americana.

A criação dessa central ocasionou um grande debate nacional, que levou a protestos públicos e a intenso escrutínio pelo Congresso sobre os dados mantidos pelos órgãos federais, o potencial uso indevido destes e as ameaças à privacidade representadas pelas novas tecnologias. Como resultado, o projeto foi encerrado e o debate ali iniciado culminou na aprovação do *Privacy Act* de 1974. A Lei disciplinou práticas para coleta, manutenção, uso e disseminação de informações pessoais mantidas por agências federais; proibiu a divulgação de registros sem o consentimento do indivíduo – ressalvadas algumas exceções legais; disciplinou meios para obtenção de acesso e modificação de registros e estabeleceu requisitos para manutenção de informações pelas agências.

Danilo Donedo destaca que esse caso foi fundamental para que se atentasse, ainda, à importância de ser dada atenção à arquitetura da estrutura informacional, já que se verificou, a partir do caso, que o banco de dados descentralizado é a melhor opção para a proteção de dados do titular, com o intuito de se preservar as informações coletadas.

Em movimento semelhante ao observado nos Estados Unidos, na França, o *Institut National de la Statisti*, sob o mesmo pretexto, propôs o denominado SAFARI - *Système Automatisé pour les Fichiers Administratifs et Répertoires des Individus*, em 1970. O SAFARI era um sistema automatizado de arquivos administrativos e de listas de pessoas físicas que visava à interligação de arquivos pessoais da administração francesa, em especial a partir do número de seguridade social.

---

[10] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 3.ed. São Paulo: Revista dos Tribunais, 2021.

O projeto francês igualmente sofreu forte oposição daqueles preocupados com a preservação das liberdades individuais dos cidadãos, gerando reações na doutrina especializada e na imprensa. O projeto acabou encerrado e levou o governo a criar a *Comission Nationale de L'informatique et des Libertés*, que está na origem da lei de proteção de dados de 1978 (Lei n°78-17 – *Loi informatique et libertés*).

As primeiras normas relativas a proteção de dados pessoais surgiram, assim, na década de 1970, tendo como preocupação central a proteção de direitos e liberdades. Além dos países e das normas acima mencionados, releva-se nesse contexto que também a Alemanha, por circunstâncias históricas e culturais próprias, desenvolveu um grande arcabouço normativo referente a proteção de dados pessoais, que é reconhecido como pioneiro e dos mais robustos em nível mundial. Regimes autoritários tendem a ser os mais interessados e eficazes em atividades de vigilância da população, criando órgãos especializados na tarefa de coletar dados e promover o controle político em seu território. Exemplos como a *Geheime Staatspolizei* (Gestapo – Polícia Secreta do Estado), durante o período do Nazismo, e a *Staatssicherheitsdienst* (Stasi – Serviço de Segurança do Estado) na Alemanha oriental, durante o Governo da *Deutsche Demokratische Republik* (DDR – República Democrática Alemã), marcaram a história do país e justificam seu pioneirismo no tratamento da matéria.

A Lei de Proteção de Dados do estado federal de Hesse, que entrou em vigor em 1970 (*Datenschutzgesetzgebung)*, é considerada a primeira lei formal de proteção de dados do mundo. Ainda nessa primeira geração de normas relativas a proteção de dados, pode ser mencionada a lei sueca de 1973.

Também em solo alemão importante marco jurisprudencial foi fixado em decisão do Tribunal Constitucional Federal (*BVERFGE* 65, 1)[11], que analisou a Lei do Censo (*Volkszählungsgesetz*) de 1983. Referida decisão menciona princípios englobados em normas brasileiras sobre proteção de dados e foi mais de uma vez mencionada em julgamentos importantes acerca do tema pelo Supremo Tribunal Federal.

Por conta dessa Lei do Censo, foi ordenado o recenseamento geral da população, com determinação de coleta de dados sobre profissão, moradia e local de trabalho para fins estatísticos. Em um de seus dispositivos, a lei também previu a possibilidade de comparação

[11] BVerfGE 65, 1, "Recenseamento" (*Volkszählung*). In: MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do tribunal constitucional federal alemão**. Montevidéu: Fundação Konrad Adenauer, 2005. Disponível em: https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf . Acesso: 27 de outubro de 2022.

das informações coletadas com aquelas presentes em outras bases de dados e a transmissão de dados anonimizados[12] a repartições públicas outras para fins de execução administrativa.

A Lei do Censo alemã deu causa a diversas Reclamações Constitucionais, nas quais se alegava violação a direitos fundamentais, em especial ao direito ao livre desenvolvimento da personalidade. O Tribunal, analisando as Reclamações, declarou a nulidade de alguns dispositivos, entre os quais os que permitiam comparações com dados coletados em outras bases e possibilidade de seu compartilhamento e transmissão para fins de execução administrativa.

Foram pontos de destaque da decisão do Tribunal Constitucional Federal (TCF): 1) o direito geral da personalidade garante o poder de o indivíduo decidir, em princípio, sobre a exibição e o uso de seus dados pessoais, caracterizando o que chamou "autodeterminação sobre a informação"; 2) esse direito não é absoluto, devendo ser ponderado diante do interesse predominante da coletividade e aplicado o princípio da proporcionalidade; 3) deve ser dado tratamento diferenciado ao tema, conforme se cuide de dados não-anônimos ou anonimizados, estes para fins de estatística; 4) em dados anônimos não se pode exigir vinculação estreita e concreta dos dados à finalidade, uma vez que estes devem ser utilizados em diversas tarefas, não determináveis de antemão, assim como pode ocorrer transmissão e uso por agências diversas; 5) não existem dados irrelevantes, em especial quando ainda são individualizáveis.

O fundamento central utilizado pelo TCF nessa decisão paradigmática foi a proteção do livre desenvolvimento da personalidade (art. 2º, parágrafo 1º, da LF) e da dignidade da pessoa humana (art. 1º, parágrafo 1º, da LF), destacando-se que o direito da personalidade não possui direção única, abrangendo nuances diversas, entre as quais a possibilidade de autodeterminação e, neste caso em particular, de autodeterminação informativa. Esses direitos somente poderiam ceder a um interesse geral preponderante, o qual deveria ser identificado por meio de uma base legal que cumprisse a exigência de clareza das normas e de proporcionalidade. Veja-se que o fundamento foi constitucional, não havendo aprofundamento de referência à Lei Federal de Proteção de Dados (*Bundesdatenschutzgesetz*, *BDSG*) alemã, que entrou em vigor em 1979 e vige até hoje ao lado de leis próprias editadas pelos estados federais para regular primariamente o processamento e uso de dados pelas autoridades públicas estaduais.

O período mencionado nos três exemplos acima cuida de um tempo em que o estado da tecnologia não permitia ainda coleta massiva de dados e tratamento tão detalhado como o possível diante dos recursos atuais, havendo limitação da quantidade de informações registradas

[12] A Lei Geral de Proteção de Dados define como anonimizado o dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

sobre um indivíduo. Ademais, tradicionalmente não existia interesse em grande quantidade de informações; estas normalmente eram superficiais e armazenadas de forma descentralizada; seu acesso era difícil e havia grande dificuldade de interpretar e inferir informações a partir dos dados coletados.

No novo cenário tecnológico, porém, dados são gerados em diversas atividades humanas e são coletados por organizações públicas e privadas em volume, variedade e velocidade jamais vistos, o que gera preocupações associadas à segurança dos dados e à privacidade dos cidadãos. Receia-se que essa grande capacidade de coleta, armazenamento e tratamento possa gerar um sistema de vigilância em que as características pessoais, as atividades, os hábitos e as relações dos indivíduos fiquem sujeitas à observação, manipulação e uso indevido para fins ilegais ou intrusivos.

Esse novo contexto, como visto, não passa despercebido ao Poder Público. À medida que os processos de registro de informações se tornam mais eficientes e mais baratos, avança o interesse de governos em conhecer os cidadãos e coletar dados sobre estes, não raras vezes condicionando o uso de certas benesses estatais à entrega de informações pelo administrado, estas cada vez mais completas e sensíveis.

É nesse ambiente que se insere a presente geração de normas de proteção de dados pessoais, dentre as quais se destaca, para os fins do presente trabalho, a Lei Geral de Proteção de Dados Pessoais brasileira (LGPD). A normatização da matéria levou em conta a evolução do conceito de privacidade e seu desdobramento em direção à proteção de dados, ocorrida de forma gradativa, como explicitado nas linhas que seguem.

2.2 A transformação do conceito de privacidade e a proteção de dados pessoais em tempos de *big data:* da privacidade à autodeterminação informativa

O conceito de privacidade varia bastante conforme se analisem diferentes marcos temporais, geográficos e sociais, apresentando forte dinamicidade. As notas de abrangência dependem fundamentalmente da forma como as instâncias legislativas e judiciárias reconhecem seu espaço como um conceito mais ou menos elastecido em dado contexto.

Diante da dificuldade de delineamento de um conceito preciso, Daniel J. Solove[13], propõe uma nova teoria da privacidade. Destaca o catedrático que a maioria dos teóricos tenta defini-la buscando um denominador comum em todos os casos em que pode ser arguida e que

[13] SOLOVE, Daniel. **Understanding Privacy**. Harvard University Press, 2008, p. 8.

essa tentativa de identificar características essenciais ou centrais da privacidade não pode obter sucesso. Em substituição a esse modelo, desenvolve uma abordagem em que sugere a busca de uma "semelhança familiar", de forma que, de elementos diferentes, extraiam-se características relacionadas. Ademais, propõe um conceito que se desenvolva de baixo para cima, isto é, partindo de contextos particulares e não em abstrato, além de realçar as diferentes atitudes em relação à privacidade nas várias culturas. Na abordagem sugerida pelo autor, portanto, a privacidade deve ser analisada de forma plural, sem um identificador unitário, criando um ambiente flexível o suficiente para acomodar as naturais mudanças, de forma que se torne firme o suficiente para permanecer estável e útil. Adotada ou não a posição sugerida, observa-se uma transformação do conceito de privacidade, que pode ser apresentada nos termos a seguir.

Fundamentalmente, tem-se uma evolução que parte de uma visão individualista de privacidade, como "um direito de ser deixado só", para uma concepção em que se agregam elementos de controle sobre o manuseio de informações pessoais, que atingem a liberdade individual e, em mais larga escala, a conformação político-social de uma dada comunidade. Com vistas a proteção mais abrangente aos últimos valores citados, vai-se delineando um novo direito, que, de implícito em diversos corpos normativos, concretiza-se como um direito autônomo inserto em leis e textos constitucionais.

Nesse quadro, tradicionalmente aponta-se que a ideia inicial de privacidade foi delineada no final do século XIX com a publicação do artigo *The Right to Privacy*[14], de Samuel Warren e Louis Brandeis. No texto, os autores destacam, já em seu tempo, uma necessidade de evolução de conceitos para proteção adequada dos direitos. Usando como exemplo a proteção pessoal e patrimonial, afirmam que estas precisavam ser revisitadas para nova definição de sua exata natureza e extensão, abrangendo não apenas os atos físicos relacionados à sua proteção, mas os pensamentos e sentimentos envolvidos em seu contexto (por exemplo, o direito à liberdade não abrangeria apenas o ir e vir, mas a liberdade de escolher modos de vida; a propriedade não seria apenas exercida sobre objetos físicos, mas igualmente sobre bens imateriais). A partir da ideia de revisitação de direitos consolidados, passam os autores a defender também a necessidade de inovação para proteção de novos direitos, ali mencionando a privacidade, apresentada no texto como o direito de ficar só e de somente ver divulgadas informações de caráter pessoal mediante consentimento do indivíduo. Este, portanto, poderia

[14] WARREN, Samuel; BRANDEIS, Louis. **The Right to Privacy**. Civilistica.com. Rio de Janeiro, a.2, n.3, jul.-set./2013. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/127/97 . Acesso: 08 de novembro de 2023.

definir o quanto gostaria de comunicar acerca de seus pensamentos e intenções. O direito à privacidade, nesse contexto, somente cessaria quando houvesse publicização dos fatos pelo próprio sujeito ou mediante seu consentimento.

No artigo, problematiza-se a indevida ingerência de terceiros sobre aspectos pessoais dos indivíduos em geral, dando-se especial destaque às publicações de imprensa. Na ausência de específica e formal proteção a esse âmbito denominado privacidade, destacam a inexigibilidade de recurso a analogia a outros direitos reconhecidos, tais como os acima mencionados (direitos pessoais e patrimoniais), uma vez que havia tratamento normativo específico que proibia já algumas ações que se enquadrariam como representativas do direito geral de privacidade, o qual poderia ser dali extraído e estendido a situações assemelhadas. Os exemplos usados no texto dizem com o direito de não ter pensamento ou sentimentos publicizados, bem como a possibilidade de definição da extensão da publicidade caso esta ocorresse; a partir desses casos, outros assemelhados que demonstrassem igual vinculação ao desejo de ter respeitado o espaço privado deveriam estar compreendidos no direito à privacidade ali defendido.

Naquele contexto, a privacidade estaria representada pelo direito do indivíduo a "ser deixado em paz", como um direito que impõe, portanto, uma abstenção capaz de garantir uma vida autônoma e tranquilidade emocional e psicológica. O espaço em que esse direito poderia ser exercido estava bem identificado com o ambiente doméstico, na separação tradicional da esfera privada (casa) da esfera pública (mundo exterior). Dentro de seu ambiente puramente privado, o sujeito estaria a salvo de indevidas ingerências sobre suas informações pessoais e seu modo de vida, protegido do escrutínio público.

O fato de haver uma esfera privada protegida de indevidas interferências, não significa, porém, que esse desejo de ali estar deva ser tomado de forma absoluta, em um completo isolamento do indivíduo do círculo social. Hannah Arendt[15] reflete sobre a importância da interação do sujeito com o meio, onde pode, em intercâmbio com outros, exercer sua verdadeira humanidade, pois o "homem que não se dá a conhecer é como se não existisse." Portanto, deve-se considerar que deve haver um âmbito de proteção que vá além daquele possibilitado pelo simples isolamento do indivíduo do mundo exterior, mas que leve em consideração a necessidade de manutenção das naturais interações com o meio social.

---

[15] ARENDT, Hannah. **A condição humana**/Hannah Arendt; tradução de Roberto Raposo, posfácio de Celso Lafer. 10.ed. Rio de Janeiro: Forense Universitária, 2007, p.68.

Bruno Bioni destaca que seria na esfera privada que as pessoas refletiriam e pensariam criticamente para voltar a público e discutir os mais variados assuntos. Esse isolamento permitiria o pleno desenvolver de sua personalidade e de suas ideias, que poderiam, empós, diante do desejo e controle do indivíduo, vir a público para interferência no arranjo social. Nesse contexto, destaca o direito à privacidade como basilar à própria democracia[16].

Em considerando essa dual divisão de espaços – público e privado – a privacidade garantiria ao indivíduo a vedação de acesso a suas informações pessoais e íntimas, escolhendo aquelas que seriam reveladas ao público. É nesse sentido que se entende a privacidade como o direito de ser deixado em paz, ou direito de ser deixado só.

Em certa medida, a legislação nacional acatou essa dualidade, ao referir-se, quando trata da vida privada e de sua proteção, aos espaços físicos e aos objetos do tratamento normativo. Nesse sentido, lê-se, no artigo 5°, XI[17], da Constituição da República, norma que indica a casa como o asilo inviolável do indivíduo; no inciso seguinte[18], a inviolabilidade do sigilo da correspondência e das comunicações, dando-se noções básicas do que abrangido pela esfera privada do sujeito. Considerando-se as lições de Solove, a partir dos elementos apontados no texto constitucional, outras situações assemelhadas estariam incluídas no amplo guarda-chuva em que consiste a privacidade nos termos propostos.

Contudo, a dinâmica social trouxe transformações significativas na forma de interação dos sujeitos com o mundo, de forma que a divisão entre espaços públicos e privados restou cada vez mais fluida. Essas mudanças decorreram em especial do desenvolvimento das tecnologias de informação e comunicação, que impuseram novas formas de relacionamento na sociedade.

Nesse contexto, existe uma transformação do conceito de privacidade, elastecido a fim de que novos aspectos de liberdade sejam nele incluídos. Veja-se, no entanto, que não se trata de uma substituição das anteriores concepções; o desenvolvimento de definições atualizadas visa a trazer novos elementos como objeto de proteção, em um somatório, visto que

---

[16] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2021, p. 91.

[17] Art. 5º, XI: a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial.

[18] 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.

operarão em diferentes níveis. Assim, observa-se um enriquecimento da noção de esfera privada, incluindo situações diversas como juridicamente relevantes.

Na análise histórica de todo esse arcabouço, percebe-se que o continente europeu, por razões ligadas à sua história e desenvolvimento político, mostrou-se sempre atento à adequada proteção de direitos e garantias individuais. Essa particularidade, levou-o a ser pioneiro no reconhecimento da evolução aqui narrada, além de exercer grande influência sobre o arcabouço de proteção de dados em âmbito internacional.

Stefano Rodotà, um dos precursores nos estudos em torno da proteção de dados, desenvolveu obra que cuida das transformações em torno do conceito de privacidade e as implicações sobre a esfera de proteção jurídica dos indivíduos em uma sociedade marcada pelo desenvolvimento tecnológico. Desenvolve ali a ideia de que, na sociedade da informação, tendem a prevalecer definições funcionais de privacidade, as quais, de diversas formas, "fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas"[19]. O autor cuida, assim, do que chama de uma "proteção dinâmica", que vai além do recurso estático de ações contra acesso a informações pessoais, cuidando agora de aspectos voltados em especial à circulação e uso dos dados coletados. Nesse contexto, a sequência mais importante é "pessoa-informação-circulação-controle" e não mais "pessoa-informação-sigilo", que vigoraria na concepção clássica de privacidade[20].

Essa transformação social e a necessidade de criação de formas de proteção adequada de direitos basilares para a pessoa humana levaram também o Tribunal Constitucional alemão a fazer uma revisão de sua jurisprudência, que culminou com o reconhecimento do direito fundamental à autodeterminação, como uma expressão da proteção constitucional ao direito geral de personalidade e ao livre desenvolvimento da personalidade. O direto à autodeterminação e, ainda, o direito à autodeterminação informativa influenciou diversos ordenamentos estrangeiros e foi incorporado como um dos fundamentos da Lei Geral de Proteção de Dados brasileira (LGPD), sendo de elevada importância nos estudos acerca da proteção de dados. Uma breve análise dos casos paradigmáticos julgados pelo Tribunal mencionado revela a relevância da nova abordagem adotada.

Laura Schertel Ferreira Mendes, em artigo que tem como base capítulo de sua tese de doutorado, traz um apanhado histórico da jurisprudência do Tribunal Constitucional da

[19] RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. São Paulo: Renovar, 2008, p. 92.
[20] *Op. cit.* p. 93

Alemanha até o reconhecimento do direito à autodeterminação informativa, reconhecido constitucionalmente pela primeira vez na decisão referente ao recenseamento da população, em 1983[21]. Destaca a autora que o reconhecimento desse direito se apoia na evolução da interpretação de um único artigo da Lei Fundamental da Alemanha: o artigo 2º, parágrafo 1º, que garante que todos têm direito ao livre desenvolvimento da personalidade.

O conteúdo e a extensão desse direito não possuem contornos bem definidos, de modo que o entendimento do que estaria abrangido nessa concepção variou conforme o tempo, em especial na definição da amplitude da interpretação a ser-lhe conferida. Mendes, citando decisão proferida no caso "Elfes" (BVERFGE 6, 32), no ano de 1957, elucida a posição do Tribunal Constitucional, que inseriu, na definição do direito mencionado, uma liberdade geral de ação, não um direito geral da personalidade.

O processo em referência analisou pedido formulado por cidadão alemão que teve negado pedido de prorrogação de validade de passaporte sob o fundamento de ameaça à segurança e a interesse relevante da República Federal da Alemanha. Embora o reclamante tenha defendido sua posição valendo-se do direito à liberdade de locomoção e ao domicílio (art. 11, parágrafo 1º, da LF), o Tribunal analisou o caso também à luz do direito geral à personalidade, fixando sua abrangência e aplicação ao caso.

Em tradução livre, a autora traz trecho do julgado que elucida a questão:

> [...] o dispositivo constitucional que estabelece o 'livre desenvolvimento da personalidade' não pode ser entendido apenas como base para um direito à personalidade, que constitui a essência do homem como ser moral, pois não seria compreensível que o desenvolvimento de sua personalidade poderia infringir a lei moral, os direitos de terceiros ou até mesmo a ordem constitucional de uma democracia liberal, conforme estabelece a parte final do dispositivo. São precisamente estas restrições impostas ao indivíduo como membro da comunidade que mostram que a Lei Fundamental em seu art. 2º, §1º, compreende a liberdade de ação em sentido abrangente. (BVerfGE 6, 32, Elfes, tradução livre)[22].

Apesar dessa primeira posição do Tribunal, observa-se que houve posteriormente a adoção de um entendimento em que a liberdade geral de ação já não se mostrava suficiente para a proteção adequada de novas questões envolvendo o direito da personalidade, realizando-se uma releitura do direito inserto na Lei Fundamental.

---

[21] MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. **Pensar – Revista de Ciências Jurídicas**. Fundação Edson Queiroz - Universidade de Fortaleza. V. 25, n.4. 2020. Disponível em: https://ojs.unifor.br/rpen/article/view/10828/pdf . Acesso em: 11 de novembro de 2023.

[22] *Op. cit.* p. 3.

Assim, num momento seguinte, o Tribunal Constitucional reconheceu que o direito ao livre desenvolvimento da personalidade abrangia não apenas o direito de liberdade geral de ação, mas também o direito ao respeito à esfera privada. Mendes aponta que essa posição foi firmada com as decisões exaradas no caso do microcenso (BVerfGE 27, 1 (6)) e dos autos de divórcio (BVerfGE 27, 344 (352), dos anos 1969 e 1970.

Veja-se um resumo do primeiro caso:

> O juízo de Fürstenfeldbruck viu-se obrigado a aplicar norma de uma lei do micro-censo de 1957 que previa uma multa de até 10 mil marcos alemães para o caso de recusa pelos entrevistados de responder sobre os quesitos "viagens de férias" e "viagens de repouso". O juízo considerou tal dispositivo inconstitucional por violar o Art. 2 I c.c. Art. 1 I GG, e como de sua validade dependia o julgamento do caso, viu-se obrigado a, de acordo com o Art. 100 I GG, suspender o processo e apresentar a questão de constitucionalidade ao TCF.
>
> O TCF julgou presentes as condições processuais da apresentação judicial e no mérito confirmou a constitucionalidade dos dispositivos da lei do micro-censo, que havia sido questionada pelo juízo representante. Na fundamentação, o TCF considerou, em suma, que os dados levantados não atingiam a esfera íntima intocável do indivíduo e que a intervenção estava justificada por ser formalmente permitida pelo Art. 2 I GG e materialmente proporcional em face do propósito de abastecer o Estado com dados necessários ao planejamento da ação estatal[23].

Nesse processo, muito embora o Tribunal tenha permitido o uso das informações que se pretendia vetar (locais de destino em viagens de férias e viagens de repouso), destacou que a coleta dos dados somente seria permitida porque não atingia a esfera privada e íntima dos indivíduos, visto que a viagem consistia em aspecto externo de comportamento, de conhecimento do público em geral. Firmou-se que, embora a pesquisa tenha se referido a um âmbito da vida privada, não houve revelações da esfera íntima do indivíduo, assim como não concedeu ao Estado visão sobre relações que não são acessíveis ao mundo exterior e deteriam caráter sigiloso.

É de relevo destacar que, na decisão, o Tribunal ressaltou com vigor que o Estado não pode, por nenhuma medida, nem mesmo por lei, ferir a dignidade humana ou atingir a liberdade da pessoa em sua essência. Com isso, demarcou o Tribunal, concede-se ao cidadão um âmbito intangível de vida privada que não está submetido ao Poder Público, "um "espaço

[23] *BVerfGE* 27, 1, "Microsenso" (*Mikrozensus*). In: MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do tribunal constitucional federal alemão.** Montevidéu: Fundação Konrad Adenauer, 2005. Disponível em: https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf . Acesso: 11 de novembro de 2023.

interior", no qual ele "pertence a si mesmo" e ao qual "pode se recolher, ao qual os outros não têm acesso, no qual é deixado em paz, desfrutando do direito à solidão".

Linha semelhante foi adotada no caso debatido no *BVerfGE* 27, 344 (352). Neste, o Tribunal reconheceu que o direito geral de personalidade decorrente do artigo 2º, parágrafo 1º, da LF, protege a esfera íntima e privada, delas fazendo parte o âmbito familiar e as relações pessoais, bem como as relações sexuais com um parceiro. Na ação, discutia-se a possibilidade de envio dos autos de um processo de divórcio para instrução em processo administrativo disciplinar no qual uma das partes era investigada. O Tribunal, julgando o processo, considerou que os autos do divórcio estão submetidos a sigilo, com fulcro no artigo. 2º, parágrafo 1º, combinado com o artigo 1º, parágrafo 1º, da LF.

A aplicação do direito ao livre desenvolvimento da personalidade foi ganhando, portanto, contornos a partir do julgamento de casos concretos, que mostravam a necessidade de evolução – ou de adição – de novas fórmulas para proteção adequada diante das transformações sociais. Num próximo passo, o Tribunal enfrentou os desafios de proteção jurídica dos indivíduos diante das novidades tecnológicas.

Nesse novo cenário, embora os conflitos não girassem em torno da esfera íntima e privada em uma concepção tradicional, observava-se a vulnerabilidade do direito de personalidade, que exigia nova parametrização em defesa de direitos fundamentais. Um caso tradicionalmente apontado como definidor de nova postura do Tribunal refere-se ao *BVerfGE* 35, 202, caso Lebach. Veja-se resumo da lide:

> Em 1969, quatro soldados foram assassinados e um ficou gravemente ferido durante um roubo de armas e munições. O caso ficou conhecido como "o assassinato dos soldados de Lebach", em referência ao lugarejo localizado a oeste da República Federal da Alemanha onde o crime ocorreu, tendo ganhado grande notoriedade pela brutalidade com que foi cometido. Os dois principais autores foram condenados à prisão perpétua e um terceiro fora condenado a seis anos de prisão por ter auxiliado na preparação da ação criminosa.
>
> No ano de 1972, uma emissora de televisão anunciou a produção de um documentário sobre o delito, no qual reconstituiria o latrocínio, com referência aos nomes e fotos dos envolvidos, detalhes da relação entre os condenados - incluindo ligações homossexuais -, além de particularidades sobre a perseguição e prisão. O programa iria ao ar poucos meses antes da data do livramento condicional do partícipe, razão pela qual pleiteou-se medida liminar para impedir sua exibição, sob o argumento de que a veiculação desses fatos seria prejudicial à sua ressocialização, em afronta ao direito de desenvolvimento da personalidade.
>
> O Tribunal Constitucional Federal da Alemanha, tentando harmonizar os direitos em conflito (direito à informação versus direitos de personalidade), julgou procedente o pedido. A Corte entendeu que, no caso, a tutela dos direitos da personalidade preponderava sobre a liberdade de comunicação, o que justificaria a

> intervenção para proibir a transmissão do documentário até a decisão final da ação principal pelos tribunais ordinários competentes[24].

Na decisão, o Tribunal afirmou que os meios de comunicação de massa exercem forte influência sobre a opinião pública, de forma que a liberdade de imprensa deve se submeter a uma análise de proporcionalidade frente a outros direitos e interesses. No caso concreto, como a população já havia sido informada sobre o caso à época dos acontecimentos, entendeu-se que o interesse público foi atendido. Concluiu-se que as inserções posteriores na vida do condenado afetariam a esfera de seus direitos da personalidade, de modo que qualquer nova veiculação da informação usando sua imagem e seus dados foi proibida.

Para o presente estudo, interessa a percepção de que o direito ao livre desenvolvimento da personalidade ganha contornos de proteção de informações de forma mais geral, independentemente de estarem inseridas ou não no que se considera o contexto de vida privada e íntima. Ademais, esse direito de personalidade igualmente não se restringe mais à liberdade geral de ação.

No centro da questão está, ainda, a ideia de autodeterminação, segundo a qual o indivíduo pode escolher como deseja se apresentar ao público, estando a salvo de indevidas ingerências que possam traçar um perfil diverso daquele com o qual se identifica o sujeito ao desenvolver sua personalidade.

Trilhado esse caminho, outros desdobramentos foram construídos até se chegar à ideia de autodeterminação informativa, também inserida no contexto de proteção do direito ao livre desenvolvimento da personalidade, adaptado às novas necessidades decorrentes das transformações sociais. Esse novo direito foi mencionado no julgamento da lei do Censo, de 1983, referida preteritamente neste trabalho.

Informa Mendes[25] que o desenvolvimento desse conceito, apesar de inserido no julgado do Tribunal Constitucional, foi formulado, pela primeira vez, em parecer redigido por Wilhelm Steinmüller, Bernd Lutterbeck, Christoph Mallmann, Uwe Harbort, Gerhard Kolb e Jochen Schneider, por incumbência do Ministro do Interior da Alemanha. Nos termos do

---

[24] *BVerfGE* 35, 202, "Caso Lebach"(*Soldatenmord von Lebach*). **Boletim de Jurisprudência Internacional**: Direito ao Esquecimento. 5.ed. Brasília: Supremo Tribunal Federal, 2018. Disponível em: https://www.stf.jus.br/arquivo/cms/jurisprudenciaInternacional/anexo/BJI5DIREITOAOESQUECIMENTO.pdf . Acesso em 11 de novembro de 2023.

[25] *Op. cit.* p.10.

parecer, resulta do art. 2º, parágrafo 1º, da Lei Fundamental da Alemanha, um direito de autodeterminação do cidadão, segundo o qual pode ele decidir, em princípio, sobre si próprio e o uso de seus dados pessoais, definindo quais informações pessoais deseja sejam reveladas e dentro de quais limites.

Essa ideia foi inserida no clássico julgamento do Tribunal Constitucional (*BVerfGE* 65,1 (42), Recenseamento), que delineou linhas precisas da autodeterminação informativa. Nesse julgado paradigmático, observamos a referência a todos os casos anteriores aqui mencionados.

Inicialmente, mostrou o Tribunal adesão à realidade ao pontuar preocupação com a coleta de informações sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável. Ressaltou a possibilidade de armazenamento de dados ilimitado e dilatado no tempo, bem como de cruzamento entre bases diversas, que podem formar um quadro de personalidade completo – ou quase – sem que a pessoa possa controlar com exatidão o uso que será feito dessas informações e por quem. Esse cenário pode inibir substancialmente a formação da personalidade e o exercício da liberdade, afetando não apenas uma esfera individual, mas a ordem social como um todo. Nesse contexto, destaca-se a intimidação que pode ser gerada na livre participação da vida social quando o sujeito não sabe o que se sabe sobre ele e como essa informação está sendo utilizada.

Disso resulta que o livre desenvolvimento da personalidade impõe, nas condições modernas de evolução tecnológica e no uso concreto que se faz dos dados pessoais, a proteção do indivíduo contra a coleta, armazenamento, processamento, uso e transmissão de dados pessoais. Neste caso, já não importa se as informações coletadas se enquadram como íntimas, privadas ou públicas; antes, quaisquer dados são relevantes, diante do potencial lesivo de seu processamento.

Percebe-se, nesse contexto, que, mesmo dados que refugiriam à esfera do privado de um indivíduo dentro de uma concepção tradicional, passam a ter relevância considerável quando associados a outros, sendo capazes de permitir a formação de um perfil social relevante, que compromete o próprio exercício da liberdade individual. Desloca-se o foco, trazendo como objeto de proteção não mais (ou apenas) a esfera privada, mas o desenvolvimento de um direito fundamental voltado à proteção da informação e seu processamento. Observa-se, nesse quadro, que não há mais informações pessoais irrelevantes e que todo dado pessoal é capaz de, sob gestão maliciosa, acarretar exposição e comprometimento de direitos e garantias individuais.

Esse apanhado revela, portanto, como houve uma transição do âmbito de proteção dos direitos fundamentais, antes destinada a uma esfera fixa – esfera íntima ou privada – voltando-se ao poder de decisão sobre a informação.

A esse novo reconhecido direito à autodeterminação informativa e à proteção de dados, agregam-se outros que lhe são correspondentes ou deles se desdobram, como o direito ao acesso aos dados, à sua retificação, ao conhecimento dos usos que deles são feitos etc. Cuida-se, assim, de um direito abrangente, que vai além do sigilo ou vedação de acesso.

A transformação do contexto protetivo aqui desvendado ocorreu igualmente em diversos documentos de direito internacional, em cartas constitucionais e textos legais, com a finalidade de dar proteção adequada aos direitos de privacidade, autodeterminação e proteção de dados pessoais.

A evolução acima explicitada, que separa privacidade da proteção de dados, ganhou corpo formal definitivo na Carta de Direitos Fundamentais da União Europeia, do ano 2000, que trouxe em seu texto o reconhecimento da proteção de dados como um direito autônomo. A Carta, no artigo 7°, cuida do respeito pela vida privada e familiar, estabelecendo que "todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações"; no artigo seguinte, lê-se que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito". Seguindo, o artigo 8° complementa as regras para tratamento de dados pessoais, estipulando a necessidade de um tratamento leal desses dados, o uso especificado e o consentimento da pessoa interessada ou indicação de fundamento legal. Por fim, o diploma prescreve o direito de acesso e retificação dos dados, bem como a sujeição a fiscalização do cumprimento das regras por parte de uma autoridade independente. Assim, vê-se em um texto normativo a definitiva individualização de privacidade e proteção de dados como conceitos e direitos autônomos.

Além da Carta de Direitos Fundamentais da União Europeia, existem outros importantes instrumentos legislativos do continente europeu em matéria de proteção de dados:

- Convenção 108, de 1981, do Conselho da Europa[26]: convenção para a proteção das pessoas relativamente ao tratamento de dados de caráter pessoal;

[26] CONSELHO DA EUROPA. **Convenção 108**. Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2 . Acesso em 16 de novembro de 2023.

- Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995[27]: relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;
- Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002[28]: relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas;
- Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016,[29]: estabelece as regras relativas relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) nº 45/2001 e a Decisão nº 1247/2002/CE;
- Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016[30]: relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho;
- Regulamento (UE) n.º 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018[31]: relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas

[27] PARLAMENTO EUROPEU. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho**, de 24 de outubro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 16 de novembro de 2023.

[28] PARLAMENTO EUROPEU. **Diretiva 2002/58/CE do Parlamento Europeu e do Conselho**, de 12 de julho de 2002. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002L0058. Acesso em: 16 de novembro de 2023.

[29] COMISSÃO EUROPEIA. **REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO**, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434 . Acesso em 16 de novembro de 2023.

[30] PARLAMENTO EUROPEU. **Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 16 de novembro de 2023.

[31] PARLAMENTO EUROPEU. **Regulamento (UE) n.º 2018/1725 do Parlamento Europeu e do Conselho**, de 23 de outubro de 2018 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1725. Acesso em: 16 de novembro de 2023.

instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE, entrou em vigor em 11 de dezembro de 2018;

- Artigos sobre a proteção de dados em atos legislativos setoriais[32]:

— O artigo 13.º (sobre a proteção dos dados pessoais) da Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave;

— O capítulo VI (sobre salvaguardas em matéria de proteção de dados) do Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol);

— O capítulo VIII (relativo à proteção de dados) do Regulamento (UE) 2017/1939 do Conselho, de 12 de outubro de 2017, que dá execução a uma cooperação reforçada para a instituição da Procuradoria Europeia.

Na esteira do movimento do continente europeu, na segunda metade do século XX e início do século XXI, houve a adoção de normas de proteção de dados ao redor do mundo. A Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD) realizou em 2021 estudo acerca da legislação de proteção de dados e de privacidade em todo o globo, obtendo um resultado revelador. Segundo a pesquisa, 137 dos 194 países implementaram legislação para garantir a proteção dos dados e da privacidade; 71% dos países possuíam, portanto, legislação, 9% possuíam projetos de lei, 15% não possuíam legislação, não havendo dados dos outros 5% restantes[33].

A UNCTAD mostrou, ainda, que as numerosas iniciativas nacionais, regionais e internacionais seguiram abordagens regulatórias bastante diferentes, mantendo, porém, um notável grau de harmonização e coerência em torno dos princípios fundamentais que as

[32] PARLAMENTO EUROPEU. **Fichas técnicas sobre a união Europeia** – 2023. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em: 16 de novembro de 2023.

[33] **Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD). Data Protection and Privacy Legislation Worldwide. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em 16 de novembro de 2023.**

sustentam. Os princípios comuns incluem, segundo relatório elaborado pela Conferência[34], a necessidade de haver uma razão legítima para qualquer atividade de processamento; preocupação com obrigações relativas à qualidade dos dados pessoais que estão sendo processados, exigindo-se que sejam precisos, completos e mantidos atualizados. Outros princípios comuns são a necessidade de mútuo benefício, para processador e processamento; adoção de medidas de segurança dos dados contra uso indevido, perda ou destruição acidental dos dados.

Embora se observe um certo consenso sobre os princípios gerais aplicáveis à proteção de dados, não há identidade na forma como seriam melhor realizados. Diversas abordagens são adotadas com o objetivo de garantir um nível satisfatório de atendimento dos preceitos: separação dos sujeitos destinatários da norma ou sua unificação (setor privado e público, por exemplo); abordagem geral ou setorial; modos de fiscalização da aplicação das normas etc.

O modelo europeu parece seguir uma abordagem geral, diferentemente da regulação da proteção de dados nos Estados Unidos da América. Dada a influência que este país exerce na organização jurídica de muitos outros do mundo ocidental, relevante também trazer notas sobre sua organização no campo em estudo.

Não existe, nos Estados Unidos, uma regulamentação da proteção de dados em lei geral nacional. A regulação do tema é feita de forma setorial, por meio de diversos textos legais que protegem categorias ou setores bem delimitados. Exemplificativamente, podem ser citados: *Gramm Leach Billey Act* (GLBA)[35], aplicada a instituições financeiras; *Health Information Portability and Accountability Act* (HIPAA)[36], responsável pela proteção de informações confidenciais sobre a saúde de pacientes; *Children Online Privacy Protection Act* (COPPA)[37], que visa a proteger informações pessoais de crianças; *Fair Credit Reportin Act* (FCRA)[38],

---

[34] CONFERÊNCIA DAS NAÇÕES UNIDAS SOBRE COMÉRCIO E DESENVOLVIMENTO (UNCTAD). Data protection regulations and international data flows: Implications for trade and development. Disponível em: https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf. Acesso em: 16 de novembro de 2023.

[35] ESTADOS UNIDOS DA AMÉRICA. **Gramm Leach Billey Act** (GLBA). Disponível em: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf. Acesso em: 16 de novembro de 2023.

[36] ESTADOS UNIDOS DA AMÉRICA. **Health Information Portability and Accountability Act** (HIPAA). Disponível em: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf . Acesso em: 16 de novembro de 2023.

[37] ESTADOS UNIDOS DA AMÉRICA. **Children Online Privacy Protection Act** (COPPA). Disponível em: https://www.ftc.gov/system/files/2012-31341.pdf . Acesso em: 16 de novembro de 2023.

[38] ESTADOS UNIDOS DA AMÉRICA. **Fair Credit Reportin** Act (FCRA). Disponível em: https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-may2023-508.pdf. Acesso em: 16 de novembro de 2023.

definidor de proteção de dados coletados por agências de informações ao consumidor, como empresas de informações médicas e agências de crédito, entre outros[22].

Na América Latina, observa-se uma evolução no tratamento da proteção de dados pessoais entre os membros do Mercosul[39].

A Argentina editou a Lei de Proteção de Dados Pessoais nº 25.326, sancionada em outubro de 2000[40]. Em 2023, foi apresentado projeto de Lei de Proteção de Dados Pessoais[41] em ação conjunta do país com a Agência de Accesso a la Información Publica (AAIP), que está em tramitação.

No Paraguai, a proteção de dados era feita com fundamento constitucional usando como instrumento o *habeas data*. Infraconstitucionalmente, o principal diploma de tratamento do tema era a Lei nº 1682/2001[42], que dispunha sobre "regulamentação da informação em caráter privado". Em 2023 foi promulgada a Lei de Proteção de Dados Pessoais Creditícios[43], a qual, apesar de remeter a uma proteção setorial, é aplicada ao tratamento de dados em registros públicos e privados.

No Uruguai, foi editada a Lei nº18.331, que trouxe regulamentação específica sobre proteção de dados. O tema não foi tratado constitucionalmente, mas foi reconhecida a proteção de dados como "institucionalmente presente" em comunicado da *Unidad Reguladora y de Control de Dados Personales* (URCDP) – autoridade reguladora do país. Ali, a regulação do tema foi complementada pelo Decreto nº64/2020[44].

---

[39] LIMA, Cíntia Rosa Pereira de e FIGUEIREDO, Mariana Ferreira. **10 anos de proteção de dados pessoais nos países ativos do Mercosul:** Breve análise da evolução do cenário legislativo entre 2013 e 2023. Migalhas de proteção de dados. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/394405/10-anos-de-protecao-de-dados-pessoais-nos-paises-ativos-do-mercosul . Acesso em: 19 de novembro de 2023.

[40] ARGENTINA. **Habeas Data**. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790 . Acesso em: 19 de novembro de 2023.

[41] ARGENTINA. **Proyecto de Ley de Protección de Datos Personales**. Disponível em: https://www.argentina.gob.ar/sites/default/files/2018/10/proyecto_leypdp2023.pdf . Acesso em: 19 de novembro de 2023.

[42] PARAGUAI. **Ley 1.682**. Disponível em: https://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado . Acesso em: 19 de novembro de 2023.

[43] PARAGUAI. **Ley 6.534.** Disponível em: https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-de-datos-personales-crediticios . Acesso em: 19 de novembro de 2023.

[44] URUGUAI. **Reglamentacion de los arts. 37 a 40 de la ley 19.670 y art. 12 de la ley 18.331**, referente a proteccion de datos personales. Disponível em: https://www.impo.com.uy/bases/decretos/64-2020 . Acesso em: 19 de novembro de 2023.

Esse trabalho legislativo e jurisprudencial em ambiente estrangeiro influenciou o tratamento do tema em âmbito nacional, o que pode ser observado na evolução da proteção normativa explicitada no item a seguir.

3 REGIME JURÍDICO DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO NO BRASIL

3.1 O direito fundamental à proteção de dados

A proteção de dados pessoais foi alçada a direito fundamental expresso na Constituição da República por meio da Emenda Constitucional n° 115, de 10 de fevereiro de 2022, após aprovação e promulgação da Proposta de Emenda à Constituição (PEC) n° 17/19.

A Emenda alterou o artigo 5° para incluir no rol de direitos fundamentais o direito à proteção de dados, inclusive nos meios digitais. Modificou também os artigos 22 e 23, estabelecendo como competência da União legislar sobre, organizar e fiscalizar a proteção e o tratamento de dados pessoais.

Antes de se chegar à alteração formal do texto constitucional, porém, a discussão acerca do conceito e âmbito de proteção de direitos previstos na Constituição diante dos novos desafios e transformações das relações sociais seguiu caminho semelhante àquele traçado no ambiente estrangeiro acima descrito.

É importante que se destaque, ainda, que, mesmo com a previsão expressa de um direito à proteção de dados, ainda exsurgem dúvidas acerca de sua extensão e real potencialidade diante da dinâmica das relações estabelecidas na vida em sociedade. Disso se extrai a importância de analisar a construção doutrinária, legislativa e jurisprudencial em ambiente nacional, a fim de se perquirir o que pode ser esperado da aplicação dos princípios e regras que giram em torno da proteção de dados.

Inicialmente, observa-se que a Constituição da República de 1988 reproduziu, em seu texto original, a ideia de proteção da vida privada e das comunicações na forma estática sugerida nos estudos de Warren e Brandeis, como um direito negativo, um direito à não intervenção. Essa leitura é extraída do texto do artigo 5º, no qual se lê a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (inciso X), bem como do sigilo da correspondência e das comunicações (inciso XI). Nesse contexto, também é clara a dicotomia entre as esferas pública e privada, percebendo-se no texto um indicativo a partir da enumeração de situações que ocorrem em um ambiente marcadamente privado (correspondências e comunicações).

Na doutrina, o estudo do direito à privacidade seguiu rota semelhante, como expressão da tendência externa e análise preliminar do próprio texto constitucional. Tércio

Ferraz Júnior, em clássico artigo publicado em 1993, largamente citado em diversos julgados do Supremo Tribunal Federal, em que aborda o direito à privacidade e os limites à ação fiscalizadora do Estado, expressa essa propensão. No texto, expõe o jurista a correlação entre o sigilo de dados e o direito fundamental à privacidade, identificando-o como "o direito de o indivíduo excluir do conhecimento de terceiros aquilo que a ele só é pertinente e que diz respeito ao seu modo de ser exclusivo no âmbito de sua vida privada.[45]"

Essa posição foi adotada também na jurisprudência do Supremo Tribunal Federal que, em mais de uma oportunidade, interpretou de maneira bastante limitada o conteúdo do direito à privacidade. No ano 2001, o Tribunal reconheceu a possibilidade de o Ministério Público solicitar informações bancárias de beneficiários de auxílio governamental no Mandado de Segurança 21.729/DF.

Veja-se resumo do caso:

> "O Banco do Brasil ajuizou mandado de segurança arguindo como ato de constrangimento o ofício do procurador-Geral da República de folha 21, reclamando o atendimento a pedidos anteriores, da Coordenadoria da Defesa dos Direitos da Pessoa Humana da Procuradoria da República no Distrito Federal, visando ao fornecimento da lista dos beneficiários de liberação de recursos, em caráter emergencial ao setor sucroalcoleeiro, bem como dados sobre encontrarem-se, ou não, os favorecidos com os créditos em débito para com o Banco, pedindo-se deste, ainda, esclarecimentos sobre a natureza das operações e as respectivas situações." [46]

No processo em análise, o Ministro relator, Marco Aurélio Mello, pontuou que o direito à preservação da intimidade mostrava-se de forma alargada e que, nos termos do texto constitucional, o sigilo de dados somente poderia ser excepcionado mediante ordem judicial para fins de investigação criminal ou instrução processual penal, não sendo possível solicitação por órgão não investido no ofício judicante. Ventilou, ainda, a limitação ao próprio acesso em razão do texto do artigo 5º, XII, da Constituição, e que a expressão "no último caso" para muitos estaria ligada apenas ao sigilo das comunicações. Com esse fundamento, concedeu a ordem solicitada.

Contudo, prevaleceu, no Tribunal, entendimento divergente, no sentido de que seria possível a cessão das informações dos usuários ao Ministério Público Federal para os fins visados. O ministro redator do caso foi Néri da Silveira, que proferiu voto no sentindo vencedor.

---

[45] FERRAZ JÚNIOR, Tércio. **Sigilo de dados**: o direito à privacidade e os limites da função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, p. 430-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231 . Acesso em 11 de novembro de 2023.

[46] BRASIL. Supremo Tribunal Federal. **Mandado de Segurança 21.729**. Distrito Federal. Relator: Ministro Marco Aurélio. Redator do acórdão: Ministro Néri da Silveira. DJ PP-00033. VOL-02048-01. PP-00067, 19 de outubro de 2001. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85599 . Acesso em: 11 de novembro de 2023.

Silveira fundamentou voto aduzindo que "não cabe chegar ao ponto de afirmar que a mera referência ao nome de quem teria sido beneficiado ou contratante, em um determinado empréstimo subsidiado pelo erário federal, em razão de um plano de Governo, constituiria matéria encoberta pelo sigilo bancário". Há destaque no voto ao fato de haver envolvimento de recursos públicos na análise. Com base nesse fundamento, indeferiu a segurança pleiteada.

Vale destacar, ainda, nesse julgamento, manifestação do Ministro Maurício Corrêa, o qual defendeu que o direito à privacidade, destinado a proteger indivíduos, "não protege operações bancárias praticadas em contas fictícias – que não têm privacidade a ser juridicamente protegida – nem pode acobertar crimes ou outros ilícitos, sejam administrativos ou civis". Ademais, ressaltou que o direito individual tem por limite interesses maiores, que dizem respeito ao interesse público. O ministro concluiu seu voto deferindo a segurança apenas por entender que não pode haver a solicitação referida por autoridade administrativa, sendo impositiva intervenção e autorização judicial como moderadora na resolução dos litígios em que se observe conflito de interesses; neste caso, o interesse individual de privacidade e o interesse do órgão do Ministério Público de limitá-la para exercício de suas funções.

Interessa nesse julgado a posição bastante conservadora do STF no que respeita à privacidade do indivíduo, a qual é vista como passível de afastamento diante de "interesse público maior". No caso, não houve, por parte dos Ministros, problematização quanto ao alcance específico das normas do artigo 5º, X e XII, mas a observação de que não existem direitos de caráter absoluto.

Veja-se, ainda, que o pedido realizado pelo Ministério Público para o Banco do Brasil, e referendado pelo Tribunal, foi bastante genérico, requerendo-se informações de todos os favorecidos pela política pública, não apenas daqueles sobre os quais recaía alguma suspeita de fraude ou possível prática de crime aptas a serem investigadas. Essa questão, porém, não foi enfrentada no voto de qualquer dos Ministros julgadores, mas foi um dos elementos decisivos em decisão futura, quando o STF declarou inconstitucional Decreto que determinava às empresas de telefonia a entrega de informações de cadastros dos consumidores no período da pandemia da Covid-19, como será visto a seguir.

Em 2006, o tema voltou à tona no Supremo Tribunal Federal no julgamento do Recurso Extraordinário 418.416-8/SC[47]. Eis um resumo do caso:

---

[47] BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 418.416-8/SC**. Distrito Federal. Relator: Ministro Sepúlveda Pertence. Redator do acórdão: Ministro Sepúlveda Pertence. Julgamento em 10 de maio de 2006. DJ 19 de dezembro de 2006. Ementário n° 2261-6. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790 . Acesso em: 11 de novembro de 2023.

> Em juízo federal, foi deferido pedido de busca e apreensão na sede de duas empresas, das quais o recorrente era sócio-gerente, sob o fundamento de que documentos que instruíam requerimento do Ministério Público – autos de reclamação trabalhista e declaração de importação e fatura – indicavam a existência de "caixa 2", "falta de registro de empregados" e "sonegação de tributos.
>
> Após a apreensão, o juízo determinou a extensão dos efeitos do decreto de busca e apreensão para que a Receita Federal e a fiscalização do INSS tivessem acesso aos dados, documentos e informações fiscais, bancárias, financeiras e eleitorais das empresas.
>
> O recorrente foi condenado criminalmente, com decisão confirmada em segunda instância. Interpôs o recurso extraordinário alegando: 1) omissão na análise de teses de defesa e 2) equívoco da condenação, que teria sido baseada em prova obtida por meio ilícito, alegando que a decisão que determinou a busca e apreensão violou a proteção constitucional ao sigilo das comunicações (artigo 5º, X, XI, XII, LIV, LV e LVI).
>
> O recorrente também impetrou habeas corpus (HC 83.168-1/SC) com o objetivo de cassar a decisão que autorizou a quebra da confidencialidade de elementos sigilosos obtidos na busca e apreensão, ao estender à Receita Federal e à Fiscalização do INSS o acesso a todos os dados obtidos.

Foi relator do processo o Ministro Sepúlveda Pertence, que emitiu voto vencedor no sentido de negar provimento ao recurso extraordinário e julgar prejudicado o HC 83.168-1/SC, que transcorria apensado. Assim, foi mantida a condenação sob o fundamento de não ter havido ofensa à norma constitucional do sigilo de dados. Foi voto vencido apenas o Ministro Marco Aurélio Mello, que deu provimento ao recurso acolhendo a primeira tese defendida de ausência de análise, pelo tribunal de origem, de teses relevantes da defesa.

Asseverou o Ministro Sepúlveda Pertence, acompanhado dos demais, que a proteção a que se refere o artigo 5º, XII, da Constituição "é da comunicação 'de dados' e não os dados, o que tornaria impossível qualquer investigação administrativa, fosse qual fosse". Ademais, destacou que as instâncias de mérito não valoraram nenhum dado resultante da busca e apreensão e, portanto, não teria havido, no ponto, prejuízo concreto ao recorrente.

No julgamento, o Ministro Cezar Peluso reforçou a tese ao pontuar que a norma do artigo 5º, XII, quando alude ao sigilo das correspondências e das comunicações telegráficas, refere-se não propriamente ao que constitua o objeto das comunicações, "ou seja, os registros ou o conteúdo dos relatos da comunicação considerados em si mesmos, mas à integridade do processo de comunicação ou de relacionamento intersubjetivo". Observa-se, portanto, que se considerava a proteção voltada apenas ao processo de transmissão de informações, mas não aos dados em si mesmos considerados.

Por fim, insta realçar que somente o Ministro Ricardo Lewandowski demonstrou reprovação quanto ao envio dos dados apreendidos para a Receita Federal e a fiscalização do INSS. Assim, votou com o relator no recurso extraordinário, concedendo parcialmente a ordem

no *habeas corpus* para que os dados não fossem utilizados por terceiros, salvo para fins específicos de processo criminal.

Nesta fase, o Supremo Tribunal Federal demonstrou, portanto, não considerar os dados objetos passíveis de proteção por si, mas somente a sua transmissão. Considera-se pertencente à esfera privativa esta última, a qual não seria passível de violação por terceiros estranhos à comunicação. Outrossim, não se problematizou questão referente ao compartilhamento de dados e ao uso específico que se poderia fazer deles, nem mesmo o impacto que esta conduta poderia causar à esfera de privacidade dos usuários do serviço, questões de extrema relevância no estágio atual da disciplina normativa.

Num passo seguinte, tem-se uma guinada na posição do Tribunal. Esta foi observada nos autos da ADI 6.387 MC-Ref/DF, na qual, em decisão paradigmática do plenário, chancelou-se provimento monocrático da ministra Rosa Weber para reconhecer a necessidade de proteção de dados como garantia do direito à privacidade, à autodeterminação informativa e ao livre desenvolvimento da personalidade. O teor do julgamento merece destacada atenção, uma vez que traz importantes reflexões e o posicionamento da Suprema Corte acerca dos limites de atuação do Estado para persecução de seus fins diante da necessidade de proteção de dados e informações pessoais dos administrados[48].

Tenha-se presente o caso:

> Foi proposta ADI pelo Conselho Federal da Ordem dos Advogados do Brasil – CFOAB contra o inteiro teor da Medida Provisória (MP) n° 954, de 17 de abril de 2020, a qual 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 n° 13.979, de 6 de fevereiro de 2020*".
>
> Para atendimento dos fins visados na norma, as empresas telefônicas deveriam disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, números de telefone e endereços dos consumidores, pessoas físicas ou jurídicas. Ressaltava a MP, outrossim, que o procedimento seria aplicado por prazo determinado – duração da situação de emergência de saúde pública decorrente do coronavírus, que os dados não seriam disponibilizados para quaisquer empresas públicas ou privadas ou a órgãos da administração pública de quaisquer entes federativos, bem como que seria realizado e divulgado relatório de impacto à proteção de dados pessoais nos termos preconizados pela LGPD e que, superada a situação de emergência de saúde pública, as informações seriam eliminadas das bases de dados da Fundação IBGE.

[48] A Medida Provisória n° 954/2020, foi objeto, ainda, das ADIs n° 6388, 6389, 6390 e 6393, propostas, respectivamente, pelo Partido da Social Democracia Brasileira (PSDB), Partido Socialista Brasileiro (PSB), Partido Socialismo e Liberdade (PSOL) e Partido Comunista do Brasil (PCB).

Apesar da demonstração de cuidado, por parte do Executivo quando da edição da Medida provisória, com algumas normas preconizadas pela LGPD acerca do tratamento adequado de dados, como realização de relatório de impacto, limitação do compartilhamento dos dados e sua eliminação após cessados os motivos que justificaram a coleta no formato apresentado, a ministra relatora concedeu medida cautelar suspendendo a eficácia da Medida Provisória, o que foi confirmado pelo plenário do Tribunal.

Destacou a Ministra Rosa Weber a especial proteção que a Constituição da República conferiu à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade. Ademais, realçou que, a fim de instrumentalizar tais direitos, a Constituição previu, no artigo 5°, XII, a inviolabilidade do sigilo de dados, direitos que seriam malferidos caso as informações solicitadas fossem repassadas.

Ponto relevante, ainda, do voto, consiste na afirmação de que o respeito à privacidade e à autodeterminação informativa foram positivados no artigo 2°, I e II, da LGPD, como fundamentos específicos da disciplina de dados pessoais. Por fim, ressaltou a ausência de indicação precisa da finalidade da coleta das informações, a falta de mecanismo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, bem como o equívoco de se realizar relatório de impacto após o início da coleta e do tratamento dos dados.

Os fundamentos utilizados pela relatora foram acolhidos pelos demais ministros da Corte, ressalvado o voto divergente do ministro Marco Aurélio Mello, o qual negou referendo à medida cautelar concedida, entendendo hígida a Medida Provisória em referência. Ressaltou o Ministro a importância dos dados para a execução da política pública, bem como a confiabilidade a ser conferida ao Instituto Brasileiro de Geografia e Estatística.

Na votação do plenário, merecem destaque, ainda, os votos dos Ministros Luiz Fux e Gilmar Mendes, que pontuaram de forma enfática a necessidade de a Corte aprofundar a identificação, na ordem constitucional brasileira, de um autônomo direito à proteção de dados pessoais, a fim de se estabelecer o âmbito de resguardo de direitos e os limites constitucionais à intervenção do Estado nessa esfera.

Dessa forma, ainda que não tenha constado expressamente na ementa do julgado, discutiu-se na ADI – com defesa expressa nos votos mencionados – a existência, no Brasil, de um implícito direito à proteção de dados pessoais, autônomo em relação ao direito à privacidade, mas consectário deste e do princípio da dignidade da pessoa humana.

Destaca-se, nesta oportunidade, trecho do voto do Ministro Gilmar Mendes, que expressa opinião relevante no presente estudo. Nos termos de sua manifestação, o direito fundamental à proteção de dados estaria lastreado em três bases fundamentais: (i) no direito fundamental à dignidade da pessoa humana; (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, X, da CF/88) diante dos novos riscos derivados do avanço tecnológico e (iii) no reconhecimento da centralidade do *habeas data* enquanto instrumento de tutela material do direito à autodeterminação informativa.

Objetiva-se analisar neste trabalho os riscos decorrentes da coleta e tratamento de dados realizados para fins de segurança pública e de atividade de investigação e repressão de infrações penais, as quais não possuem delimitação precisa no ambiente normativo já elaborado no país. Relembra-se que a LGPD, no artigo 4º, inciso III, traz expressa exceção à aplicação do diploma, não havendo ainda sido produzido qualquer documento normativo que visa à regulação da proteção de dados nesse setor.

Diante do vácuo legislativo, faz-se mister o recurso às normas constitucionais e legais já existentes, que deverão guiar o Poder Público na atividade de coleta, tratamento, uso e compartilhamento de dados para fins de segurança e investigação penal. Ressalta, assim, a importância do destaque feito no voto do Ministro Gilmar Mendes à força normativa da Constituição, com a necessidade de exercício de uma interpretação das normas constitucionais que lhes garanta uma concretização ótima, adaptando-a aos fatos concretos da vida.

Esta foi, pois, a evolução do tratamento jurisprudencial dado à privacidade e à proteção de dados no direito brasileiro, ao qual foi somada a promulgação da Emenda Constitucional n° 115, de 10 de fevereiro de 2022, e da Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei n° 13.709, de 14 de agosto de 2018.

Além da Constituição e da LGPD, há proteção adicional à privacidade e aos dados em diversos outros diplomas legais do país, os quais, de maneira setorial, regularam a matéria. Entre estes: o Código de Defesa do Consumidor (Lei n° 8.078/90 – Seção VI – Dos Bancos de Dados e Cadastros de Consumidores); a Lei do Cadastro Positivo (disciplina a formação e consulta a bancos de dados com informações de adimplemento para formação de histórico de crédito); a Lei de Acesso à Informação (Lei n° 9.507/97); o Marco Civil Internet (Lei n° 12.965/2014).

A importância do conhecimento do arcabouço normativo relativo à proteção de dados é essencial para garantir proteção adequada aos direitos e liberdades individuais.

Outrossim, merece destaque a determinação expressa no artigo 5º, §2º, da Constituição da República, que dispõe que direitos e garantias nela expressos não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais de que o Brasil faça parte. Fazem parte do bloco de constitucionalidade, contudo, apenas tratados e convenções internacionais sobre direitos humanos aprovados em regime equivalente ao de emendas constitucionais, pelo art. 5º, § 3º.

Visto o histórico estrangeiro e brasileiro da evolução do direito à privacidade e à proteção de dados pessoais, passa-se à análise específica do regime jurídico aplicado ao Poder Público no Brasil nesta seara.

3.2 Análise principiológica da proteção de dados no setor público

A Lei Geral de Proteção de dados (LGPD), promulgada em 2018, tem como objetivo declarado regulamentar a atividade de tratamento de dados pessoais e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Observa-se, portanto, um grande direcionamento da lei para proteção do indivíduo em sua esfera privada.

No texto, são minudenciados os fundamentos da disciplina da proteção de dados, os princípios aplicáveis, as hipóteses em que o tratamento de informações é permitido, bem como regras específicas aplicadas ao setor público, entre outras.

Dentre as normas de realce, está aquela que veicula a base principiológica para tratamento de dados, a qual se direciona ao ambiente privado e ao público. Os princípios aplicados às atividades de tratamento estão descritos no artigo 6º, nomeadamente: I – finalidade; II – adequação; III – necessidade; IV – livre acesso; V – qualidade dos dados; VI – transparência; VII – segurança; VIII – prevenção; IX – não discriminação e X – responsabilização e prestação de contas.

Os princípios mencionados devem ser respeitados em todas as atividades que envolvem o gerenciamento de dados, sendo aplicáveis mesmo nas hipóteses em que a LGPD ressalva sua aplicação. Na norma do artigo 4º estão situações de exceção da aplicabilidade da Lei, entre as quais o tratamento de dados realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. No §1º do dispositivo, vê-se a expressa menção à aplicação dos princípios gerais da proteção de dados mesmo nos casos de segurança nacional e instrução penal, devendo, nessa

hipótese, serem atendidos, ainda, o devido processo legal, os direitos do titular previstos na Lei e comedimento na adoção de medidas para atendimento do interesse público.

Revelado todo o potencial tecnológico na coleta, armazenamento, tratamento e análise de dados, que possibilita a empresas e governos elevado grau de perfilhamento e identificação de indivíduos em grupos sociais, ressalta a importância de proteção adequada por meio das normas postas. Observado, ainda, o uso efetivo dessas informações para delineamento de estratégias e tomada de decisões, estas passíveis de interferência por vieses e inconsistências, essencial o arcabouço principiológico delineado na LGPD. A própria Lei, ao enumerá-los, define seu conteúdo, fixando limites de conduta e garantias dos indivíduos no processo de tratamento de dados pessoais.

Referidos princípios devem conviver e se harmonizar com outros que circundam a atuação do Poder Público, expostos na Constituição, em leis esparsas e na doutrina especializada. Aqui, ganham destaque aqueles que interessam à coletividade, em grande medida imperativos diante de interesses privados. Nesse contexto, surge a questão de como harmonizar, na seara pública, princípios que, ao menos de início, parecem caminhar em direções opostas.

Na Constituição, no capítulo que trata da administração pública, lê-se que esta obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência. A Lei n°9.784/99, que regula o processo administrativo no âmbito da União, indica outros tantos: finalidade, motivação, razoabilidade, proporcionalidade, interesse público.

Destes, percebe-se que alguns convergem de forma imediata para aqueles previstos na LGPD. O princípio da legalidade amolda-se com perfeição, vez que, na proteção de dados pessoais, cuida-se das bases legais que autorizam o tratamento no âmbito do Poder Público. O princípio da impessoalidade se avizinha ao da não-discriminação, o qual determina a impossibilidade de realização de tratamento de dados para fins discriminatórios ilícitos ou abusivos. A razoabilidade e a proporcionalidade aproximam-se do princípio da necessidade, entendido como a limitação do tratamento ao mínimo necessário para realização de suas finalidades.

Contudo, parece haver um convívio mais conflituoso entre os princípios da publicidade, da eficiência e do interesse público diante dos princípios e regras que visam à proteção das informações dos cidadãos diante da ação pública.

Veja-se que mesmo termos que parecem inicialmente confundir-se diante de um sentido comum, como transparência (princípio da LGPD) e publicidade (princípio da administração pública em geral), indicam contextos distintos. A transparência indicada na LGPD representa garantia, aos titulares (pessoais individuais), de informações claras, precisas

e facilmente acessíveis sobre a realização e tratamento de dados, não destinadas imediatamente ao público em geral, ao qual deve ser aplicada moderação no acesso aos dados de terceiros. A publicidade como princípio da administração pública, ao revés, é destinada ao grande público e exige do Estado a maior transparência possível nas ações e decisões, para que toda a população tenha acesso a suas razões e resultados.

Existe, assim, uma aparente tensão entre publicidade e privacidade, que tem sido suscitada no contexto da necessidade de conciliar as regras que impõem ao Estado um elevado grau de transparência em suas atividades e aquelas que exigem que dados pessoais sejam tratados de maneira a preservar a intimidade e a vida privada dos cidadãos[49].

Dentro dessas balizas deve ser analisado também o princípio da supremacia do interesse público sobre o interesse privado, o qual, embora não previsto em dispositivo específico da Constituição, pode ser extraído a partir de manifestações concretas de sua aplicação, a exemplo do princípio da função social da propriedade, da defesa do meio ambiente, entre outros. Como expressão desta supremacia, a Administração pode, por representar o interesse público, afastar proteção a certos direitos dos cidadãos individualmente considerados, constituir terceiros em obrigações e outros atos imperativos de Estado. Nessa esteira, aqueles direitos e valores protegidos pela LGPD poderiam ser atingidos, criando um estresse jurídico.

O deslinde para essa questão deve vir da consideração de dois elementos essenciais. Celso Antônio Bandeira de Mello[50] destaca, no que interessa ao ponto aqui levantado, que o princípio da supremacia do interesse público terá apenas a extensão e compostura que a ordem jurídica lhe houver atribuído na Constituição e nas leis com ela consonantes. Assim, não cabe sua invocação abstrata, vez que sua dimensão, intensidade e tônica serão delineados pela ordem jurídica como um todo e, na aplicação da supremacia do interesse público sobre o privado, balizas deverão ser aplicadas, entre estas os textos normativos que cuidam da proteção de dados pessoais.

Outrossim, é necessário que se dê uma visão mais alargada da privacidade e da proteção de dados pessoais, que leve em consideração seu valor de caráter social e não meramente individualista. É comum uma visão mais tradicional do liberalismo que põe em tensão indivíduos – e seu direito à privacidade – e a comunidade mais ampla. Nessa visão, a

---

[49] WIMMER, Miriam. O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In: BIONI, Bruno Ricardo; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (org.). **Tratado de proteção de dados pessoais**. São Paulo: Forense, 2022.

[50] MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 32.ed. ed. rev. e atualiz. São Paulo: Malheiros, 2015.

privacidade é tida como uma indulgência individual em detrimento da sociedade, levando à negligência das necessidades do coletivo.

Argumentando contra essa posição, Solove[51] destaca que normalmente os efeitos da perda de privacidade na liberdade, cultura, criatividade, inovação e vida pública não são considerados na avaliação realizada nesse tensionamento. Visando à superação de uma dicotomia aparentemente irreconciliável, propõe uma abordagem pragmática do valor privacidade, que deve ser avaliado com base em suas contribuições para a sociedade e em acordo com o bem comum.

O autor ressalta a dificuldade de pessoas participarem livremente da vida pública sem algum grau de controle sobre sua reputação e vida privada. Assim, a privacidade, mais do que uma necessidade ou desejo psicológico, é, em seu entender, uma dimensão profunda da estrutura social, com efeitos sobre a dinâmica do poder e da liberdade da sociedade como um todo.

Na mesma linha do aqui exposto, a decisão do TCF acerca da Lei do Censo de 1983, anteriormente mencionada, destaca que a ausência de controle dos cidadãos sobre quem, o que e quando se sabe sobre eles não são compatíveis com o direito de autodeterminação na informação. Tal implicação não prejudicaria apenas, acresce a decisão, as chances de desenvolvimento individual do cidadão, mas também o bem comum, dado que autodeterminação é condição funcional elementar para uma sociedade democrática e livre, fundada na capacidade de ação e de participação de seus cidadãos. Essa questão será aprofundada em item seguinte deste trabalho.

Do exposto, tem-se que, se entendida a privacidade apenas do ponto de vista do indivíduo, esta pode estar em desvantagem diante dos interesses sociais. Contudo, quando vista em seu valor social, fornece proteção adequada à coletividade contra danos, controles e rupturas indesejadas. Esta última é a concepção vigente acerca da privacidade, que passou por uma profunda transformação decorrente das mutações sociais, entre as quais o desenvolvimento de tecnologias capazes de atingir direitos fundamentais históricos e, de maneira ainda mais incisiva, a própria ordem democrática. O desenvolvimento desse tema levou ao reconhecimento da proteção de dados como direito autônomo e, no caso brasileiro, elevado a nível constitucional pela Emenda Constitucional n°115, de 10 de fevereiro de 2022. Nesse cenário, importante a consideração da proteção de dados pessoais para além de um interesse meramente individual, alocando-o como um valor social também relevante.

---

[51] SOLOVE, Daniel J. **Understanding Privacy**. Cambridge: Harvard University Press, 2008.

As especificidades dessa questão não foram esquecidas pela LGPD, que trouxe capítulo específico para regular o tratamento de dados pessoais pelo Poder Público, ditando, desde logo, que este somente poderá ser realizado para o atendimento de finalidade pública, persecução de interesse público, execução de competências legais ou cumprimento de atribuições legais do serviço público, bases legais bem delimitadas, examinadas a seguir.

3.3 Bases legais para o tratamento de dados pelo Poder Público

A partir da segunda metade do século XX, observou-se no mundo, como anotado em linhas pretéritas, grandes transformações sociais, políticas e culturais, algumas das quais influenciadas pela revolução ocorrida no âmbito da tecnologia e dos sistemas de comunicação. As tecnologias digitais, que ainda no século XX já conviviam com a integração em rede e inteligência artificial, tornaram-se cada vez mais sofisticadas e integradas, ganhando a tecnologia papel central na articulação de novas relações.

Klaus Schwab[52], que cunhou o termo Quarta Revolução Industrial para identificação desse período, informa que esta não diz respeito apenas a sistemas e máquinas inteligentes e conectadas, diferenciando-se de outras fases de evolução pela fusão de tecnologias e interação entre os domínios físicos, digitais e biológicos.

Schwab apresenta 23 mudanças tecnológicas em curso, que transformam radicalmente o universo humano. Estas dizem respeito a: 1) acesso à tecnologia, com avaliação da presença digital na internet e uso de equipamentos inteligentes, como *smartphones*; 2) alterações no ambiente social, com o desenvolvimento da internet das coisas, de casas conectadas e cidades inteligentes; 3) alterações gerenciais nos Estados com o incremento de informações propiciadas pelo *big data* e pela inteligência artificial e 4) mudanças biológicas, como conecção de pessoas a dispositivos, para comunicação, localização e monitoramento.

Entre as principais características desse movimento, são destacados: a *velocidade* da inovação, que cresce em ritmo exponencial; a *amplitude* desta, dada a escala surpreendente dos números que congrega e o espaço de influência que atinge e a *integração* de descobertas e disciplinas diferentes.

Dentre os fenômenos desse universo tecnológico, tem-se o *Big Data*, marca distintiva da contemporaneidade, que vive uma explosão de dados. A conectividade e a

[52] SCHWAB, Klaus. **A Quarta Revolução Industrial**. São Paulo: Edipro, 2016, p. 19.

expansão das relações em rede geram um imenso volume de informações que cresce de forma exponencial. Esse conceito ganhou notoriedade no começo dos anos 2000, quando Doug Laneyschwa formulou a definição de *Big Data* sustentada em três premissas: volume, velocidade e variedade[53].

Esses dados podem ser tratados com a utilização de inteligência artificial por meio de algoritmos, ou podem ser processados para que se analisem padrões e façam prognósticos, encontrando, sem qualquer comando prévio, padrões e resultados de interesse.

Nesse contexto, são inúmeras as formulações teóricas que propõem que os novos recursos tecnológicos devem ser usados pela Administração Pública com o fito de melhor gerir a atividade a ser prestada aos cidadãos. Vantagens como indicação da melhor alocação de serviços públicos, intercomunicação entre os órgãos e atores sociais e ampliação do acesso a serviços e à Administração são destacados como vantagens desse modelo[54]. O uso de tecnologia pela Administração Pública já não é apenas uma projeção, porém, sendo utilizado nas diversas atividades estatais.

São muitos os benefícios que podem advir do uso da tecnologia na esfera pública decorrentes das predições e das decisões automatizadas. Contudo, também são muitas as preocupações a ela relativas. Shoshana Zuboff[55] explica como o capitalismo da vigilância baseia-se no *behavioral suplus*, i.e., no superávit comportamental, que entrega dados além dos necessários para os fins que justificam sua coleta. Adverte, ainda, como pensamentos, sentimentos e interesses podem ser construídos a partir de informações desestruturadas a respeito dos indivíduos.

Devido ao cenário anotado, procura-se bem delimitar e controlar as hipóteses em que está autorizado o tratamento de dados pessoais, visto que os resultados daí decorrentes podem levar ao desrespeito e tolhimento de direitos individuais e, em última instância, ao comprometimento da própria ordem social.

---

[53] ARAÚJO, Valter Shuenquener de; ZULLO, Bruno Almeida; TORRES, Maurílio. Big Data, algoritmos e inteligência artificial na Administração Pública: reflexões para a sua utilização em um ambiente democrático. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 20, n. 80, p. 241-261, abr./jun. 2020.

[54] REIS, Camille Lima; CARVALHO, Fábio Lins de Lessa. O fomento às novas tecnologias na Administração Pública como direito ao desenvolvimento. **International Journal of Digital Law**, Belo Horizonte, ano 1, n. 3, p. 11-28, set./dez. 2020. Disponível em: https://journal.nuped.com.br/index.php/revista/article/view/15. Acesso em: 14 de fevereiro de 2022.

[55] ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução George Schlesinger, 1. Ed. Rio de janeiro: Intrínseca, 2020, p. 85.

A Lei Geral de Proteção de Dados delimita as hipóteses em que poderá ser realizado o tratamento no artigo 7º e, em se tratando de dados sensíveis, no artigo 11. Esses dispositivos devem ser interpretados de forma sistemática, adicionando-se-lhes os critérios do artigo 23, que complementa os anteriores e norteia o caminho interpretativo das bases legais. Cuidar-se-á daquelas aplicáveis ao Poder Público.

3.3.1 Consentimento

A LGPD define consentimento, no artigo 5º, XII, como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Da apresentação posta, percebe-se a existência de alguns elementos centrais para que esse consentimento seja considerado válido, permitindo o tratamento de dados pessoais do seu titular.

Em primeiro lugar, tem-se que a decisão de autorizar o uso de dados deve ser precedida de plena informação acerca dos usos e riscos do tratamento dos dados, atendendo-se também nessa vertente ao mandamento de transparência, alocado como princípio da LGPD. A informação deve ser clara, precisa e facilmente acessível. Adicionalmente, em se tratando de dados sensíveis, o consentimento deve ser dado de forma específica e destacada (art. 11, I, LGPD).

Em complemento, a manifestação deve ser inequívoca, sendo vedada a autorização tácita e para finalidades genéricas. O consentimento deve, por fim, ser livre, de forma que não será válida a autorização dada de forma compulsória para o acesso a serviço ou ao exercício de direito pelo titular.

No campo público, será bastante comum o tratamento de dados para cumprimento de obrigações legais ou regulatórias, para atendimento de políticas públicas ou para fins de segurança e defesa nacionais e instrução em procedimentos penais, mostrando-se a base legal do consentimento bastante mitigada, embora não totalmente excluída. Ressalta-se, outrossim, que a informação de dados será exigida para acesso a muitos serviços, de forma que não poderá ser considerado que esses dados foram conferidos mediante consentimento livre.

A Autoridade Nacional de Proteção de Dados (ANPD) reconhece, no Guia Orientativo para Tratamento de Dados Pessoais pelo Poder Público[56] a dificuldade de aplicação

[56] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo para Tratamento de dados pessoais pelo Poder Público**. Versão 2.0. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-

desta base legal, recomendando que outras devem ser preferidas na indicação a ser fornecida pela Administração.

3.3.2 Legítimo interesse

A base legal do legítimo interesse está prevista no artigo 7º, IX, da LGPD. Assim como no caso do consentimento, essa base terá aplicação bastante restrita no ambiente público.

Depende a hipótese da realização de um juízo de proporcionalidade, avaliando-se, de um lado, o interesse legítimo do controlador ou de terceiro e, de outro, o do titular dos dados, seus direitos e liberdades fundamentais.

Adverte a ANPD, no guia orientativo, que sua utilização não é apropriada quando o tratamento de dados pessoais é realizado de forma compulsória ou quando for necessário para o cumprimento de obrigações e atribuições legais do Poder Público, as quais conformam-se em bases legais próprias.

Nessas situações, adverte a Autoridade Nacional, não há como realizar uma ponderação entre as expectativas dos titulares e os interesses estatais, visto que estes deverão prevalecer por imposição normativa. É recomendável, portanto, que os órgãos e entidades da Administração Pública evitem recorrer ao legítimo interesse como base legal para ação.

Não obstante, eventualmente essa base pode ser aceita quando a utilização dos dados não for compulsória ou quando a atuação estatal não se basear no exercício de prerrogativas estatais típicas, que decorrem do cumprimento de obrigações legais. Nesse caso, deverá ser feita a ponderação entre os interesses e legítimas expectativas de todos os sujeitos envolvidos no tratamento dos dados.

O Guia fornece como exemplo tratamento de dados pessoais com finalidade de garantir segurança dos sistemas de informação – servidores devem fornecer dados pessoais para acesso restrito a matérias de interesse público. Nesse caso, vislumbra-se o equilíbrio entre as legítimas expectativas dos envolvidos. Destaca-se, porém, que é necessário que sejam adotadas medidas para garantir a transparência do tratamento de dados na hipótese.

3.3.3 Cumprimento de obrigação legal ou regulatória

publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 17 de novembro de 2023.

O artigo 23, da LGPD, determina que o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. O artigo 7º, por sua vez, indica a hipótese como "cumprimento de obrigação legal ou regulatória pelo controlador" dos dados.

A aplicação do dispositivo ocorrerá, portanto, em dois contextos distintos, que serão diferenciados conforme a natureza da norma jurídica que estabelece a obrigação a ser cumprida. O Guia da ANPD diferencia-as entre "normas de conduta" e 'normas de organização".

Normas de conduta são regras que disciplinam "um comportamento, em geral estabelecendo um fato ou uma hipótese legal, com uma possível consequência em caso de descumprimento"[57]. O comportamento mandatório por ser positivo ou negativo, o qual, desrespeitado, sujeita o agente a penalidades estabelecidas.

Normas de organização, por sua vez, são normas que estruturam órgãos e entidades e estabelecem suas competências e atribuições[58]. Neste caso, o tratamento de dados será necessário para o exercício de prerrogativas estatais típicas, viabilizando a execução das atividades que está a cargo do agente, do órgão ou da entidade efetivar. O descumprimento da norma pode inviabilizar ou dificultar a atividade em si, mas não sujeita o agente a qualquer sanção. Exemplo dessa modalidade é o tratamento de dados realizado pelo Tribunal Superior eleitoral para organização e realização de eleições.

3.3.4 Execução de políticas públicas

O inciso II, do artigo 7º, da LGPD, estipula que poderá haver tratamento de dados pessoais 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 referente às regras especiais aplicáveis ao Poder Público. Em se tratando de dados sensíveis, exige-se que a política pública esteja prevista em lei ou regulamento, não se admitindo outros instrumentos formalizadores daquela (artigo 11, II, *b*, LGPD).

O artigo 23, da LGPD, por seu turno, menciona os requisitos a serem observados para tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do artigo 1º, da Lei 12.527/2011 (Lei de Acesso à informação).

---

[57] *Ibid*. p. 9.
[58] *Ibid*. p.9.

Podem realizar o tratamento de dados nesta modalidade aquelas pessoas indicadas no diploma complementar. São elas: órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo Cortes de Contas, Judiciário e Ministério Público; autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios. Destaque-se que as empresas públicas e sociedades de economia mista que atuam em regime de concorrência, e exploram diretamente atividade econômica terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares (artigo 24, LGPD); terão, por outro lado, o mesmo tratamento dos órgãos e entidades do Poder Público quando estiverem operacionalizando políticas públicas e no âmbito de execução destas.

Segundo o Guia da ANPD, o conceito abrange todas as entidades que estejam no exercício de funções administrativas, não no exercício de suas funções típicas (ressalvado o Poder Executivo). Conforme se esclarece, todos os órgãos e entidades mencionados possuem funções típicas, tais como a de legislar ou de julgar, e funções atípicas, entre as quais a de administração e gerenciamento, espaço acobertado pela autorização legislativa de tratamento de dados. Assim, a eventual assinatura de convênios ou acordos de cooperação com outros órgãos ou entidades visando ao atendimento de finalidade pública ou de interesse público, estará inserida na base legal indicada.

Relevante, ainda, cuidar-se da definição de política pública, termo não definido pela LGPD, mas com indicativo de conteúdo revelado pela Autoridade Nacional de Proteção de Dados. A ANPD propõe uma análise com base na definição usual do termo, composto por dois elementos centrais: um de natureza formal e um de fundo substancial.

No campo formal, exige-se a presença de um instrumento que constitua a política pública, o qual pode vir sob a forma de lei, regulamento, contrato, convênio ou outros instrumentos congêneres. Assim, inclui-se na previsão não apenas atos normativos, mas também ajustes contratuais. Lembre-se, contudo, que estes últimos não serão aceitos quando o tratamento envolver dados sensíveis do titular, diante da proibição do artigo 11, já mencionado.

Referidos instrumentos devem, como regra, trazer informações sobre os sujeitos envolvidos, as ações a serem praticadas, o programa de execução, instrumentos e meios de ação, prazos etc., revelando-se informações que permitam a análise do atendimento das normas aplicáveis para o tratamento de dados, em especial finalidade, necessidade, adequação e transparência.

Quanto ao aspecto material, a política pública deve envolver a definição de um "programa ou ação governamental específico"[59] a ser executado por um órgão ou entidade públicos. Assim, deve, inicialmente, envolver os sujeitos já indicados como pertencentes à administração pública, além de ter como objeto uma ação ou projeto governamental para atingimento de uma finalidade específica. A ANPD, no Guia Orientativo, propõe que a expressão seja interpretada de forma ampla, de modo a incluir todas as ações e programas desenvolvidos pelo Estado para concretizar direitos e para atingir os fins que lhe são impostos.

É importante que se diga que a previsão normativa dessa base legal é bastante elástica, conferindo grande margem de discricionariedade para a atuação estatal. Esta flexibilidade foi alcançada, porém, após longo processo de debate e modificação da proposta de texto original da LGPD, como pode ser observado no quadro a seguir:

Anteprojeto da Lei Geral de Proteção de dados Pessoais apresentado pelo Ministério da Justiça para consulta pública em 2010:	**Texto do Projeto de Lei 5276/2016, enviado à Câmara dos Deputados:**	**Texto final da LGPD**
Art. 13. O consentimento será dispensado quando o tratamento: (...) III – for necessário para o exercício de funções próprias dos poderes do Estado.	Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos.	Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei.

Considera-se, portanto, subsumida às normas de adequado tratamento de dados as ações ou os projetos previstos em ato formal expedido pelo Poder Público no exercício da

[59] *Ibid*. p.12.

função administrativa, para atingimento de finalidades públicas ou execução de políticas públicas, dentro da ampla margem da LGPD.

3.3.5 Segurança pública, defesa nacional, segurança do Estado, investigação e repressão de infrações penais

Extrai-se do artigo 4º, III, da LGPD, que o Poder Público poderá, ainda, realizar tratamento de dados pessoais para fins de segurança pública, defesa nacional, segurança do Estado, investigação e repressão de infrações penais. Essa hipótese não está sujeita, porém, às regras ordinárias da Lei Geral de Proteção de Dados, devendo ser regulamentada por meio de legislação específica. A norma a ser criada deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, devendo respeitar, ainda, os princípios gerais expostos na LGPD, os direitos do titular dos dados e o devido processo legal. Eis o mandamento do §1º, do artigo 4º, da LGPD.

Visando a dar concretude ao preceito, foi enviado para a Câmara dos Deputados projeto de lei para regulamentação da chamada Lei Geral de Proteção de Dados Penal para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública e de investigação e repressão de infrações penais (LGPD Penal), o qual agora tramita como PL nº 1515/2022, de autoria do Deputado Coronel Armando.

O anteprojeto de lei foi realizado por uma comissão de juristas liderada pelo então Ministro do Superior Tribunal de Justiça, Nefi Cordeiro. A comissão foi instituída em novembro de 2019 pelo presidente da Câmara dos Deputados com quinze membros, os quais concluíram os trabalhos por meio da entrega do anteprojeto em 05 de novembro de 2020.

O próprio texto apresentado indica os objetivos da regulamentação: assegurar a eficiência das ações dos órgãos responsáveis pelas atividades indicadas na Lei, possibilitar de maneira segura e adequada o compartilhamento de dados pessoais entre autoridades competentes pelas mesmas atividades e proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural.

O projeto traz também em seu texto a base legal de cada uma das modalidades de ação estatal descritas, as quais não diferem em grande medida daquelas já fixadas na LGPD: cumprimento de obrigação legal da autoridade competente, execução de políticas públicas e proteção da vida ou da incolumidade física do titular dos dados ou de terceiro, contra perigo certo ou iminente.

O acesso aos dados e a facilidade de seu compartilhamento mostram-se mais ou menos flexíveis conforme as diferentes categorias de titulares de dados, que variam desde aqueles sobre os quais recaem apenas indícios de prática de infrações penais até os que já estão processados ou cumprindo penas em razão de condenação pela incidência criminosa. Essa gradação varia, portanto, conforme mais frágil se torna o princípio da presunção de inocência. A norma não deixa claro, porém, se a flexibilização em relação ao tratamento de dados de quem já teve condenação ou é sujeito à investigação ocorre de maneira geral ou apenas no caso concreto em que inserido o titular.

Os princípios aplicáveis na atividade de tratamento e compartilhamento de dados pessoais nas hipóteses em que elenca são, outrossim, assemelhados àqueles constantes na LGPD: finalidade, necessidade, adequação, segurança da informação, prevenção, qualidade dos dados e auditabilidade. A estes, somam-se outros específicos: licitude e supremacia do interesse público, os quais são extraídos de princípios gerais aplicados à Administração Pública expostos em linhas anteriores. Cuida a licitude da atuação dentro das bases legais fixadas; a supremacia do interesse público, por sua vez, determina que, em caso de conflito, deve ser dada a primazia ao interesse público sobre o particular.

É digna de nota, ainda, regra que prevê a necessidade de distinção entre dados pessoais baseados em fatos de dados pessoais baseados em avaliações pessoais (artigo 6º). O PL mostra tolerância com avaliações subjetivas, as quais não estão sujeitas a qualquer parametrização a fim de evitar erros, vieses e, consequentemente, prejuízo aos direitos e garantias dos titulares dos dados. A única ressalva diz com a possibilidade de retificação ou apagamento dos dados tratados de forma inexata ou ilícita, conforme previsão do §1º respectivo. A retificação, porém, não poderá ocorrer se as informações coletadas decorrerem de percepções pessoais colhidas por agentes de autoridades competentes e testemunhas (artigo 27).

De grande repercussão, ainda, é a ampla possibilidade de compartilhamento dos dados entre órgãos e entidades federais, distritais, estaduais e municipais ou entre órgãos incumbidos das atividades mencionadas no título do PL: segurança de Estado, defesa nacional, segurança pública e investigação e repressão de infrações penais.

Como garantia importante para o administrado, o Projeto também contempla vedação a tomada de decisão baseada exclusivamente em tratamento automatizado que possam levar a efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa. Das decisões automatizadas não podem decorrer, ainda, quaisquer medidas coercitivas ou restritivas de direitos, sendo exigida a auditabilidade para aferição da precisão e da acurácia das decisões sugeridas.

O Projeto da LGPD Penal absorve diversos direcionamentos postos na legislação europeia a respeito do tema e é importante instrumento para proteção de direitos e garantias individuais frente ao poder de vigilância do Estado. Enquanto não aprovado o texto, valerão normas genéricas da LGPD e legislação específica já existente voltada ao disciplinamento da ação do Estado na segurança pública, as quais serão em parte a seguir analisadas.

Uma das questões fundamentais diz respeito não apenas aos limites para coleta e tratamento de dados pessoais, mas igualmente às regras para compartilhamento daquelas informações obtidas pelos diversos órgãos públicos para alcance dos fins do Estado. Importantes, portanto, as considerações do item seguinte.

3.4. Uso secundário e compartilhamento de dados pelo Poder Público

É frequente a demanda por compartilhamento de bases de dados entre órgãos e entidades do Poder Público. A partilha de informações é impulsionada pelo desejo de desburocratização, de simplificação e economia de recursos no ambiente público, evitando o custo econômico e social, tanto para o erário quanto para o cidadão, da coleta de informações que já estariam armazenadas em bases de dados de organismos congêneres.

Ocorre que o compartilhamento pode afastar o uso dos dados da finalidade inicial para a qual foram recolhidos, trazendo complicações no atendimento de diversos princípios que circundam a proteção de dados, nomeadamente finalidade, necessidade e adequação. Tendo em vista, porém, o amplo benefício que pode ser gerado na entrega de políticas públicas, serviços públicos e ações de interesse coletivo, insta delimitar-se em que medida pode ser realizado o compartilhamento de dados custodiados pelo Estado sem malferimento dos princípios da proteção de dados e dos direitos dos titulares.

A Lei Geral de Proteção de Dados não desconheceu a importância do tema, embora o tenha regulamentado de forma pouco sistemática. Com vistas a dar concretude e pragmatismo ao compartilhamento, previu, no artigo 25, que os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado. Esses dados poderão ser utilizados para a execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública e a disseminação e acesso das informações pelo público em geral.

No mesmo sentido caminha a Lei nº 14.129, de 29 de março de 2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública. Nos termos da Lei, esta seria alcançada especialmente por meio da desburocratização,

da inovação, da transformação digital e da participação do cidadão. A Lei prevê a atuação integrada entre os órgãos e as entidades envolvidos na prestação e no controle dos serviços públicos, com o compartilhamento de dados pessoais quando for indispensável para a prestação do serviço, nos termos da LGPD.

Mais adiante, a Lei do Governo Digital ainda determina a instituição de mecanismo de interoperabilidade para criação de meios unificados de identificação do cidadão para a prestação de serviços públicos, para realizar tratamento de informações das bases de dados e para facilitar o intercâmbio de informações entre órgãos do governo. Busca-se, com isso, aprimorar a gestão de políticas públicas e aumentar a confiabilidade dos cadastros de cidadãos existentes na administração pública.

A legislação federal possui, portanto, um plexo de diplomas que visam a permitir a interoperabilidade de bancos de dados de diversos órgãos e entidades com vistas ao melhor atendimento do interesse público, sempre com o desafio de fazê-lo atendendo aos direitos fundamentais e às normas legais de proteção de dados pessoais.

No artigo 5º, XVI, a LGPD cuida dos formatos em que pode ocorrer a interconexão e o tratamento compartilhado de dados, conforme os sujeitos envolvidos. Nesse sentido, define que o compartilhamento pode ser feito (i) entre entidades públicas, no cumprimento de suas obrigações legais; (ii) entre entes públicos e privados, mediante autorização específica ou (iii) entre órgãos privados.

O compartilhamento realizado entre entidades públicas é disciplinado no artigo 26 da LGPD. Determina-se que devem ser atendidas as finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades da Administração, respeitados os princípios de proteção de dados elencados na Lei. Observa-se, pois, que há exigência de que a base legal seja atendida, devendo o receptor dos dados indicar com base em qual fundamento legal justifica o recebimento e o tratamento dos dados solicitados dentre aqueles indicados nos artigos 7º, 11 e 23 da LGPD. Há, ainda, importante ressalva quanto à plena aplicação dos princípios que regem a Lei, devendo ser atendidos a finalidade, necessidade, adequação e transparência, segurança e prevenção em cada etapa do uso dos dados.

A segunda hipótese cuida do compartilhamento público-privado, que pode acontecer: (i) em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado (art. 26, §1º, I); (ii) nos casos em que os dados forem acessíveis publicamente (art. 26, §1º, III); (iii) quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres (art. 26, §1º, IV) e (iv) na hipótese de a transferência dos dados objetivar

exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades (art. 26, §1º, V).

Das hipóteses expostas, percebe-se grande restrição à possibilidade de uso dos dados pelo ente privado que os acessa quando não forem acessíveis ao público. A delimitação de uso exclusivo e vedação expressa de tratamento para finalidade diversa da que justifica o compartilhamento buscam garantir segurança e integridade do titular de dados, que os vê acessados fora da esfera pública. Com vistas ao aumento da segurança, exige-se, ainda, que a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado sejam informados à autoridade nacional.

O consentimento do titular também é exigido na norma, podendo ser dispensado, porém, nas exceções ao consentimento ao próprio ente público. Observa-se, contudo, que o consentimento não costuma ser base legal para atuação dos órgãos e entidades da Administração, que normalmente utilizam o poder de império e sobrepõem-se aos interesses particulares, em relação de significativa assimetria. Assim, não será comum o trânsito dentro dessa base legal.

Esses dispositivos devem ser sempre lidos em harmonia com as demais disposições da LGPD, as principiológicas e as que delimitam as bases legais para atuação do Poder Público.

Importante, nesse tema, o princípio da transparência, que garante aos titulares dos dados, também na etapa de compartilhamento, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, incluídos aqui aqueles que recebem os dados por meio de compartilhamento. Essa também a previsão do artigo 9º, V, que garante o livre acesso do titular dos dados a informações acerca do uso compartilhado destes pelo controlador e à finalidade àquele subjacente.

Outrossim, a invocação dos dispositivos que permitem o compartilhamento de dados deve vir associada à indicação da base legal em que se sustenta a possibilidade de tratamento daqueles pelo receptor, respeitando-se a delimitação posta nos artigos 7º, 11 e 23 da LGPD.

Essa atividade de compartilhamento já foi impulsionada no Estado brasileiro por meio de diversas iniciativas normativas. Exemplificativamente, o Decreto 9.094, de 17 de julho de 2017, dispõe, entre outras medidas, sobre simplificação do atendimento prestado aos usuários de serviços públicos. Com esse fim, disciplina o compartilhamento de documentos, atestados, certidões que constem em bases de dados oficiais da administração pública federal para todos os órgãos e entidades do Poder Executivo federal. A norma expressa o

encaminhamento da solicitação aos órgãos detentores das informações vedando nova exigência de entrega aos usuários dos serviços públicos.

Antes deste, outro decreto já havia sido editado para disciplinar o compartilhamento de bases de dados na administração pública federal – Decreto 8.789, de 29 de junho de 2016 – o qual foi substituído pelo Decreto 10.046, de 09 de outubro de 2019, que dispôs sobre a governança no compartilhamento de dados no âmbito da administração pública federal e ampliou ainda mais a possibilidade de compartilhamento de dados. Referido Decreto instituiu, ainda, o chamado Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

Essas iniciativas de amplo compartilhamento entre órgãos e entidades da Administração Pública não passam imunes a críticas doutrinárias e a controle jurisprudencial, que procura traçar diretrizes, fixar limites e reconhecer salvaguardas institucionais para o compartilhamento de informações.

Forte é a resistência ao que se denomina "unidade informacional", na qual os dados podem circular de maneira alargada, com manifestos prejuízos ao regime constitucional de proteção de dados pessoais.

Nesse contexto, o mencionado Decreto nº 10.046, de 09 de outubro de 2019, teve sua validade discutida em duas ações judiciais – Ação Direta de Inconstitucionalidade nº 6.649 e Arguição de Descumprimento de Preceito Fundamental nº 695, julgadas em definitivo em junho de 2023. No julgamento, foram traçados alguns parâmetros para a interpretação conforme da norma e subtração de seu campo semântico de aplicações ou interpretações que conflitem com o direito autônomo à proteção de dados pessoais. Dada a importância do precedente fixado no julgamento referido, importante a análise dos principais fundamentos da decisão prolatada.

Veja-se resumo da ADI nº 6.649:

> O Conselho Federal da Ordem dos Advogados do Brasil ajuizou ação direta de inconstitucionalidade, com pedido de medida cautelar, contra o Decreto 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.
>
> Em suas razões, impugnou o regulamento por afronta à dignidade da pessoa humana; à inviolabilidade da intimidade, da privacidade, da vida privada, da honra e da imagem das pessoas; ao sigilo dos dados; e à garantia do *habeas data* enquanto instrumento de tutela material do direito à autodeterminação informativa.
>
> Alega que o Decreto 10.046/2019 desrespeita princípios básicos da Lei Geral de Proteção de Dados Pessoais, pois permite o compartilhamento amplo e irrestrito de informações entre os órgãos públicos federais, sem a devida indicação de protocolos de ação e independentemente da precisa identificação dos agentes públicos envolvidos no tratamento.
>
> Ademais, frustra-se o ordenamento jurídico pela criação do Cadastro Base do Cidadão e do Comitê Central de Governança de Dados, que desrespeitaria as diretrizes da LGPD, institucionalizando base de dados unificada que poderá ser livremente compartilhada pelos órgãos públicos federais, além de acarretar riscos de vazamentos e de incidentes de segurança.

> Por fim, afirma que a ampliação da base de dados dos cidadãos brasileiros, mediante utilização de conceitos vagos e genéricos, potencializa a capacidade de controle político sobre a população, em descompasso com o disposto na LGPD e na Constituição Federal.

O Decreto nº 10.046/2019 previa, em sua redação originária, ampla possibilidade de compartilhamento de informações do Estado, cujos mecanismos deveriam ser desenvolvidos de forma a facilitar a execução de políticas públicas orientadas por dados nos órgãos e entidades da administração pública federal. Ademais, no cadastro base, diversos dados pessoais seriam coletados, servindo como central de informações sobre os cidadãos para os órgãos e entidades do Poder Executivo Federal.

O Ministro relator Gilmar Mendes fez o voto condutor, o qual determinou diversos direcionamentos na interpretação e aplicação do diploma guerreado a fim de adequá-lo aos princípios constitucionais e normas gerais de proteção de dados vigentes.

Incialmente, fixou-se que o compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública somente pode ocorrer sob as seguintes condições: (i) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei nº 13.709/2018); (ii) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); (iii) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.

O compartilhamento, nos termos da decisão colegiada, deve seguir rigorosa observância ao artigo 23, I, da LGPD que cuida da publicidade ampla e irrestrita na atividade de tratamento e compartilhamento de dados. O Tribunal ressaltou, ainda, a responsabilização em caso de transgressão da norma e das diretrizes fixadas, inclusive com possibilidade de responsabilidade por ato de improbidade administrativa do agente estatal que deixar de atender ao comando legislativo.

Quanto ao Cadastro Base do Cidadão, seu acesso por órgãos e entidades governamentais fica condicionado ao atendimento integral das diretrizes acima arroladas.

O Comitê Central de Governança também foi avaliado na decisão. Nos termos do julgado, este deve realizar minuciosa atividade de controle das ações, entre as quais: "3.1. prever mecanismos rigorosos de controle de acesso ao Cadastro Base do Cidadão, o qual será limitado a órgãos e entidades que comprovarem real necessidade de acesso aos dados pessoais nele reunidos. Nesse sentido, a permissão de acesso somente poderá ser concedida para o

alcance de propósitos legítimos, específicos e explícitos, sendo limitada a informações que sejam indispensáveis ao atendimento do interesse público, nos termos do art. 7º, inciso III, e art. 23, caput e inciso I, da Lei nº 13.709/2018; 3.2. justificar de maneira formal, prévia e minudentemente, à luz dos postulados da proporcionalidade, da razoabilidade e dos princípios gerais de proteção da LGPD, tanto a necessidade de inclusão de novos dados pessoais na base integradora (art. 21, inciso VII) como a escolha das bases temáticas que comporão o Cadastro Base do Cidadão (art. 21, inciso VIII); 3.3. instituir medidas de segurança compatíveis com os princípios de proteção da LGPD, em especial a criação de sistema eletrônico de registro de acesso, para efeito de responsabilização em caso de abuso."

O Supremo Tribunal Federal demonstrou, ainda, preocupação quanto à conformação do Comitê Central de Governança de Dados. O Tribunal declarou a inconstitucionalidade do artigo do Decreto que fixava sua composição, a fim de que outra fosse realizada garantindo ao órgão "um perfil independente e plural, aberto à participação efetiva de representantes de outras instituições democráticas". Ademais, determinou a necessidade de fixação de garantias de atuação livre de pressões para seus integrantes.

Por fim, ressaltou o STF a possibilidade de responsabilização civil do Estado em caso de desrespeito às normas e parâmetros fixados, sem prejuízo de ação regressiva contra os servidores e agentes responsáveis pela infração.

A ADI em lume foi julgada conjuntamente com ADPF nº 695, que traz relevante caso envolvendo órgão de inteligência do Estado e, portanto, entidade cuja ação encontra-se fora da esfera de aplicação direta da LGPD, nos termos da exceção posta artigo 4º, III. Eis o caso:

> "Em 6 de junho de 2020, o site jornalístico "The Intercept" noticiou que ABIN e SERPRO estabeleceram tratativas visando ao compartilhamento de dados dos mais de 76 milhões de brasileiros que possuem a Carteira Nacional de Habilitação – CNH (o equivalente a 36% da população total do país), originalmente coletados e armazenados pelo do Departamento Nacional de Trânsito (DENATRAN)"
>
> Na ADPF 695, o Partido Socialista Brasileiro (PSB) requereu a invalidação do ato do poder Público, editado com lastro normativo no Decreto 10.046, de 9 de outubro de 2019. Sustentou, em síntese, que a "transferência massiva e indiscriminada dos dados pessoais de todos os portadores de CNH no país para a Agência Brasileira de Inteligência" violava os direitos fundamentais à privacidade, à proteção de dados pessoais e à autodeterminação informativa.
>
> Às vésperas da sessão de julgamento, a AGU peticionou nos autos informando a revogação de Termo de Autorização concedido à ABIN para acesso à base dados da Carteira Nacional de Habilitação e requereu que fosse declarada a perda de objeto da ADPF.
>
> O Ministro relator reconheceu a persistência do interesse na análise da matéria, dado que o ato do Poder Público impugnado na ADPF revelava um quadro de insegurança mais geral, o qual deveria ser enfrentado.

Na ação, o requerente ressaltou que a ABIN possuía poderes para requisitar informações de quaisquer órgãos componentes do Sistema Brasileiro de Inteligência, inclusive dados de investigações sigilosas, relatórios do COAF, dados de sigilo telefônico, quebra de sigilo fiscal, entre ouras informações sensíveis e sigilosas. Argumentou que o compartilhamento de informações com a ABIN não deveria ser automático – mas acompanhado de motivação – e que sua ação ocorria em dissonância com direitos fundamentais, tal como o sigilo protegido por reserva de jurisdição (art. 5º, XII, CF) e o respeito à intimidade e vida privada (art. 5º, X, CF).

No curso da ação, o partido Rede Sustentabilidade apresentou petição mencionando haver informações de que a ABIN teria confeccionado relatórios para auxiliar a defesa de Flávio Bolsonaro, senador e filho do então presidente Jair Bolsonaro, em investigações criminais em curso. Solicitaram ao STF que proibisse SERPRO e Receita Federal de fornecer qualquer informação sobre o "Caso Queiroz", em que investigado suposto esquema de "rachadinhas" envolvendo o senador. Requereram, ainda, que a ABIN justificasse os fundamentos dos relatórios produzidos e disponibilizasse processos, procedimentos e registros de acesso que envolvam o "caso Queiroz".

Adotadas algumas medidas administrativas junto à Procuradoria Geral da República, e tendo em vista a discussão do tema em ação própria, a Ministra relatora, Carmen Lúcia, não aprofundou o tema no julgamento do mérito da ação.

Os Ministros julgaram a questão para dar interpretação conforme ao artigo 4º, da Lei nº 9.883, de 07 de dezembro de 1999, que institui o Sistema Brasileiro de Inteligência e cria a Agência Brasileira de Inteligência – ABIN. Veja-se o conteúdo da conclusão:

> "(...) acordam os Ministros do Supremo Tribunal Federal, em Sessão Virtual do Plenário, na conformidade da ata de julgamento, por unanimidade, em conhecer parcialmente da ação direta de inconstitucionalidade e dar interpretação conforme ao parágrafo único do art. 4º da Lei n. 9.883/1999 para estabelecer que: a) os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados; b) toda e qualquer decisão de fornecimento desses dados deverá ser devida e formalmente motivada para eventual controle de legalidade pelo Poder Judiciário; c) mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo, em razão daquela limitação, decorrente do respeito aos direitos fundamentais; d) nas hipóteses cabíveis de fornecimento de informações e dados à ABIN, são imprescindíveis procedimento formalmente instaurado e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização em caso de eventual omissão, desvio ou abuso."

Na decisão, o Supremo Tribunal Federal incorporou diversos elementos que passaram a constar no Projeto de LGPD Penal, tais como necessidade de motivação no tratamento e compartilhamento de dados (art. 2º,V), respeito a reserva judicial e registro minucioso de acesso (seção III).

As preocupações exaradas na oportunidade do julgamento acabaram sendo reforçadas por notícias posteriores, quando, em outubro de 2023, vieram à tona informações de uso pela Agência Brasileira de Inteligência de ferramentas que monitoraram a localização de cidadãos por meio do celular durante o governo de Jair Bolsonaro. Segundo apuração jornalística[60], o sistema para monitoramento foi acionado mais de 30 mil vezes; desse montante, 2.200 usos foram relacionados a políticos, jornalistas, advogados e adversários do governo federal.

O caso em referência demonstra os riscos associados à vigilância estatal e o poder que a esta é conferido quando não respeitados os limites do regime constitucional e das normas do ordenamento pátrio. Opressão, controle, silenciamento de adversários e o rompimento do regime democrático e da ordem constitucional são consequências marcantes da prática, como será aprofundado a seguir.

Em momento anterior, o Supremo Tribunal Federal já havia estabelecido outros limites para o fluxo informacional entre órgãos e entidades da administração pública. Menciona-se, por citado no voto do Ministro Gilmar Mendes na ADI nº 6.649, o Mandado de Segurança nº 36.150 MC, na qual foi cassada determinação do Tribunal de Contas da União (TCU) que ordenara ao Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP a entrega de dados individualizados do Censo Escolar e do ENEM, com o fim de realizar auditoria do Programa Bolsa Família, avaliando sua efetividade. Argumentou o TCU que com os dados seria possível apurar se jovens integrantes de famílias beneficiárias acessavam o mercado formal de trabalho. O impetrante argumentou, em contrário, que a entrega das informações quebraria a confiança daqueles que fornecem os dados, colocando em risco sua capacidade de pesquisa e monitoramento das políticas públicas de educação e redundaria em afronta a direitos de terceiros que têm garantia de sigilo sobre seus dados pessoais.

Na decisão do MS, o relator, ministro Luís Roberto Barroso, aprofundou a noção de finalidade como princípio norteador da atividade de tratamento e compartilhamento de

[60] O GLOBO. **Caso ABIN**: operação para investigar programa espião afasta número três da agência e prende dois servidores. Dispnível em: https://oglobo.globo.com/politica/noticia/2023/10/20/caso-da-abin-pf-faz-operacao-para-investigar-programa-secreto-que-monitorou-localizacao-de-pessoas-por-meio-do-celular.ghtml. Acesso em 18 de novembro de 2023.

dados, apontando o risco de descolamento da autorização concedida pelos titulares dos dados pessoais no ato da coleta. Para o Ministro, a transmissão dos dados para finalidade diversa da que motivou a colheita inicial subverteria a autorização daqueles que concordaram em prestar as declarações e colocaria em risco a capacidade do INEP de pesquisar e monitorar políticas públicas, dada a quebra da confiança e possível comprometimento das declarações em consultas futuras.

Em conclusão, é importante que se perceba que as normas de compartilhamento de dados nos diversos diplomas normativos vêm com o objetivo de permitir um grau ótimo de atendimento do interesse público por meio das atividades desenvolvidas pelos diversos órgãos e entidades da Administração. É indubitável que a utilização de dados para direcionamento de políticas públicas, execução de serviços e planejamento de programas de governo são de extrema valia, não sendo razoável que este imenso potencial proporcionado pela tecnologia seja afastado na tomada de decisões.

A Constituição Federal mesma impõe ao Estado que desenvolva a atividade administrativa do modo mais eficiente, econômico e adequado ao interesse público, o que pode ser alcançado por meio do uso das modernas tecnologias e ferramentas digitais.

Diversos exemplos positivos podem ser dados para demonstrar que a tecnologia e suas ferramentas são grandes aliadas no atendimento do interesse público.

Desenvolvida pelo Serpro para o Ministério da Economia, a Prova de Vida Digital foi inovação que trouxe imenso benefício para aposentados e pensionistas no Brasil. A iniciativa foi lançada em meio à pandemia de Covid-19, quando o Governo Federal disponibilizou a ferramenta, que considera atendida a exigência de prova de vida mediante reconhecimento facial de quem possui Carteira Nacional de Habilitação ou biometria cadastrada no Tribunal Superior Eleitoral e a comprova por meio de aplicativo disponibilizado pelo Poder Público. A iniciativa foi premiada no 26º Concurso Inovação no Setor Público, da Escola Nacional de Administração Pública (Enap).

Em outra parceria entre Serpro e Ministério da Economia, foi desenvolvida a "Recomendação de serviços" que usa inteligência artificial no endereço eletrônico Gov.br, onde diversas informações e certidões podem ser facilmente acessadas pelos meios virtuais.

Assim, a tecnologia mostra-se grande aliada na facilitação de acesso a serviços e no fornecimento de informações que auxiliam o Poder Público na tomada de decisões e no gerenciamento da coisa pública, de forma que o uso de ferramentas de tecnologia deve ser não desestimulado, mas explorado positivamente no atendimento do interesse público e com respeito aos direitos fundamentais.

A busca desse quadro de eficiência somente não pode afastar o Estado do necessário atendimento aos preceitos éticos que informam o ordenamento jurídico, exigindo responsabilidade no tratamento dos dados pessoais dos cidadãos.

4. TRATAMENTO DE DADOS PESSOAIS PARA FINS DE SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL

Muitos são os desafios postos ao Estado no campo da segurança pública com vistas à proteção da coletividade contra o terrorismo, a delinquência e a violência, que exigem um aperfeiçoamento das formas de combate ao crime.

Nessa conjuntura, as ferramentas tecnológicas podem ser grandes aliadas e já são hoje efetivamente utilizadas para prevenção de delitos e investigação criminal, o que tem alterado a dinâmica de todo o sistema de segurança pública.

A utilização de câmeras de monitoramento, de sistemas de análise de imagens e de reconhecimento facial, policiamento preditivo por meio de tratamento de dados criminais passados são realidade recorrente. Esses instrumentos trazem indiscutível resultado positivo, mas demonstram, na mesma medida, os grandes desafios para uso da tecnologia sem perdas significativas dos cidadãos em seus direitos e garantias individuais.

Dando início à problematização da questão referente ao uso da tecnologia pelo Estado, tenham-se presentes os exemplos a seguir.

Mayer-Schonberger e Cukier[61] relembram caso ocorrido nos Estados Unidos que demonstram o potencial do uso dos dados na elaboração de políticas públicas adequadas, mesmo quando estes são coletados e tratados sem consentimento.

Em 2009, um novo vírus de gripe foi descoberto, combinando elementos da gripe aviária e da gripe suína – H1N1. O vírus alastrou-se rapidamente e as autoridades sanitárias temiam um surto equivalente ao de grandes epidemias que custaram a vida de milhões de pessoas em todo o globo. Para controle da disseminação do vírus, autoridades determinaram que novos casos deveriam ser reportados pelas unidades de saúde, a fim de que se controlasse a forma de disseminação, antecipando-se como poderia ser o alastramento melhor combatido.

Ocorre que a doença possui tempo de incubação, além de existir um considerável lapso até o momento em que, depois de aparecidos os sintomas, os indivíduos procuram auxílio profissional. Ademais, as próprias unidades médicas retardavam o envio de informações, de forma que as autoridades governamentais somente tinham um mapeamento adequado da situação com uma ou duas semanas de atraso.

---

[61] MAYER-SCHONBERGER, Viktor e Cukier, Kenneth. **Big Data**: A Revolution that Will Transform How We Live, Work and Think. Nova Iorque: Houghton Mifflin Harcourt Publishing Company, 2013. *E-book*.

Algumas semanas antes de o vírus chegar às manchetes de jornais, engenheiros da gigante Google publicaram artigo na revista *Nature* em que reportaram como poderiam prever a propagação da gripe de inverno nos Estados Unidos por meio da análise do que as pessoas buscavam em pesquisas na Internet.

A empresa checava as principais ocorrências de pesquisa, em termos como "quais os sintomas da gripe" ou "remédios para tosse e febre". Comparando as informações de pesquisa coletadas no passado com dados empós divulgados por agências oficiais, conseguiram fazer um relatório mais ou menos preciso de como ocorreu o alastramento do vírus. O software encontrou uma combinação de 45 termos de pesquisa que, quando usados em modelo matemático, mostraram forte correlação da sua previsão com os números oficiais de todo o país tempos depois.

Quando o vírus H1N1 apareceu em 2009, o sistema fornecido pelo Google proveu o governo de estatísticas que demonstravam o alastramento do vírus com uso do mesmo modelo anteriormente testado. O acesso instantâneo aos dados de pesquisa e a consequente antecipação dos locais de circulação do vírus permitiram a construção, pelas autoridades governamentais, de estratégias mais efetivas de enfrentamento da sua disseminação.

O exemplo acima demonstra como o uso da tecnologia pode impactar positivamente a política estatal.

Usos menos nobres da tecnologia também são experenciados, no entanto. Na China, cidadãos são monitorados e pontuados por comportamentos a partir de um rígido esquema de vigilância montado pelo governo. Segundo informações trazidas por Chin e Lin[62], no início dos anos 2020, perto de 350 milhões de câmeras registravam o movimento nas ruas chinesas, em praças, estações de metrô e no entorno de prédios comerciais. Mais de 840 milhões de *smatphones* enviavam fluxos constantes de dados de localização para operadoras de telecomunicações. Os sistemas de pagamento móvel registravam milhões de operações por dia em bancos de dados.

Esclarecem os autores que a vigilância em massa na China tornou-se quase instantânea, de forma que cada traço do comportamento do indivíduo é analisado para fazer um retrato que cada vez mais vem servindo ao controle e abuso daqueles que detêm os dados.

Essa política de controle traz profundas implicações na sociedade de um dos países mais populosos do mundo. Defende seu governo que, com esse modelo de vigilância e de informações, pode-se prever os problemas sociais antes que estes ocorram para dar-lhes

[62] CHIN, Josh e LIN, Liza. **Surveillance State**: inside China''s quest to lauch a New era of Social Control. New York: St. Martin's Press, 2022, p. 7.

resposta adequada, aumentando a eficiência do governo; contudo, observa-se seu manuseio também para reprimir dissidentes que possam pôr em risco a organização política vigente.

Reporta-se que, duramente a pandemia de Covid-19, quando era esperado um declínio de confiança no governo em razão do surgimento e disseminação do vírus no país, a confiança no sistema subiu a níveis maiores. Enquanto em outros países o número de mortes crescia, restando clara a ausência de controle adequado do alastramento da doença, a China conseguiu criar política eficiente de combate ao alastramento dos vírus e tratamento imediato dos infectados, de forma que cresceu, no país, a confiança no Partido e no seu modelo de vigilância estatal generalizada.

Quando confrontados por pedidos de proteção de privacidade, os autores destacam, ainda, abordagem inovadora dos líderes chineses. Estes cooptaram e redefiniram a noção de privacidade: esta não é mais um direito individual abstrato; em vez disso, é identificada como um conceito coletivo de segurança nacional[63]. Por meio dessa abordagem, a renúncia a graus mais elevados de privacidade traria benefícios a todo o corpo coletivo, garantindo o exercício de uma atividade estatal ótima no cuidado com o país e seus habitantes.

Apesar do discurso governamental e das vantagens conferidas pelo sistema de vigilância, muitos são os protestos realizados contra o governo e o excesso de controle sobre a vida dos cidadãos. Como forma de burlar o elaborado sistema de vigilância, cidadãos chineses usam os mais diversos artifícios: uso de ponteiros de lasers para evitar o reconhecimento facial por câmeras, uso de máscaras, óculos, capacetes; pagamento em dinheiro para ingresso em transportes públicos, evitando o uso de cartões que registram os deslocamentos efetuados; troca de mensagens por aplicativos com segurança de criptografia e comunicação por sistemas de *bluetooth* e *Apple AirDrop*, entre outros.

O formato chinês demanda atenção. Outros países no mundo têm demonstrado interesse nos sistemas de vigilância construídos ali, concebidos para aperfeiçoar e fortalecer o pleno controle estatal. Como destacado por Lin, a lista inclui autocracias como Arábia Saudita e regimes híbridos como Uganda, mas também governos de democracias avançadas como França e Alemanha.

No Brasil, sistemas análogos começaram a ser utilizados em algumas cidades, gerando reações e discussões em torno do respeito a direitos fundamentais constitucionalmente assegurados.

---

[63] *Op. cit.*, p. 210.

Neste trabalho, dois projetos que se encontram em curso no Brasil serão analisados a fim de que se problematize, a partir dos casos concretos, vantagens e riscos advindos do tratamento de dados pessoais para fins de segurança pública. Empós serão realizadas considerações e propostas de uso adequado dos instrumentos tecnológicos nesta seara, garantindo-se o respeito aos direitos humanos.

4.1 Reconhecimento facial

O uso de tecnologias de segurança cresceu rapidamente nos últimos anos. Empresas e governos desenvolvem sistemas capazes de monitorar a atividade de todos os setores da sociedade civil, com importante papel também nas forças policiais da sociedade.

No setor da segurança, a coleta e armazenamento de grande quantidade de informações é indispensável para uma atividade mais planejada e eficiente, em especial diante do incremento em criatividade e sofisticação de forças criminosas. O benefício social envolvido nessa modernização deve, porém, ser analisado ao lado do considerável potencial de desrespeito aos direitos humanos. Embora haja exemplos positivos do uso da tecnologia no combate e prevenção ao crime e na manutenção da ordem pública, diversos são os relatos de abusos por parte de autoridades e governos e casos de ataque frontal a direitos e liberdades individuais.

Tecnologia que vem sendo usada de maneira recorrente como instrumento auxiliar das forças de segurança pública é o reconhecimento facial de imagens. O reconhecimento facial "é o processamento automático de imagens digitais contendo faces para identificação ou verificação de indivíduos usando modelos de rosto"[64]. Embora esse seja um instrumento importante para prevenção e combate ao crime, consiste em um sistema de vigilância que representa sério risco à privacidade, à proteção de dados pessoais e à ordem social, como demonstrado a seguir.

O governador do Estado de São Paulo anunciou, em 2022, a entrega, no Centro de Controle Operacional do Metrô, do Sistema de Monitoramento Eletrônico (SME3), que usa software de reconhecimento facial. Este sistema mapeia os pontos do rosto – padrão facial – e compara a imagem com outras contidas em bancos de dados de interesse, a fim de atender a finalidades determinadas.

---

[64] CONSELHO DA EUROPA. **Guidelines on facial recognition**. Convenção 108. Disponível em: file:///Users/kelvianebarros/Downloads/020221GBR_Facial%20recognition%20Convention%20108.pdf . Acesso em: 20 de novembro de 2023.

Pelo projeto, 5 mil câmeras de monitoramento seriam instaladas com o objetivo, segundo o governo, de ampliar a segurança e melhorar o atendimento aos passageiros. Este informou, ainda, a retirada de câmeras analógicas, substituídas por uma nova rede com alta qualidade de imagem e significativa capacidade de armazenamento por 30 dias.

Diante do monitoramento realizado na cidade, foi ajuizada, em 03 de março de 2022, ação civil pública (processo nº 1010667-97.2022.8.26.0053)[65] pela Defensoria Pública do Estado de São Paulo, Defensoria Pública da União, Instituto Brasileiro de Defesa do Consumidor (IDEC), Intervozes – Coletivo Brasil de Comunicação Social e Artigo 19 Brasil, estas últimas associações civis sem fins lucrativos.

Na ação mencionada, alegam as requerentes que a Companhia do Metropolitano de São Paulo implementou sistema de reconhecimento facial em suas estações e faz tratamento de dados pessoais sem consentimento dos titulares. Juntam os termos do processo de licitação, o qual traz exigência, como requisitos técnicos mínimos, possibilidade de armazenamento das imagens de todos os usuários e de entrar em operação integrada com outros sistemas de monitoração eletrônica com reconhecimento facial. Aduzem, ainda, a falta de transparência e disponibilização de informações, como a finalidade do tratamento, bem como que não se adotou qualquer medida para avaliação de impacto e mitigação de riscos inerentes à tecnologia de reconhecimento facial. Assim, alegam que a medida é abusiva e desproporcional, violando direitos humanos fundamentais e dos consumidores.

Na ação são indicadas diversas normas da LGPD e da legislação consumerista que seriam violadas e o impacto desproporcional do sistema de reconhecimento facial sobre populações vulneráveis, especialmente pessoas negras e LGTQIAPN+, ofendendo o direito à igualdade e à não-discriminação insertos nas normas constitucionais e nos tratados internacionais ratificados pelo Brasil. Ressaltou-se, por fim, na ação, que os casos de discriminação algorítmica são públicos e notórios.

---

[65] TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Processo nº 1010667-97.2022.8.26.0053. Disponível em: https://esaj.tjsp.jus.br/pastadigital/abrirPastaProcessoDigital.do?nuProcesso=1010667-97.2022.8.26.0053&cdProcesso=1H000LRDS0000&instanciaProcesso=pg&cdProcessoMaster=1H000LRDS0000&cdForo=53&baseIndice=INDDS&nmAlias=PG5JM&tpOrigem=2&flOrigem=P&cdServico=190101&acessibilidade=false&ticket=MX0UHU9QI3xhDMraFDVa7so7DbaRQP0ciU9v3jTQY9D9pp%2FukCo7Z1l9%2BNqSR0VuI5%2FThVsJM6o9i6eV%2FtdI83SvYZyB2%2BPASJuRZjyEBu8toeALcKdZXL1r8EQPkYB5adoy%2BaEbZQ7R1O9EWz0XTeIp9g7JXyGkhoHtpqOc6F6vvEakJvbzSC%2F2DAcCr59VsCS5PdXV8BTflut3i%2B0vdsEcUH2JSJgWVvm%2BYFbiYpXgh4CtIi67oGqA%2BA82XXh0vZMK76ArMaSuXQ1ry%2FK167iR2IhKLQTLE0i864b0NUzXQCMH2SniRirBgTRyR39H%2FaRdkcUcz%2BjT7bwf25RWZdxTW%2Fi7MASM1NfpXkjqXctfEET417PC91lTaHIrpJ7HI65L8He%2B7fDLT5DhFHM5oEeqJWEHgfbVr%2BZSYGwtH0E0WWOCHazJdB3w5VO1viFoOQh6A%2Frf3qKPzE%2F2kAzuEeKLRdvDt52yvJTqNZXa8Qz6ZhOZwo87m2%2B%2Fk%2FNdsmQnWL4hOSPeSnnT1SKQpn3pjO6Ta5N5Pc4aoxMnyXJLnac%2BdkcVtlP%2F0zTGPAdPRPqP . Acesso em: 20 de novembro de 2023.

Em 22 de março de 2022, a juíza do caso proferiu decisão concedendo parcialmente a liminar requerida anotando questões importantes em sua fundamentação. Reportou que "não foi disponibilizada qualquer informação sobre os critérios, condições, propósitos da implementação do sistema de reconhecimento facial pela Ré". Também argumentou que não foram apresentadas informações precisas sobre o armazenamento das informações e utilização do sistema de reconhecimento facial. Reconheceu, por fim, a potencialidade de se atingir direitos fundamentais dos cidadãos com a implantação do programa, pelo que determinou o impedimento de execução do sistema de captação e tratamento de dados biométricos dos usuários do metrô para sua utilização em sistemas de reconhecimento facial, admitindo-se apenas a instalação." O processo encontra-se ainda pendente de decisão definitiva.

A instalação das câmeras rendeu também ajuizamento de ação civil pública pelo Instituto Brasileiro de Defesa do Consumidor (IDC) em face da empresa Concessionária da linha 4 do Metrô de São Paulo S.A. (Via Quatro) – Processo n°1090663-42.2018.8.26.0100[66]. Na ação, foi pedida a proibição de coleta e tratamento de imagens e dados biométricos sem prévio consentimento dos usuários das linhas de metrô operadas pela ré e o pagamento de indenização por danos coletivos.

Na sentença, destacou o juízo a evidência da captação da imagem dos usuários do transporte público para fins publicitários, já que se buscava detectar as principais características dos indivíduos e suas reações à publicidade veiculada no equipamento. Ressaltou-se, ademais, que os usuários não foram advertidos ou comunicados prévia ou posteriormente sobre a captação e uso de suas imagens. Estas foram, ainda, consideradas dados sensíveis, objeto de especial proteção pela LGPD. Nos termos da decisão, o reconhecimento facial e a detecção facial, ainda que não seja possível a identificação concreta do indivíduo, mas com acesso à sua imagem e face, esbarram no conceito de dado biométrico, legalmente considerado dado sensível.

---

[66] TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Processo n°1090663-42.2018.8.26.0100. Disponível em: https://esaj.tjsp.jus.br/pastadigital/abrirPastaProcessoDigital.do?origemDocumento=P&nuProcesso=1090663-42.2018.8.26.0100&cdProcesso=RI006J6T80000&cdForo=990&tpOrigem=2&flOrigem=S&nmAlias=SG5TJ&instanciaProcesso=SG&cdServico=190201&ticket=7upz7TIHKDNDY8NvtgdTSTbDmGLf%2FMwTyeWqRiDkbRjeBxdKdyk%2FYfy%2FDhiHd%2BmJjaqDc4rVoVv7L3tBqAQ1%2B3m0ArDoTWSHF595wJYaYlVPrlfAaS0eLZjx6Zjg5skxSSa%2FaaSwdKVZgUo3VY5mVJXav8I0xIIxnkJKU8XBAhT1vZtkMsMoTCfZC2FQSIsdpu5I0oERzG8vZnF6zX%2B3tbWf0lgJ5KvdiRmS8I88YzUgGjXBWOcKra1PGlypZB9oTh9iQscDPddDS2TXZNz5czLm72Pep3dAK0DgAz9rGVLNHMpEZaJHRiQYETkAbmTR6CDVwtspJ%2FFaedoWNQ46OQ9AKp3NtW6mRHfKnVpFvfi39HTDtgExoh4Q%2BvF9LdQP257D5bGmSmuYaFSaAJWgiuW87xlBcMrqsD575oKMQBXnbdz5JEiKkCCtRSGJ5Y6mOL48iqb2SKBpZJgIZqZhb%2Bt3XFWrDOFsI9vsDyUg4OrHKC0W5GwZpoQnmdZIOPjt1UyyzpQEZ51Aml01sUfyXjtgW0Hbn8v%2FjkonbofRGZ1%2BLAzGMSi692qsEFamJgHm. Acesso em: 20 de novembro de 2023.

Como fundamentos normativos, mencionou-se o desrespeito às normas da LGPD – art. 2º; art. 6º, I (finalidade com propósitos legítimos, específicos e explícitos); art. 11, §3° (vedação de obtenção de vantagem econômica), além dos artigos 6º, III e IV e 31 do Código de Defesa do Consumidor.

Com base nesses argumentos, proibiu-se que a requerida captasse imagens, sons ou quaisquer outros dados pessoais dos consumidores usuários através de câmeras ou outros dispositivos sem consentimento prévio do consumidor e condenou-se a requerida ao pagamento de indenização de R$100 mil reais.

No Tribunal de Justiça, a condenação foi confirmada, majorando o valor da indenização por dano moral para R$500 milhões.

A preocupação externada pelas acionantes apresenta fundamentação válida. Estudos demonstram que ferramentas de reconhecimento facial apresentam repetidamente erros e geram problemas de inclusão recorrente nos grupos indicados na ação.

Em 2020, professores, pesquisadores e estudantes fizeram um abaixo-assinado contra um sistema criado nos Estados Unidos que visava a detectar a probabilidade de pessoas cometerem crimes a partir do cruzamento de informações biométricas do rosto e fichas criminais[67]. O sistema, alimentado por dados de criminalidade racialmente carregados, levou a equivocadas identificações, diante do enviesamento de dados.

Também em 2020, o The New York Times[68] veiculou caso de erro de acusação por algoritmo. Robert Julian-Borckak Williams estava trabalhando quando recebeu telefonema do Departamento de Polícia de Detroit solicitando seu comparecimento à delegacia para ser preso. Uma hora após a ligação, ao chegar em casa, foi detido por policiais, os quais não informaram o motivo da ação.

Robert foi levado para um centro de detenção onde foram coletadas suas impressões digitais e DNA, ficando detido por toda a noite. Durante o interrogatório, foram-lhe mostradas fotografias de um homem furtando uma loja de luxo, com o qual foi confundido. Segundo o jornal, este pode ser o primeiro caso conhecido de um americano detido injustamente em razão de reconhecimento facial falho por algoritmo.

---

[67] UOL. **Racismo Calculado**: Algoritmos de plataformas e redes sociais ainda precisam de muita discussão para fugir de estereótipos. Disponível em: https://www.uol.com.br/tilt/reportagens-especiais/como-os-algoritmos-espalham-racismo/#end-card. Acesso: 31 de outubro de 2023.

[68] THE NEW YORK TIMES. **Wrongfully Accused by an Algorithm**. Disponível em: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html . Acesso em: 19 de novembro de 2023.

O caso foi encerrado duas semanas depois, mas gerou grande comoção e discussão a respeito do uso de sistemas de reconhecimento facial para controle e vigilância e os riscos agregados à população.

O relato de Julian-Borckak ocorreu no mesmo período em que IBM, Microsoft e Amazon anunciaram cessação do fornecimento de tecnologias de reconhecimento facial para a aplicação da lei.

A primeira empresa a fazê-lo foi a IBM, cujo CEO Arvind Krishna enviou carta ao Congresso dos Estados Unidos informado sobre o não fornecimento de software de reconhecimento facial ou análise de uso geral. Veja-se trecho da carta[69]:

> A IBM não oferece mais software de análise ou reconhecimento facial de uso geral. A IBM se opõe firmemente e não tolerará o uso de nenhuma tecnologia, incluindo a tecnologia de reconhecimento facial oferecida por outros fornecedores, para vigilância em massa, criação de perfil racial, violações de direitos humanos e liberdades básicas ou qualquer finalidade que não seja consistente com nossos valores e Princípios de Confiança e Transparência. Acreditamos que agora é a hora de iniciar um diálogo nacional sobre se e como a tecnologia de reconhecimento facial deve ser empregada pelas agências policiais nacionais.
>
> A inteligência artificial é uma ferramenta poderosa que pode ajudar a aplicação da lei a manter os cidadãos seguros. Porém, fornecedores e usuários de sistemas de IA têm uma responsabilidade compartilhada de garantir que IA seja testada quanto a viés, particularmente quando usada na aplicação da lei, e que esse teste de viés seja auditado e relatado. (Tradução livre)

O gesto das empresas foi bastante simbólico e põe em foco a necessidade de enfrentamento dos riscos advindos do uso do reconhecimento facial para os direitos humanos e para as liberdades básicas.

Em artigo publicado pelo Centro de Privacidade e Tecnologia da Georgetown Law, Clare Garvie[70] revela detalhes do procedimento adotado pela polícia americana para reconhecimento facial de suspeitos a fim de subsidiar as investigações conduzidas pelas diversas agências de segurança.

O documento desvenda que não existem regras acerca das imagens que podem ser submetidas para algoritmos de reconhecimento facial a fim de se gerar pistas investigativas. Como consequência, as agências podem submeter uma diversidade de materiais na tentativa de encontrar resultados positivos em suas bases de dados. Essas imagens podem ser oriundas de

---

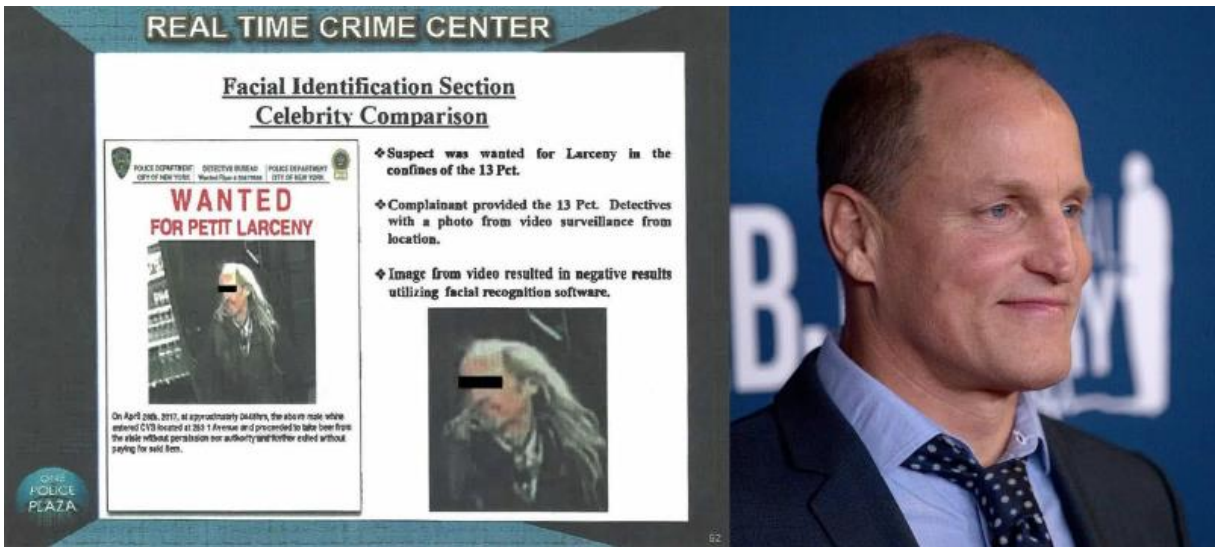
[69] IBM. IBM CDEO **Letter to Congress on racial Justice Reform**. Disponível em: https://www.ibm.com/policy/facial-recognition-sunset-racial-justice-reforms/ . Acesso em: 19 de novembro de 2023.

[70] GARVIE, Clare. **Garbage In, Garbage Out**: face recognition on flawed data. Georgetown law – Center on Privacy & Tecnology. Disponível em: https://www.flawedfacedata.com/. Acesso em: 20 de novembro de 2023.

fragmentos de vídeo de baixa qualidade, fotos de mídias sociais alteradas por filtros ou fotos digitalizadas de álbuns, por exemplo.

A pesquisadora relata caso curioso que demonstra a ausência de controle sobre os instrumentos utilizados pela polícia no processo de reconhecimento facial. Em abril de 2017, um suspeito foi flagrado por uma câmera de vigilância furtando uma cerveja na cidade de Nova Iorque. A câmera captou o rosto do autor do crime, mas a imagem ficou com baixa qualidade, escura e pixelizada. Apesar da baixa qualidade, a imagem foi utilizada no sistema de reconhecimento facial, que não retornou nenhuma resposta positiva. Contudo, um dos detetives responsáveis pelo manuseio do sistema observou que o suspeito se parecia com o ator Woody Harrelson, conhecido por atuações em programas de televisão.

Visando a buscar um resultado positivo na busca, os detetives resolveram então buscar uma foto de alta qualidade do ator no Google para submetê-la ao sistema de reconhecimento facial. Quando usada a foto, esta retornou resultados positivos, sendo identificada uma pessoa que acreditavam ser, não o ator, mas um provável suspeito da prática criminosa. Eventualmente alguém foi identificado e sujeitado a abordagem policial simplesmente por possuir traços assemelhados a um ator de Hollywood.

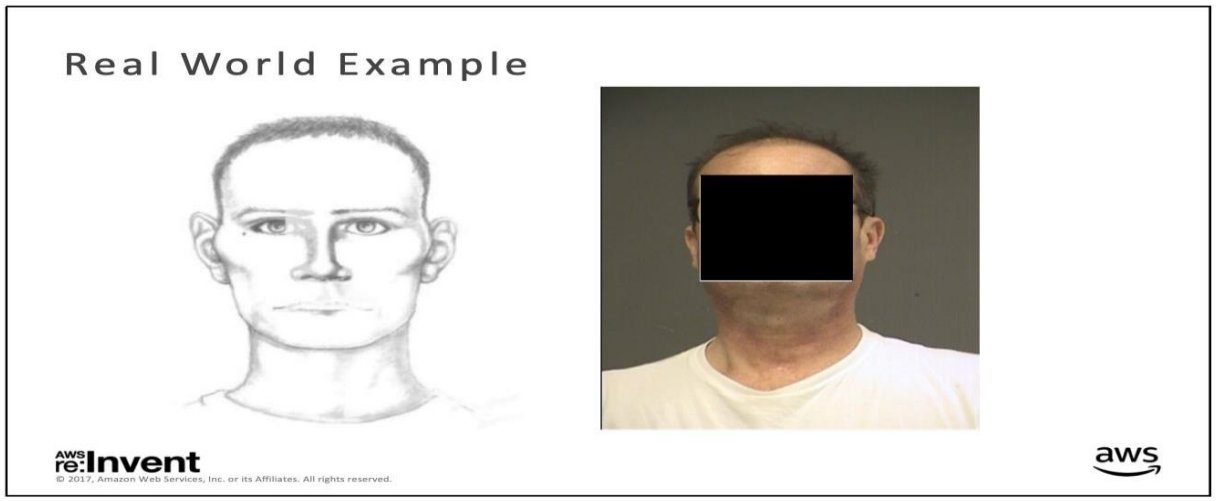


Fonte: https://www.flawedfacedata.com/

A história é pitoresca e revela a frouxidão com que algumas vezes sistemas potentes são utilizados sem a responsabilidade que se espera dos agentes que detêm seu controle. Não se aguarda que em um Estado democrático alguém seja privado de direitos ou perturbado em

sua paz em razão de elementos fracos de convicção em condução investigativa. O absurdo da situação é evidente.

Departamentos de polícia utilizam também esboços como “retrato falado” ou composições artísticas para uso comparativo nos sistemas. Os esboços são rostos desenhados a mão ou gerados por computador com base nas descrições fornecidas pela vítima ou por uma testemunha. Vejam-se exemplos:



Forensic sketch real world example
Figure 2 : Slide from an AWS presentation titled "Washington County Sheriff's Office Rekognition Case Study." (Source: Public records obtained by ACLU Oregon & Northern California.)
Fonte: https://www.flawedfacedata.com/

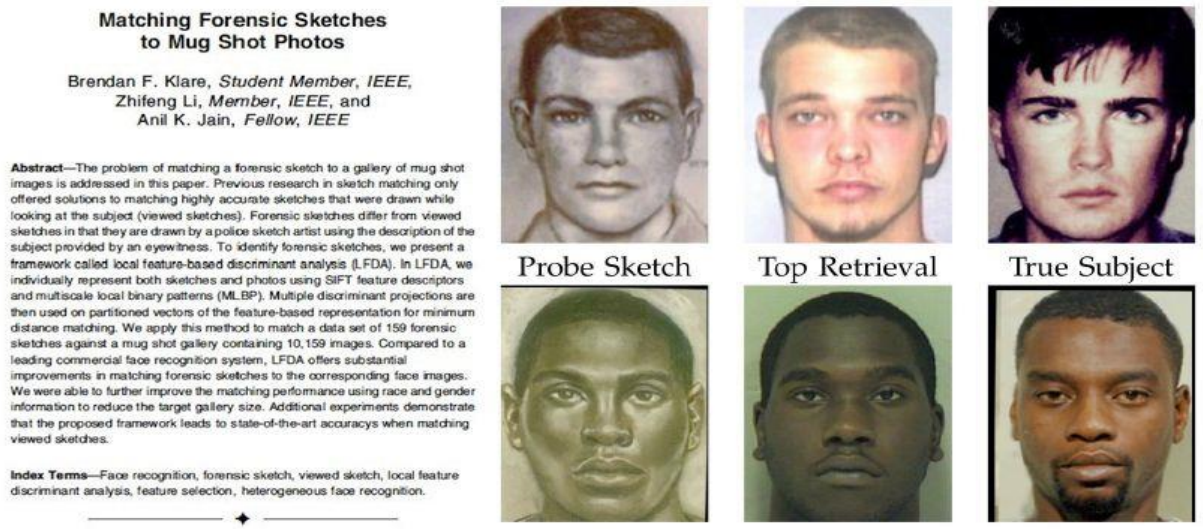


Figure 3 : Examples where an imposter, not the subject of the forensic sketch, is returned as the highest ranking face recognition match. (Source: Klare, Li, & Jain (2010), all rights reserved.)
Fonte: https://www.flawedfacedata.com/

O artigo reporta que pelo menos meia dúzia de departamentos de polícia nos Estados Unidos permitem ou encorajam a utilização de pesquisas de reconhecimento facial fundadas em esboços forenses. A preocupação com o uso desse material advém da baixa qualidade da imagem que oferecem, as quais decorrem não só da técnica utilizada, mas por estarem submetidas a altos índices de subjetividade.

A construção da figura depende: (i) da descrição realizada pela vítima ou testemunha, a qual frequentemente terá visto o ofensor sob efeito de profunda emoção, que compromete a avaliação e sensibilidade de percepção de traços de fisionomia; (ii) da possibilidade de somente haver memória de alguns traços da pessoa descrita (como olhos, queixo ou cabelo), o que exigirá que o desenhista complemente os demais traços de fisionomia de forma aleatória e (iii) da habilidade do profissional, a qual nem sempre poderá ser devidamente atestada. Ainda que se considere o melhor resultado possível em cada uma dessas etapas, o desenho daí advindo, por mais detalhado que seja, apenas trará um imagem pobre para fins de busca em um sistema de reconhecimento facial.

Estudos analisaram o desempenho de sistemas de reconhecimento facial em desenhos dessa natureza. Uma pesquisa da Universidade do Estado de Michigan realizada em 2011 observou que aqueles sistemas não são projetados para comparar esboços com rostos reais. No teste, o algoritmo foi programado para retornar uma lista de 200 correspondências possíveis pesquisando um banco de dados de 10.000 imagens. Para esboços, ele recuperou a correspondência correta entre 4,1% e 6,7% das vezes[71]. Apesar dos resultados revelados, empresas de desenvolvimento de softwares trabalham sob a promessa de êxito também com uso desse material.

Em 2014, o *National Institute of Standards and Technology* (NIST)[72] também realizou pesquisa de desempenho de algoritmos de reconhecimento facial. A pesquisa, bastante detalhada, mostrou diversos elementos que influenciam a acurácia do reconhecimento facial realizado pelo algoritmo, as quais devem ser considerados na avaliação dos resultados.

A qualidade da foto ou outro material fornecido como base para a pesquisa no banco de dados, a qualidade do sistema de inteligência artificial desenvolvido, a extensão do banco de dados (quantidade de perfis cadastrados para análise comparativa pelo sistema), o

---

[71] KLUM, Scott; HAN, Hun e JAIN, Anil K.. **Department of Computer Science and Engineering**. Michigan State University. Sketch Based Face Recognition: Forensic vs. Composite Sketches. Disponível em: https://openbiometrics.org/publications/klum2013sketch.pdf. Acesso em: 20 de novembro de 2023, p. 6.

[72] GROTHER, Patrick e NGAN, Mei. **Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms, NIST Interagency Report 8009**, 4 (May 26, 2014). Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf . Acesso em 19 de novembro de 2023, pp. 3 e 4.

grupo social do sujeito (resultado fortemente influenciado pela idade) são componentes centrais na determinação da precisão dos resultados.

Na investigação, conclui-se que a identificação precisa depende consideravelmente da idade do sujeito. Para todos os algoritmos testados, indivíduos mais velhos são mais fáceis de serem reconhecidos como eles mesmos e como distintos de outros. Isso decorre da modificação craniofacial – mudança de formato do rosto – que é mais acentuada em indivíduos mais jovens. Outrossim, o tamanho da base dados também traz influência considerável; à medida que mais identidades são inscritas em um sistema biométrico, aumenta a possibilidade de um falso positivo devido à existência de muitas faces assemelhadas.

Devido aos riscos associados, muitos organismos de segurança não consideram o reconhecimento facial realizado por algoritmo como uma identificação positiva suficiente por si, exigindo a complementação das informações por outros elementos de investigação. Assim, provas adicionais devem ser agregadas antes de haver a abordagem a qualquer suspeito indicado por meio da ferramenta tecnológica.

Visando a mitigar os riscos mencionados, Garvie apresenta algumas propostas:

- Vedação de uso de imagens de celebridades ou pessoas assemelhadas para alimentar os sistemas de reconhecimento facial; tendo em vista que o reconhecimento é considerado biométrico, é vedado à polícia substituir a biometria de uma pessoa pela outra.
- Vedação de uso de esboços artísticos, dada a baixa probabilidade de que tragam resultados corretos, além das deficiências decorrentes da subjetividade de quem descreve e de quem desenha.
- Definição de padrões mínimos de qualidade fotográfica como a densidade de *pixels* e a porcentagem do rosto que deve estar visível na foto original, descartando-se as fotos que não atendam a esses requisitos mínimos.
- Documentação de qualquer edição feita nas imagens com o fito de torná-las mais claras para os sistemas de reconhecimento facial.
- Realização de dupla confirmação. O sistema deverá criar uma pista investigativa apenas se for confirmada a correspondência por dois analistas humanos independentes.

- Criar protocolos para corroboração do resultado do algoritmo por outros elementos coligidos durante a investigação antes de serem tomadas quaisquer medidas ofensivas contra suspeitos.
- Disponibilizar à defesa todas as informações sobre o procedimento de reconhecimento facial por meio de algoritmo, em especial a indicação do instrumento utilizado (foto, vídeo, desenho etc.), bem como de quaisquer edições realizadas e a indicação dos responsáveis pela conferência da correspondência indicada.

A qualidade do material de análise, o grupo etário em que está o sujeito inserido ou a extensão do grupo de análise não são as únicas questões problemáticas relacionadas ao reconhecimento facial, porém. O caso de Robert Julian-Borchak apenas acentuou o debate acerca de vieses dos sistemas utilizados para segurança e identificação de pessoas para persecução penal, mas há problemas adicionais.

Trabalhos realizados por institutos e grupos de pesquisa demonstram que, enquanto os sistemas de reconhecimento facial funcionam relativamente bem em relação a homens brancos, os resultados são menos precisos para outros grupos demográficos.

Joy Buolamwini, pesquisadora no MIT Media Lab., ao experimentar softwares de detecção facial, descobriu que o sistema não identificava seu rosto negro até que ela colocasse uma máscara branca, mostrada na imagem abaixo[73].

Fonte: https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

[73] No documentário "*Coded Bias*", disponível na plataforma Netflix, a pesquisadora narra a descoberta das falhas nos sistemas de reconhecimento O documentário também investiga vieses dos algoritmos.

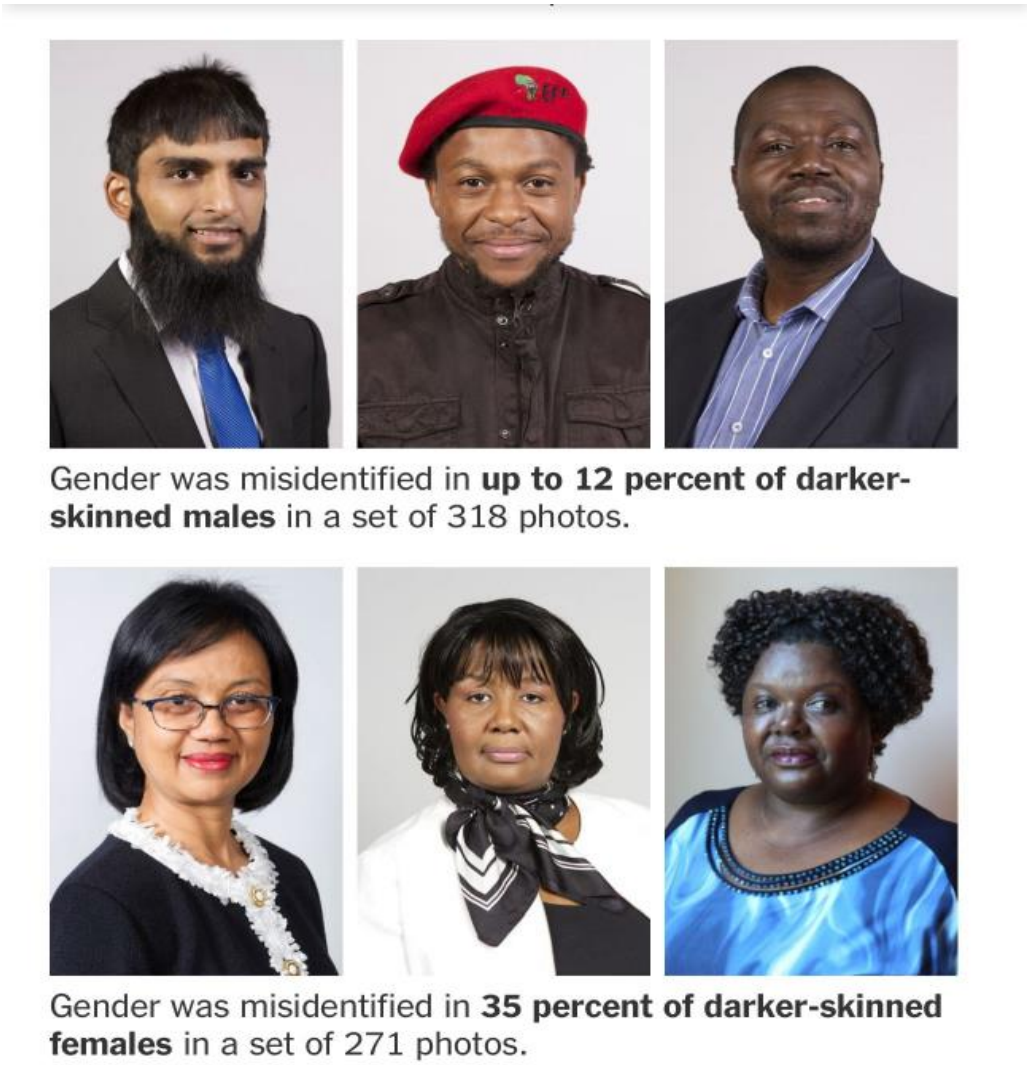
A experiência de Joy revelou a exclusão a que pessoas de sua cor estavam submetidas no desenvolvimento da tecnologia, o que refletia no próprio sistema de inteligência artificial. Ademais, revela que outros grupos igualmente estão sujeitos a resultados nocivos, como mulheres e pessoas com deficiência.

No laboratório, em 2017, foram testados softwares de reconhecimento facial produzidos por IBM, Microsoft e Face++[74]. O teste visava a aferir a acurácia para reconhecimento de gênero, o qual foi divido em duas categorias – masculino e feminino – apesar da admissão de outros gêneros não submetidos à classificação dual.

Quando confrontado com fotos de homens brancos, os softwares fizeram, em média, reconhecimento preciso em 99% das vezes; em 1% não se fez adequada identificação do gênero. Contudo, quanto mais escura a pele, mais erros de identificação surgem, com resultados ainda piores quando se cuida de mulheres.

Fonte: https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

[74] THE NEW YORK TIMES. **Facial Recognition Is Accurate, if You're a White Guy**. Disponível em: https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html .Acesso em: 20 de novembro de 2023.



Fonte: https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

A acurácia para rostos femininos brancos foi de 93%. Quando usados rostos negros, o gênero foi identificado erroneamente em até 12% dos homens de pele mais escura e 35% em mulheres de pele escura. Todas as companhias performaram melhor na análise de homens do que na análise de mulheres e todas performaram pior com mulheres negras[75]. O resultado decorre em grande medida de falhas na alimentação do banco de dados, com figuras associadas insuficientes em número ou qualidade.

[75] BUOLAMWINI, Joy e GEBRU, Timnit. **Gender Shades**: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Fairness, Accountability, and Transparency, New York, NY, February 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf . Acesso em: 20 de novembro de 2023.

Informadas dos resultados, as empresas apresentaram respostas. Os líderes da IBM Watson informaram que estão fazendo alterações em seu software de reconhecimento facial e conduzindo testes para melhoria do sistema[76]. A Microsoft informou que tomou medidas para melhorar a precisão da tecnologia de reconhecimento facial e que continua investindo em pesquisas para reconhecer, compreender e remover preconceitos[77]. Até a publicação do texto no endereço eletrônico, a Face++ não havia enviado resposta.

Após a experiência, a pesquisadora fundou o *Algorithmic Justice League* (AJL)[78], uma organização sem fins lucrativos de defesa digital com sede em Cambridge que visa a aumentar a consciência pública sobre os impactos da inteligência artificial, expondo os possíveis danos e as implicações sociais de seu uso. As primeiras ações foram voltadas para exposição do preconceito nos softwares de reconhecimento facial. Em seguida, foram inseridas discussões sobre questões de equidade e responsabilização na IA, incluindo preconceitos algorítmicos, tomada de decisões e auditoria algorítmicas. Diante dessas revelações, transparência e auditoria devem ser priorizadas.

Joy Buolamwini[79] também realça que muitos sistemas foram desenvolvidos com os rótulos binários de gênero "masculino" e 'feminino", que desconsideram a existência de pessoas trans e indivíduos intersexuais ou pessoas com mais identidades de gênero e fluidas.

Outros dados relevantes foram levantados pela organização de liberdade civil Big Brother Watch, sediada no reino Unido. A entidade divulgou relatório em 2018 documentando que a polícia metropolitana do Reino Unido testou sistemas de reconhecimento facial que combinou erroneamente pessoas com criminosos em mais de 98% das vezes. A polícia de Gales do Sul teve como resultado 91% de falsos positivos[80].

A organização ainda denuncia que a imagem de todos que passam em frente às câmeras é capturada, processando dados tão sensíveis quanto as impressões digitais, muitas vezes sem o consentimento dos indivíduos. Assim, polícia e empresas privadas cada vez mais

---

[76] Disponível em: http://gendershades.org/docs/ibm.pdf. Acesso em: 20 de novembro de 2023.
[77] Disponível em: http://gendershades.org/docs/msft.pdf. Acesso em: 20 de novembro de 2023.
[78] ALGORITHMIC JUSTICE LEAGUE. Disponível em: https://www.ajl.org/about. Acesso em: 20 de novembro de 2023.
[79] BUOLAMWINI, Joy. **Unmasking AI**: my mission to protect what is human in a world of machines. New York: Random House, 2023, p. 74.
[80] *Op. Cit.*, p. 76.

usam a tecnologia para monitorar, categorizar e rastrear pessoas, exercendo vigilância perigosamente autoritária e ameaçadora da privacidade e das liberdades[81].

Há ainda preocupações adicionais. A entidade destaca o desrespeito à privacidade e aos direitos humanos e a ausência de proporcionalidade no uso da ferramenta para encontrar suspeitos de crimes.

A questão não foi ignorada pelas Cortes internacionais. No processo Glukhin v. Rússia, a Corte Europeia de Diretos Humanos, em 04 de julho de 2023, proferiu importante decisão[82] em que analisou as implicações da Convenção dos Estados que utilizam a Tecnologia de Reconhecimento Facial (TRF).

Veja-se resumo do caso:

> Em 23 de agosto de 2019, Nikolay Sergeyechi Glunkhin (requerente) viajou pelo metrô Moscou com um papelão em tamanho real na qual existia a figura de um ativista político preso pela polícia russa em evento que ganhou grande repercussão na mídia. No cartaz, lia-se: "You must be f**king kidding me. I'm Konstantin Kotov. I'm facing up to five years [in prison] under [Article] 212.1 for peaceful protests."
>
> Houve, então, condenação administrativa do requerente por não haver notificado as autoridades acerca da sua intenção de realizar uma demonstração individual utilizando um "objeto de (des)montagem rápida". A polícia afirmou que a ação foi feita no âmbito de um inquérito conduzido com o objetivo de combater o extremismo durante eventos públicos de massa.
>
> Em 23 de setembro de 2019, o Meshchanskiy District Court of Moscow (Tribunal Distrtital de Meshchanskiy de Moscou) condenou o requerente pelas acusações. Foi apresentada apelação, mas o Tribunal manteve a condenação. Glunkhin recorreu, então, ao Tribunal Europeu de Direitos Humanos.

Glunkhin, foi detido menos de dois dias após a manifestação solitária e pacífica. Nas peças de informação, foram juntadas fotografias e vídeos publicados no Telegram; contudo, estes não possuíam qualquer informação que pudesse identificar o requerente. O relatório policial também não explicou quais medidas foram tomadas para identificá-lo.

Glunkhin afirmou que sua identidade foi aferida a partir do uso de base de dados cruzado com sistema de reconhecimento facial, o que não foi negado explicitamente pelo governo, o qual, em referência à base legal aplicada, incluiu decreto referente à instalação de câmeras no metrô de Moscou. Outrossim, o Tribunal tomou nota de informação pública acerca

---

[81] BIG BROTHER WATCH. **Big Brother is not only watching you – he's identifying you**. Disponível em: https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/. Acesso em: 20 de novemrbod e 2023.

[82] CORTE EUROPEIA DE DIREITOS HUMANOS. **Case of Glukhin v. Russia**. Application nº 11519/20. Disponível em: https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-225655%22]}. Acesso em: 20 de novembro de 2023.

de numerosos casos que envolviam a utilização de tecnologia de reconhecimento facial para identificação de participantes de protestos na Rússia. Diante dessas circunstâncias, considerou a Corte que a tecnologia de reconhecimento facial foi utilizada no caso.

No julgamento, a preocupação com a liberdade de expressão, a privacidade e o respeito à organização social democrática ficaram evidentes. Os fatos ocorridos na Rússia chamam atenção para os riscos em todas as sociedades democráticas que trabalham com tecnologias assemelhadas.

Em maio de 2017, foi noticiado no site oficial da prefeitura de Moscou a instalação de mais de 3.500 câmeras CCTV. Em setembro do mesmo ano, mais de 3.000 câmeras CCTV foram equipadas com sistema de reconhecimento facial em tempo real. Em setembro de 2020, as mais de 175.000 câmeras CCTV de Moscou estavam equipadas com a tecnologia. Foi nesse contexto que Konstantin Kotov, o ativista político detido objeto do protesto de Glunkhin, foi preso e, no final, o próprio protestante.

De acordo com o apelante, em 24 de agosto de 2019, foi reportada a realização de "monitoramento da Internet" pela unidade anti-extremismo da polícia de Moscou, a qual revelou sua fotografia. Após a identificação, a polícia o procurou em sua casa e, não sendo ali encontrado, foi detido numa estação de metrô. Essa questão é relevante. A decisão da Corte Europeia menciona resultados de pesquisa realizada por OVD-Info, um projeto de mídia independente em direitos humanos, chamado "Como o Estado russo usa câmeras contra manifestantes"[83].

No documento da entidade, revelam-se diversas prisões de protestantes após o fim dos eventos, acreditando-se que estas ocorrem com o uso de tecnologias de monitoramento social e reconhecimento facial. Reporta-se que, embora o uso do sistema de reconhecimento facial tenha sido largamente coberto pela mídia após janeiro de 2021, a tecnologia raramente é mencionada em documentos oficiais, o que demonstra que seu uso vem sendo feito dentro de uma zona cinzenta. O fato de as detenções ocorrerem em locais diversos – casas, locais de trabalho, cafés etc. – demonstra que a tecnologia é usada em larga medida.

A agência independente denuncia, ainda, a ausência de informações acerca das atividades de investigação e como exatamente é feita a identificação de uma pessoa em particular. A prática das detenções após os eventos (*post factum detentions*), reafirmam, possui

[83] OVD-INFO**. How the Russian state uses cameras against protesters**. Disponível em: https://en.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters#1 . Acesso em: 20 de novembro de 2023.

clara orientação punitiva, intimidatória e marginalizadora de potenciais participantes em movimentos de protestos. O argumento é reforçado pela indicação do uso da tecnologia para diversos tipos de ofensas, como atravessar a rua em lugar errado, o que evidencia que o objetivo não é atender ao interesse público, mas perseguir oponentes políticos.

Na conclusão do julgamento, a Corte Europeia de Direitos Humanos reconheceu a infração do governo russo a duas normas da Convenção Europeia de Direitos Humanos: artigo 8º, que cuida da vida privada, e artigo 10, disciplinador da liberdade de expressão:

> ARTIGO 8
>
> Direito ao respeito pela vida privada e familiar
>
> 1. Toda pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
>
> 2. Não haverá interferência de uma autoridade pública no exercício deste direito, exceto em conformidade com a lei e necessidade em uma sociedade democrática no interesse da segurança nacional, da segurança pública ou do bem-estar econômico do país, para a prevenção da desordem ou do crime, para a proteção da saúde ou da moral, ou para a proteção dos direitos e liberdades de terceiros.
>
> ARTIGO 10
>
> Liberdade de expressão
>
> 1. Todos têm o direito de liberdade de expressão. Este direito inclui a liberdade de ter opiniões e receber e transmitir informações e ideias sem interferência da autoridade pública e independentemente de fronteiras. Este artigo não impedirá que os Estados exijam o licenciamento de empresas de radiodifusão, televisão ou cinema.
>
> 2. O exercício destas liberdades, uma vez que acarreta deveres e responsabilidades, pode estar sujeito às formalidades, condições, restrições ou sanções previstas na lei e necessárias numa sociedade democrática, no interesse da segurança nacional, da integridade territorial ou segurança pública, para a prevenção de desordem ou crime, para a proteção da saúde ou da moral, para a proteção da reputação ou dos direitos de terceiros, para impedir a divulgação de informações recebidas em sigilo, ou para manter a autoridade e imparcialidade do judiciário. (Tradução livre)

A Corte destacou, no julgamento, quanto à liberdade de expressão, que a proteção do artigo 10 não é limitada à palavra falada ou escrita, mas a qualquer forma de comunicação que revele ideias e opiniões. No caso concreto, considerou que o apelante apenas expressou opinião sobre questão pública relevante, não incidindo nas hipóteses de exceção da segunda parte do artigo 10. Nos termos da decisão, "as autoridades não demonstraram grau de tolerância necessário relativamente à manifestação pacífica individual do requerente", não havendo "razões relevantes para justificar a interferência no direito à liberdade de expressão."

Sobre a privacidade, a Corte traz destaque importante: a privacidade envolve não apenas um círculo no qual o indivíduo se enquadra sem interferência de terceiros; aquela não exclui atividades que ocorram em um contexto público. Assim, mesmo ações praticadas em locais de acesso público podem ser consideradas inseridas dentro da esfera de privacidade do agente, em especial quando se cuida de demonstrações relativas a dados sensíveis, como categorizações advindas da demonstração de ideias e pensamentos.

Outra conclusão relevante diz respeito a sistematicidade ou não da captura de imagens. Ressalta a Corte que "a monitorização das ações e movimentos de um indivíduo num local público utilizando uma câmara que não gravou os dados visuais não constitui em si uma forma de interferência na vida privada"; no entanto, "podem surgir considerações de vida privada, uma vez criado qualquer registro sistemático ou permanente de tais dados pessoais, especialmente fotografias de uma pessoa identificada."

A imagem, um dos principais atributos da personalidade, revela características únicas da pessoa, distinguindo-a de seus pares. Assim, conclui a Corte, o direito de cada pessoa à proteção de sua imagem é componente essencial do desenvolvimento pessoal e pressupõe o direito de controlar a sua utilização. Nesse âmbito protetivo, enquadra-se não só a publicação da imagem, mas o direito do indivíduo de se opor à gravação, conservação e reprodução da imagem por terceiros. Conclusão importante é a de que a coleta de dados num local público constitui também intervenção na vida privada das pessoas.

Por fim, ressaltou o tribunal que é necessário um elevado nível de justificação do uso da tecnologia de reconhecimento facial e sua interferência na esfera privada dos indivíduos em uma sociedade democrática. No caso concreto, como o protesto revelava a posição política do indivíduo, a informação enquadrava-se na categoria especial de dados sensíveis, atraindo um nível de proteção ainda mais elevado.

O exemplo acima demonstra de forma evidente os riscos que a tecnologia de vigilância pode gerar em uma sociedade democrática. Por isso, diversos foram os diplomas expedidos com vistas à sua regulamentação e estabelecimento de precisos limites de aplicação.

O Alto Comissariado das Nações Unidas para os Direitos Humanos, provocado pelo Conselho de Direitos Humanos, preparou relatório temático sobre as novas tecnologias e seu impacto na promoção e proteção dos direitos humanos[84]. Para elaboração do relatório,

[84] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Conselho de Direitos Humanos. **Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests**. Disponível em: https://documents-dds-

foram ouvidos Estados e parceiros importantes como agências das Nações Unidas, instituições nacionais de direitos humanos, organizações regionais e organismos da sociedade civil.

Reportam-se no relatório importantes conclusões. Inicialmente, cita-se que as comunicações seguras e confidenciais desempenham papel fundamental no planejamento e realização de protestos pacíficos. Assim, a vigilância possibilitada pela tecnologia representa riscos significativos para exercício dos direitos humanos em reuniões pacíficas e é um ator importante na diminuição do espaço cívico em muitos países. Também no relatório informa-se que o uso da tecnologia de reconhecimento facial para identificar pessoas em um contexto de reunião tem efeitos adversos consideráveis no direito à privacidade, à liberdade de expressão e de reunião pacífica, caso não existam salvaguardas eficazes.

Outrossim, o registro e arquivamento de imagem facial sem o consentimento do titular constitui interferência no direito à privacidade, havendo um desrespeito massivo quando a coleta e processamento de imagens faciais abrange todas as pessoas capturadas pela câmera equipada com a tecnologia de reconhecimento facial.

A preocupação demonstrada pelos diversos organismos públicos e privados é justificada. Muitas pessoas se sentem desencorajadas a participar de manifestações pacíficas ou a expressar suas opiniões e ideias de forma livre quando temem ser identificadas e possivelmente sofrer consequências negativas. Por isso, a captura de imagens e seu processamento por agentes de Estado somente pode ser feita de maneira excepcional e após avaliação de três requisitos essenciais: legalidade, necessidade e proporcionalidade.

A possibilidade de uso da tecnologia de reconhecimento facial deve passar, em primeiro lugar, por uma análise indicativa da base legal que permite seu uso, a qual deve estar expressa em diplomas que tratam da matéria após acurada análise de constitucionalidade. Importante, ainda, que essa construção seja feita com amplo debate e participação democrática, com diversos grupos sociais envolvidos, a fim minorar as consequências negativas da falta de representatividade de determinadas classes mais expostas à discriminação e marginalização.

Deve ser apurada a necessidade de uso do meio invasivo diante do fim que se busca alcançar com a medida. Somente quando outros recursos menos ofensivos não possam ser utilizados com eficácia suficiente para atingimento do fim é que se pode valer-se da tecnologia de reconhecimento facial.

---

ny.un.org/doc/UNDOC/GEN/G20/154/35/PDF/G2015435.pdf?OpenElement. Acesso em: 20 de novembro de 2023.

Por fim, a análise de proporcionalidade. Esta deve sempre estar presente, ainda que se esteja diante de uma base legal e da demonstração de adequação do meio para atingimento do fim da norma. Raramente, em ambientes pacíficos, o reconhecimento facial será considerado proporcional, ressalvadas as hipóteses muitas vezes mencionadas em diplomas normativos que cuidam da matéria e tratam de comportamento criminoso, prevenção, investigação ou repressão de infrações penais.

Esse é o conteúdo também da Diretiva (EU) 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou a execução de sanções penais, e sobre a livre circulação desses dados.

A Diretiva pretende contribuir, declaradamente, para a realização de um espaço de liberdade, segurança e justiça a partir da proteção das pessoas singulares no que diz respeito ao tratamento de seus dados pessoais.

Atenção especial é dada pelo documento aos dados sensíveis que revelem origem racial ou étnica (ressaltando que a utilização do termo não significa a aceitação, por parte da União, de teorias que tentam determinar a existência de raças humanas distintas). A Diretiva impõe que esses dados não sejam tratados, a menos que o tratamento esteja sujeito a garantias adequadas aos direitos e liberdades do titular dos dados, estabelecidas por lei, e seja permitido (i) nos casos autorizados por lei; (ii) quando, ainda que não autorizado por lei, o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa; ou (iii) o tratamento diga respeito a dados manifestamente tornados públicos pelo titular dos dados. Outras diversas regras de proteção dos dados pessoais são ali elaboradas, demonstrando a preocupação internacional com uso adequado das informações pessoais no âmbito da segurança do Estado.

Esse é o cenário internacional. No Brasil, a aplicação do sistema de reconhecimento facial também tem sido difundida pelo setor público nos últimos anos. O Instituto Igarapé revela que o modelo vem sendo utilizado no país desde 2011, tornando-se especialmente popular em 2019, quando comitiva do Partido Social Liberal, ao qual pertencia o então presidente Jair Bolsonaro, viajou à China a fim de conhecer o sistema já usado no país asiático[85].

[85] INSTITUTO IGARAPÉ. **Reconhecimento Facial no Brasil**. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Avesso em: 20 de novembro de 2023.

Um impulsionamento à adesão ao modelo ocorreu em 2019 quando o então ministro da Justiça e Segurança Pública, Sérgio Moro, baixou portaria que incentiva a adoção do reconhecimento facial na segurança pública[86]. Como incentivo do modelo, a Portaria n° 793, de 24 de outubro de 2019[87], foi editada, regulamentando o aporte financeiro em ações voltadas à segurança pública e defesa social. Um dos eixos estruturantes do projeto cuida da modernização das instituições de segurança pública, com destaque para algumas linhas de atuação, entre as quais "fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por *Optical Character Recognition* - OCR, uso de inteligência artificial ou outros (art. 4º, § 1º, III, *b*)."

O início do uso desse sistema de vigilância abriu a discussão sobre seus benefícios e riscos diante dos casos observados no cenário estrangeiro. Audiências públicas foram organizadas na Câmara dos Deputados[88] e no Ministério Público[89], com vistas a debater o tema e sua implicações na conjuntura nacional. Hoje as discussões centram-se no Projeto de Lei n º 3069, apresentado em 22 de dezembro de 2022[90], o qual regulamenta o uso do reconhecimento facial automatizado pelas forças de segurança pública em investigações criminais ou procedimentos administrativos.

A matéria tramita na Câmara dos Deputados e será analisada, em caráter conclusivo, pelas Comissões de Segurança Pública e Combate ao Crime Organizado; de Constituição e Justiça e de Cidadania. Tramitando em caráter conclusivo, o projeto é votado apenas pelas comissões designadas para analisá-lo, dispensada a deliberação em plenário. O projeto perde esse caráter somente se houver decisão divergente entre as comissões ou se, aprovado ou rejeitado, houver recurso assinado por pelo menos 52 deputados para a apreciação da matéria em plenário[91]. O projeto já foi aprovado pela Comissão de Segurança Pública da Câmara em agosto de 2023.

---

[86] O PANÓTIPO. **Reconhecimento facial cresce no Brasil**; entenda como isso afeta você. Disponível em: **https://opanoptico.com.br/reconhecimento-facial-cresce-no-brasil-entenda-como-isso-afeta-voce/**. Acesso em: 20 de novembro de 2023.

[87] BRASIL. Ministério da Justiça e Segurança Pública. Portaria n°793, de 24 de outubro de 2019. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575. Acesso em: 20 de novembro de 2023.

[88] Disponível em: https://www.camara.leg.br/noticias/554826-governo-quer-lei-para-regular-vigilancia-estatal-por-meio-de-reconhecimento-facial/ . Acesso em: 20 de novembro de 2023.

[89] Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10779-mpdft-audiencia-publica-debate-uso-ferramentas-de-reconhecimento-facial. Acesso em: 20 de novembro de 2023.

[90] BRASIL. Projeto de Lei n º 3069, apresentado em 22 de dezembro de 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2228103&filename=PL%203069/2022. Acesso em: 20 de novembro de 2023.

[91] Fonte: https://www.camara.leg.br/noticias/946010-projeto-regulamenta-o-uso-de-reconhecimento-facil-por-forcas-de-seguranca-publica. Acesso em: 20 de novembro de 2023.

No projeto, a matéria é disciplinada em 8 artigos, que cuidam de detalhes práticos para aplicação do sistema em poucas normas de regulação. Entre os dispositivos de destaque, mencionam-se: (1) previsão de uso da tecnologia em investigações criminais (para identificação de suspeitos) e em procedimentos civis e administrativos (para busca de pessoas desaparecidas); (ii) necessidade de indicação, por meio de placas informativas, dos locais onde houver captura de imagens para reconhecimento facial (RF); (iii) exigência de que, em caso de identificação positiva, haja confirmação por agente público responsável e (iv) possibilidade de compartilhamento das informações com integrantes operacionais do Sistema Único de Segurança Pública.

O diploma deixa de prever normas importantes relativas a transparência e auditabilidade, avaliação de impacto da aplicação do sistema, responsabilidade em caso de erro, bem como limites precisos para o compartilhamento de informações, matérias sensíveis em se tratando de proteção de dados pessoais. A inexistência de uma legislação específica aplicada à segurança pública que traga disciplinamento mais aprofundado aponta para uma certa discricionariedade no uso da tecnologia por parte dos agentes encarregados por sua utilização.

Contudo, deve-se lembrar que, mesmo as atividades relacionadas à segurança pública, excetuadas pelo artigo 4º, III, da LGPD, devem atender aos princípios daquela norma geral. Assim, nesses casos, deve-se igualmente respeitar a finalidade, necessidade, transparência, adequação, segurança e não-discriminação, e os demais princípios, adaptados para o cenário específico do reconhecimento facial (RF) para fins de segurança pública.

Até 2020, na esfera estadual, foram identificadas quatro leis que tratam especificamente de reconhecimento facial. Em duas delas - Lei nº 16.873/2019, do Estado do Ceará e Lei nº 7.123/2015, do Estado do Rio de Janeiro, a implantação do sistema de reconhecimento facial possui finalidade específica – cadastro para fins de controle de acesso a determinados lugares. Nas outras duas - Lei nº 21.737/2015, do Estado de Minas Gerais e Lei nº 8.113/2019, do Estado de Alagoas, a previsão é genérica, para implantação de "sistemas de reconhecimento facial" em determinados lugares, podendo ser utilizado, dado não haver restrição no texto, não apenas para controle de acesso, mas também para eventual identificação de pessoas[92].

[92] DATA PRIVACY BRASIL e INSTITUTO IGARAPÉ. **Regulação do Reconhecimento Facial no Setor Público**: avaliação de experiências internacionais. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 20 de novembro de 2023.

A preocupação normativa ressoa relevante, já que a tecnologia já apresenta uso alargado no Brasil. Relatório do Laboratório de Políticas Públicas e Internet (LAPIN)[93] informa que o uso do RF pelo Poder Público é voltado a seis finalidades: segurança pública, transporte urbano, escolas, sistemas para gestão de benefícios sociais, controle alfandegário e validação de identidade.

Na segurança pública, além das câmeras de videomonitoramento, o RF tem sido utilizado principalmente para identificar pessoas procuradas pela polícia. O relatório chama atenção para o Estado da Bahia, onde até janeiro de 2021, mais de 201 foragidos foram identificados pela Secretaria de Segurança Pública do Estado.

As falhas no uso dos sistemas também começam a aparecer no solo brasileiro. Em 2019, no Rio de Janeiro, menos de duas semanas depois do início de uso, um sistema de reconhecimento facial por câmeras identificou erroneamente uma identidade[94]. Uma mulher foi encaminhada à delegacia após ser confundida com uma infratora que já estava presa. Para além dos problemas de ordem técnica dos instrumentos utilizados, assim, outra questão pode ser realçada a partir desse caso: bancos de dados desatualizados levam também a erros e abordagens equivocadas de indivíduos inocentes.

Das considerações acima, observa-se que houve um uso generalizado da tecnologia de reconhecimento facial em todo o mundo, com resultados positivos, mas grandes impactos na esfera privada de indivíduos, além de profunda capacidade discriminatória no uso daquela. Observou-se, igualmente, práticas agressivas de vigilância e controle social, que põem em risco a ordem social e democrática de muitos países.

Assim, quando o reconhecimento facial falha tecnicamente, o indivíduo pode ser investigado por conduta que não praticou, tendo mitigados direitos e garantias individuais de forma indevida em razão do equívoco da ação estatal.

Contudo, quando o sistema acerta, confere aos seus detentores ferramenta de vigilância sofisticada, que pode ser usada para fins de controle social e repressão. A articulação de legislação disciplinadora e protetiva do tema é expressão e exigência de um compromisso político que diligencie na identificação, prevenção e mitigação dos riscos aos direitos humanos

---

[93] REIS, Carolina; ALMEIDA, Eduarda Costa; DOURADO, Fernando Fellows e SILVA, Felipe Rocha da. **Vigilância automatizada**: uso de reconhecimento facial pela Administração Pública. Laboratório de Políticas Públicas e Internet (LAPIN). Disponível em: https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/ . Acesso em: 20 de novembro de 2023.

[94] Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/07/em-fase-de-testes-reconhecimento-facial-no-rio-falha-no-2o-dia.shtml. Acesso em: 20 d enovembro de 2021.

advindos do desenvolvimento de novas tecnologias, em especial aquelas que levam à vigilância e ao controle social.

Deve-se observar, outrossim, o papel do Estado como agente responsável pela promoção e defesa dos direitos fundamentais. Nesta perspectiva, conforme doutrina Daniel Sarmento e Cláudio Pereira de Souza Neto[95], enjeita-se a crença de que o Estado seja o adversário, por excelência, dos direitos humanos, de modo a ser vigiado para que os cidadãos estejam a salvo de seu arbítrio.

Embora esse controle da atividade estatal seja sempre necessário, é preciso que se aloque a questão nos termos mais adequados para uma teoria constitucional democrática e inclusiva, ressaltando-se o dever do Estado de agir como promotor e defensor dos direitos fundamentais diante dos perigos que rondam a sociedade. É essa a postura que se espera no desenvolvimento, execução e aprimoramento das tecnologias aplicadas nos diversos setores da atuação estatal.

4.2 Monitoramento por câmeras, cruzamento e compartilhamento de informações

Em 2020, em seu endereço eletrônico, o *Intercep* Brasil informou que o Ministério da Justiça expandia uma das maiores ferramentas de vigilância e controle de que se teve notícia no país: o córtex[96].

O Ministério da Justiça e Segurança Pública traz em sua página oficial informações sobre o programa, o qual visa declaradamente a integrar forças de segurança pública no combate de diversas modalidades de prática criminal[97]. Informa-se na página do governo que as funcionalidades do programa serão utilizadas para fim exclusivo de segurança pública e sempre operadas por agentes públicos cujo perfil de acesso esteja designado para atuar na plataforma.

A Portaria nº 218, de 29 de setembro de 2021[98], regulamentou a chamada Plataforma Integrada de Operações e Monitoramento de Segurança Pública – Córtex, que atua sob a coordenação da Secretaria de Operações Integradas (SEOPI), do Ministério da Justiça e

---

[95] SOUZA NETO, Cláudio Pereira de; SARMENTO, Daniel. **Direito Constitucional**: teoria, história e métodos de trabalho. 2ª ed., 6ª reimpr. Belo Horizonte: Fórum, 2019, p. 239.
[96] INTERCEPT BRASIL. Disponível em: https://www.intercept.com.br/2020/09/21/governo-vigilancia-cortex/. Aceso em: 20 de novembro de 2023.
[97] BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Plataforma de Monitoramento Córtex**. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/operacoes-integradas/destaques/plataforma-de-monitoramento-cortex. Acesso em: 18 de novembro de 2023.
[98] BRASIL. **Portaria nº 218, de 29 de setembro de 2021**. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/operacoes-integradas/cortex/publicacoes/portaria-no-218-de-29-de-setembro-de-2021/view. Aceso em: 20 de novembro de 2023.

Segurança Pública. Nos termos da normativa, a plataforma será usada para fins exclusivos de segurança, tendo como objetivos a gestão de operações, o monitoramento de atividades e indicadores oriundo de operações de segurança e mapeamento de situações a partir da integração de dados.

Foi informado pelo *Intercept Brasil* que, por meio do Córtex, é usada tecnologia de inteligência artificial para leitura de placas de veículos por meio de câmeras espalhadas em rodovias, ruas e avenidas para rastrear alvos móveis em tempo real. Afirma-se, ainda, que o sistema é integrado a bancos de dados com informações sigilosas e sensíveis, exemplificativamente a RAIS - Relação Anual de Informações Sociais, do Ministério da Economia.

Essa integração, se de fato existente, permite que os agentes operadores do Córtex tenham acesso a dados cadastrais e trabalhistas que todas as empresas possuem sobre seus funcionários, incluindo RG, CPF, filiação, endereço, relação de dependentes, salário e cargo. O acesso a tamanha base dados, associada à possibilidade de localização geográfica dos indivíduos pelo acompanhamento de seus deslocamentos, na prática, permite monitoramento e vigilância detida de indivíduos e grupos perfilhados.

O Ministério da Justiça nega que haja integração com bases de dados do Ministério da Economia. Contudo, a agência de informação veiculou vídeo em que capitão da polícia militar de São Paulo explica como usa a ferramenta Córtex. No filme[99], mostra-se a facilidade no acompanhamento dos deslocamentos dos veículos, bem como no cruzamento de informações com outras bases de dados. Uma das bases apresentadas na demonstração é exatamente a RAIS.

No vídeo exibido, narra-se que um alvo móvel, quando acessado por câmera de monitoramento, é identificado em dois segundos, indo as informações diretamente para os agentes de vigilância. A partir daí, estes podem continuar acompanhando o deslocamento, determinar abordagem pela unidade policial mais próxima ou cruzar as informações do veículo com as diversas bases de dados disponíveis por meio das parcerias firmadas.

Denúncias envolvendo a SEOPI e o Ministério da Justiça retratam bem a extensão do risco advindo de tamanho poder nas mãos do Estado.

A SEOPI, órgão que gerencia o Córtex, foi instituída em janeiro de 2019 por meio do Decreto nº 9.662, de 1º de janeiro, substituído pelo atualmente vigente Decreto nº 11.348, de 1º de janeiro de 2023. Em 2020, foi revelado que a Secretaria realizou monitoramento

[99] Disponível em: https://www.intercept.com.br/2020/09/21/governo-vigilancia-cortex/. Acesso em: 20 de novembro de 2023.

político de adversários e críticos do governo Jair Bolsonaro, como pincelado linhas atrás. Notícia do portal UOL[100] informou que foi colocada em prática ação sigilosa sobre um grupo de 579 servidores federais e estaduais de segurança identificados como integrantes do "movimento antifascismo" e 3 professores universitários, incluindo o ex-secretário nacional dos direitos humanos.

No dossiê elaborado, foram indicados nomes, fotografias, endereços de redes sociais das pessoas monitoradas, o qual foi repassado para diversos outros órgãos públicos, como Polícia Rodoviária Federal, Casa Civil da Presidência da República, Abin (Agência Brasileira de Inteligência), Força Nacional e três "centros de inteligência" vinculados à SEOPI no Sul, Norte e Nordeste do país. O relatório, portanto, foi espalhado, sem se saber quantos órgãos e pessoas individuais àquele tiveram acesso ou qual uso dele foi feito.

A denúncia realizada pelos canais de jornalismo cuida de fatos inseridos em um contexto de protestos e manifestações políticas contra atos e discursos do governo de então. Essa situação traz preocupação com monitoramento e eventual restrição ou abalamento do direito à liberdade de expressão, à privacidade e à proteção de dados dos sujeitos monitorados, com ameaça, ainda, ao próprio sistema democrático. Destaca-se que toda a ação foi realizada sem qualquer controle judicial.

A questão do compartilhamento de dados sem transparência para fins de inteligência e segurança nacional deve, então, ser enfrentada. A falta de informação sobre como se dá a cooperação e o trânsito de informações entre as instâncias de inteligência acarreta muitas incertezas sobre o real respeito aos direitos fundamentais.

A Política Nacional de Inteligência (PNI) é disciplinada pelo Decreto nº 8.793, de 29 de junho de 2016, e visa a definir os parâmetros e os limites de atuação da atividade de inteligência e de seus executores no âmbito do Sistema Brasileiro de Inteligência.

A Política é fixada pelo Presidente da República e define os parâmetros e limites de atuação da atividade de Inteligência e de seus executores. Considera-se atividade de inteligência o exercício permanente de ações especializadas, voltadas para a produção e difusão de conhecimento, com vistas ao assessoramento das autoridades governamentais nos respectivos níveis e áreas de atribuição, para o planejamento, a execução, o acompanhamento e a avaliação das políticas de Estado.

---

[100] Disponível em: https://www1.folha.uol.com.br/poder/2020/07/acao-sigilosa-do-governo-mira-professores-e-policiais-antifascistas.shtml. Acesso em: 20 de novembro de 2023.

A PNI é uma atividade permanente e exclusiva do Estado e estabelece, ainda, pressupostos, objetivos, instrumentos e diretrizes da atividade de inteligência, no âmbito do Sistema Brasileiro de Inteligência (SISBIN).

O SISBIN é um dos instrumentos da Inteligência nacional e foi instituído pela Lei nº 9.883, de 07 de dezembro de 1999 e organizado pelo Decreto nº11.693/2023. No artigo 1º da lei, determina-se que o SISBIN integra as ações de planejamento e execução das atividades de inteligência do país, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional. O Sistema é formado por todos os órgãos e entidades da Administração Pública Federal que, direta ou indiretamente, possam produzir conhecimentos de interesse das atividades de inteligência, em especial aqueles responsáveis pela defesa externa, segurança interna e relações exteriores.

Dentre os poderes do órgão central do SISBIN está o de requerer aos órgãos e às entidades do Poder Executivo federal integrantes do SISBIN "dados, informações, conhecimentos ou documentos necessários ao atendimento aos planos de trabalho estabelecidos, observados o interesse público e a devida motivação (art. 10, VII, Decreto 11.693/2023). Os demais órgãos e entidades que compõem o sistema também poderão "solicitar, obter, processar, produzir e compartilhar dados, informações e conhecimentos em conformidade com a Política Nacional de Inteligência, com os planos de trabalho e com o disposto na legislação" (art. 11, II). Ampla, portanto, a possibilidade de compartilhamento de dados.

A Lei em referência cria, além do Sistema Brasileiro de Inteligência – SISBIN, a Agência Brasileira de Inteligência – ABIN, órgão da Presidência da República central do SISBIN. À ABIN compete: (i) planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República; (ii) planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade; (iii) avaliar as ameaças, internas e externas, à ordem constitucional e (iv) promover o desenvolvimento de recursos humanos e da doutrina de inteligência, e realizar estudos e pesquisas para o exercício e aprimoramento da atividade de inteligência.

Nos termos do parágrafo único do artigo 4º da Lei nº 9.883/1999, em texto que interessa ao ponto abordado neste trabalho, estabelece-se que os órgãos componentes do Sistema Brasileiro de Inteligência devem fornecer à ABIN dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais.

Na prática, a ABIN tinha acesso, por meio de compartilhamento, a um amplo leque de informações e dados, inclusive aqueles a princípio protegidos pelo sigilo das comunicações, apesar de a agência não possuir competência para a quebra do sigilo constitucionalmente posto.

Esse quadro foi evidenciado em caso polêmico em que agentes da ABIN tiveram acesso ao conteúdo de interceptações telefônicas contidas no Guardião, sistema da Polícia Federal que armazena interceptações telefônicas[101]. O fato ocorreu no bojo da "Operação Satiagraha", desencadeada em 2004 para investigação de desvio de verbas públicas, corrupção e lavagem de dinheiro e na qual foi autorizada a interceptação de diálogos telefônicos.

Policiais da Operação repassaram a agentes de inteligência da ABIN duas senhas que deram acesso aos diálogos interceptados. Houve controvérsia quanto à possibilidade ou não desse acesso. No caso, o Ministério Público Federal de São Paulo entendeu não haver ilegalidade no compartilhamento de informações com servidores públicos da Inteligência, abrindo debate sobre o tema.

Observa-se, pois, que era bastante flexível o trânsito de informações entre os diversos órgãos componentes do Sistema, sendo de relevo notar a preocupação na redação do novo Decreto (11.693) em ressaltar a necessidade de demonstração do interesse público e da motivação para o compartilhamento das informações entre aqueles (art. 10, III).

Essa redação não existia no anterior Decreto e o novo segue linha da jurisprudência fixada pelo Supremo Tribunal Federal no julgamento da ADI nº 6529[102] no ano 2021. A ação foi ajuizada pelo Partido Sustentabilidade e pelo partido Socialista Brasileiro questionando os extensos poderes da ABIN para acessar documentos e gravações. O pedido foi julgado parcialmente procedente para dar interpretação conforme ao parágrafo único do artigo 4º, da Lei nº 9.883/1999, e fixar condições para o compartilhamento de informações entre os órgãos de inteligência, nos seguintes termos:

> "a) os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados;
>
> b) toda e qualquer decisão de fornecimento desses dados deverá ser devida e formalmente motivada para eventual controle de legalidade pelo Poder Judiciário;

---

[101] FOLHA DE SÃO PAULO. **Acesso ao Guardião da PF pela Abin gera polêmica**. Disponível em: https://www1.folha.uol.com.br/fsp/brasil/fc1211200805.htm. Acesso em: 20 de novembro de 2023.

[102] SUPREMO TRIBUNAL FEDERAL. ADI nº 6529. Relatora Ministra Cármen Lúcia. Julgamento em 11 de outubro de 2021. DJE nº217/2021 e DOU nº 208/2021. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15348384228&ext=.pdf. Acesso em: 20 de novembro de 2023.

> c) mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo, em razão daquela limitação, decorrente do respeito aos direitos fundamentais;
>
> d) nas hipóteses cabíveis de fornecimento de informações e dados à ABIN, são imprescindíveis procedimento formalmente instaurado e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização em caso de eventual omissão, desvio ou abuso (...)." (Grifo nosso)

Da jurisprudência fixada pela Corte, tem-se que, todas as normas que tratem de compartilhamento de informações entre órgãos e entidades da Administração Pública entre si ou com entidades privadas autorizadas a tanto, inseridos ou não no Sistema de Inteligência do país, devem obedecer aos requisitos ali postos, permitindo conhecimento público e controle judicial da medida.

Não há presunção de atendimento de interesse e finalidade pública, adequação e proporcionalidade pelo só fato de comporem a esfera da segurança pública, sendo imperativo o esforço das diversas instâncias para demonstrar que as bases legais que autorizam a coleta e processamento de dados dos cidadãos estão adequadamente atendidas.

É preciso um forte controle social, político e jurídico, dos usos de sistemas que permitem a vigilância dos indivíduos e seu perfilhamento, como demonstrado no exemplo apontado neste tópico. A possibilidade de alargamento das hipóteses em que dados pessoais são coletados e tratados traz riscos individuais e coletivos em médio e longo prazos.

A possibilidade de acesso a dados de localização e deslocamento, como a permitida por meio do córtex e seu monitoramento de placas de veículos dá extenso Poder ao Estado, que poderá saber não só onde encontrar o indivíduo, mas informações associadas aos locais que frequenta. A partir de dados de geolocalização é possível saber que religião o indivíduo professa, seu estado de saúde, os grupos com os quais se afina ideologicamente, preferências pessoais, todos dados sensíveis e relacionados à esfera privada do sujeito.

Essa esfera privada, propõe-se, ainda, deve ser lida não apenas como um interesse puramente individual do sujeito titular dos dados, representando antes condição para que a pessoa não seja submetida a controle que anularia a sua individualidade e ameaçaria toda a organização social ao seu redor. Nesse sentido, lição de Danilo Doneda que, por extremamente relevante, reproduz-se:

> "A trajetória percorrida pelo direito à privacidade reflete tanto uma mudança de perspectiva para a tutela da pessoa quanto sua adequação às novas tecnologias da informação. Não basta pensar a privacidade nos moldes de um direito subjetivo, a ser tutelado conforme as conveniências individuais, nem da privacidade como uma 'predileção' individual, associada basicamente ao conforto e comodidade. (...) Uma esfera privada, na qual a pessoa tenha condições de desenvolvimento da própria

> personalidade, livre de ingerências externas, ganha hoje ainda mais em importância: passa a ser um pressuposto para que ela não seja submetida a formas de controle social que, em última análise, anulariam sua individualidade, cerceariam sua autonomia privada e, em última análise, inviabilizariam o livre desenvolvimento da sua personalidade. A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento positivo, indutor da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Neste papel, a vemos como pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos."[103]

O modelo usado em nível nacional se repete nos Estados. No Estado do Ceará, a Secretaria de Segurança Pública e Defesa Social (SSPDS) apresentou uma série de sistemas que visam a fazer monitoramento de deslocamentos e combinação de informações com outras contidas em diversas bases de dados, nos moldes do modelo federal[104].

Entre as ferramentas de videomonitoramento integradas ao uso de inteligência artificial estão: Plataforma "Big Data", que usa mais de 60 fontes de dados relacionadas à segurança pública para auxílio em abordagens policiais; Projeto "Cerebrum", que busca informações de forma integrada para uso no trabalho policial; "Crime Watcher", extrator de dados que utiliza técnicas de inteligência artificial; "Agilis", que subsidia trabalhos de equipes policiais por meio de captura de dados; "Spia (Sistema Policial Indicativo de Abordagem)" e "NUVID (Núcleo de Videomonitoramento)".

O objetivo de todos os programas, segundo a SSPDS é "combater a criminalidade, seja por meio de abordagens de suspeitos com mandados em aberto a partir das informações, ou por meio de cercos inteligentes".

A Secretaria não detalha, porém, o procedimento utilizado em cada projeto e sistema mencionados. Diante da falta de informações precisas foi enviado ofício à SSPDS no dia 23 de outubro de 2023 (atendimento 6608048). Ali, foram solicitadas as seguintes informações:

> 1. Quais as bases de dados consultadas pela Secretaria por meio da Plataforma Big Data e para uso nos programas Cerebrum, Crime Watcher, Agilis, Spia e NUVID?
> 2. Quais dados dos cidadãos são utilizados para avaliação das ações executadas nos programas indicados no item 1?
> 3. Por quais meios o cidadão pode acessar o procedimento para tratamento de seus dados?

---

[103] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Renovar: Rio de Janeiro, 2006, pp. 141-142. grifos nossos.

[104] Disponível em: https://www.sspds.ce.gov.br/2021/10/28/sspds-apresenta-ferramentas-tecnologicas-durante-visita-de-comitiva-do-mato-grosso/. Acesso em 20 de novembro de 2023.

> 4. Por quais meios o cidadão pode solicitar revisão dos resultados indicados por meio do tratamento dos seus dados?
> 5. Por quais meios o cidadão pode requerer retificação de informações ou exclusão de dados utilizados pelo órgão nos projetos indicados?

A solicitação foi feita com base na Lei de Acesso à Informação e na prerrogativa de requisição de documentos e informações conferida aos membros da Defensoria Pública no Estado do Ceará (art. 64, IV, LC 06/97).

Em 23 de novembro de 2023, foi encaminhado e-mail resposta pela Secretaria com informação de que o atendimento do pedido já se encontrava com 15 (quinze) dias de atraso.

Tomados os casos mencionados, é importante que se destaque que, conquanto seja complexo o equilíbrio entre segurança e privacidade, não se pode permitir a construção de um estado de vigilância sobre todos os cidadãos sem acesso a informações e garantias mínimas de respeito aos direitos individuais constitucionalmente previstos. Para além da invasão à esfera privada dos sujeitos e desrespeito ao seu direito à proteção de dados, à autodeterminação informativa e ao livre desenvolvimento de personalidade, alcançados como luta histórica e desenhados nas primeiras linhas deste trabalho, cuida-se dos contornos de uma sociedade, a qual, com grande esforço, vem mantendo o *status* de democrática, inclusiva e promotora de direitos humanos.

No plano abstrato, privacidade, proteção de dados e segurança estão em um mesmo plano axiológico; o intérprete e o aplicador da norma deverão exercer o juízo de proporcionalidade necessário para garantir a coexistência harmoniosa de todos os interesses.

O valor segurança, porém, não pode fazer com que tenhamos "homens de vidro sob vigilância permanente e universal quanto a seus dados, seu comportamento, suas comunicações, suas escolhas, e até mesmo quanto ao seu próprio corpo, no tocante às informações biométricas."[105]

Importante nesta seara serão também os princípios norteadores da ação do Estado expressos na Lei Geral de Proteção de Dados Pessoais, nomeadamente finalidade, necessidade, adequação, livre acesso e transparência. Estes princípios possuem tamanha envergadura que

[105] MENEZES, Joyceane Bezerra de e COLAÇO, Hian Silva. Quando a Lei Geral de Proteção de Dados não se aplica? **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p. 164.

não foram afastados nem mesmo quando se cuida do exercício, pelo Estado, de funções inerentes à segurança do Estado, defesa nacional, segurança pública, investigação e repressão de infrações penais.

Por fim, deve-se registrar que todo o manancial de monitoramento deve ser informado a todos e que o acesso a informações de interesse particular do cidadão e de interesse coletivo ou geral é assegurado constitucionalmente como direito fundamental no artigo 5º, inciso XXXIII, da Constituição da República, onde se lê: "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."

O direito a informação possui a mesma relevância e *status* jurídico de outros como privacidade e proteção de dados pessoais. É, de igual modo, reforçado pelo inciso II, §3°, do artigo 37 da Constituição, que assegura "o acesso dos usuários a registros administrativos e a informações sobre atos de governo".

Nesse contexto, importante faz-se algumas considerações acerca da Lei de Acesso à Informação (Lei n° 12.527/2011). Inicialmente, o diploma normativo define o sigilo como exceção e a publicidade como regra. É o que se extrai das diretrizes arroladas no artigo 3° da Lei: (i) observância da publicidade como preceito geral e do sigilo como exceção; (ii) divulgação de informações de interesse público, independentemente de solicitações; (iii) utilização de meios de comunicação viabilizados pela tecnologia da informação; (iv) fomento ao desenvolvimento da cultura de transparência na administração pública e (v) desenvolvimento do controle social da administração pública.

Sendo a regra a transparência, as exceções precisam ser devidamente motivadas. Isso decorre da necessidade de se permitir o adequado controle social da Administração Pública, o qual somente poderá ser exercitado se houver conhecimento acerca dos atos e motivações que regem a atividade estatal.

Quando confrontada com a Lei Geral de Proteção de Dados, pode-se entender haver um certo choque entre publicidade e privacidade. Este, porém, é apenas um conflito aparente, conforme esclarecido anteriormente quando analisados os princípios que disciplinam a proteção de dados no regime jurídico constitucional brasileiro. Tanto a LGPD quanto a LAI cuidam também, em última instância, do atendimento do interesse público que se legitima e

concretiza não como uma coletivização abstrata, mas no cuidado com a aplicação harmônica de todas as categorias de direitos fundamentais.

Caberá, pois, aos agentes estatais a ponderação dos valores em jogo para garantir sua aplicação e convivência de forma congruente e atendendo aos fins maiores de uma sociedade livre, justa e democrática, nos termos preconizados pela Lei Fundamental brasileira.

Nessa perspectiva, traz-se os importantes apontamentos de Daniel Solove a respeito da privacidade em tempos de crise. Para ele, existe uma falsa dicotomia entre segurança e privacidade, como se ambos os valores fossem mutuamente excludentes. Assim, o autor critica o que chama de "argumento do pêndulo", segundo o qual, em tempos de crise, o pêndulo deve pender para o sacrifício de direitos, os quais devem ser retomados quando o pêndulo balança e se encontra em período de "normalidade". O autor destaca que tempos de crise não conferem carta branca para malferimento à Constituição.

Nesse contexto, continua, "sacrifícios de direitos e liberdades civis devem ser feitos somente quando o governo justifica adequadamente por que esses sacríficos são necessários. É preciso submeter tais restrições a um escrutínio meticuloso, especialmente porque, em tempos de crise, o medo distorce nosso julgamento"[106].

O argumento desenvolvido pelo autor põe em realce a relevância dos direitos e liberdades civis, os quais devem ser ainda mais protegidos em tempos de crise, quando estão sob ameaça e quando os indivíduos mais deles precisam. Assim, a aparente tensão entre segurança e privacidade deve ser alocada em termos adequados.

4.3 Discriminação algorítmica e grupos vulneráveis

Aspecto relevante a ser observado diz respeito à aplicação da inteligência artificial, incluindo sua aplicação em tecnologias biométricas, para reconhecimento e categorização de indivíduos. Embora essa identificação possa trazer efeitos práticos positivos para fins mercadológicos ou de segurança pública, é certo que carrega aspectos problemáticos no que tange a políticas de vigilância social, a proteção de dados pessoais e amparo da privacidade e a disseminação de preconceitos e discriminação de determinados grupos particularmente vulneráveis.

Relativamente a este último ponto, sobressaem preocupações referentes ao tratamento menos favorável a determinados indivíduos ou grupos em razão de enviesamento de

[106] SOLOVE, Daniel J. **Nothing to hide**: The false tradeoff between privacy and security. Yale University Press, 2011, p. 61.

dados ou falhas de identificação que reforçam preconceitos e discriminação contra coletividades em vulnerabilidade. Preconceitos de gênero e raça são especialmente documentados, demonstrando que mulheres, negros e pessoas pertencentes a grupos LGBTQIAPN+ são em maior parte afetados pelo tratamento de dados realizado pelo Poder Público ou por agentes que atuam em parceria ou em substituição àquele, merecendo especial atenção e cuidado por parte da esfera estatal.

A vulnerabilidade decorrente da aplicação de tecnologias de identificação e categorização refletem uma conformação social que, historicamente, marginaliza e exclui indivíduos pertencentes a esses grupos, o que demanda um esforço adicional a fim de serem expurgados vieses e falhas de identificação que potencializa a vulnerabilidade.

Em certa medida, a legislação dá um passo nesse sentido, ao prever, no que tange à proteção de dados pessoais, a natureza particularmente relevante dos dados que os identifica, enquadrando-os como dados sensíveis, com especial proteção normativa.

Veja-se que o artigo 5º, II, da LGPD, define como dado sensível aquele pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Assim, elementos relacionados a gênero e raça encontram-se expressamente previstos, merecendo tratamento diferenciado pelos agentes manipuladores de dados. Outrossim, a LGPD enumera como princípio expresso o da não-discriminação, identificando-o como a impossibilidade de realização de tratamento para fins discriminatórios ilícitos ou abusivos.

É preciso que se reconheça, contudo, que, apesar da previsão normativa, estudos empíricos têm demonstrado que esses grupos estão entre as maiores vítimas de procedimentos incorretos que recorrem ao uso da tecnologia, demandando um enfretamento mais robusto da matéria.

Na problematização da questão, parte-se de alguns casos reportados ao público.

4.3.1 Discriminação de raça

Dados e algoritmos têm sido usados no sistema de justiça há quase um século, havendo registros dos primeiros usos ainda da década de 1920. Hannah Fry[107] relembra que Ernest W. Burgess, sociólogo canadense da universidade de Chicago, foi um defensor da

[107] FRY, Hannah. **Hello World**: How to Be Human in the Age of the Machine. Random House, 2018. *E-book*.

quantificação de fenômenos sociais e, em 1928, construiu uma ferramenta para prever o risco de comportamento criminoso com base em medição de dados objetivos, não em intuição. Entre os dados, incluiu-se tipo de crime, tempo de prisão, tipo social do recluso – bêbado, imigrante etc.

Burgess elegeu 21 fatores de análise aos quais correspondia uma numeração. A depender da pontuação obtida, analisava-se a propensão ou não à reincidência. Após acompanhamento de um grupo de estudo, verificou-se um resultado notavelmente preciso. Em tempos modernos, esse modelo inspirou o desenvolvimento de ferramentas tecnológicas que usam mecanismos sofisticados de avaliação de risco por meio de algoritmos. Avançando em seu uso, referidos programas hodiernamente auxiliam os juízes também no processo de tomada de decisão sobre condenações.

Em 2017, um grupo de pesquisadores resolveu testar o quanto as previsões matemáticas seriam acuradas, analisando casos reais que foram julgados ao longo de 5 anos na cidade de Nova Iorque. O resultado mostrou que o algoritmo conseguiu alto índice de conformação da realidade à sua previsão: do grupo de risco apontado, mais de 56% não compareceu às audiências no tribunal e 62,7% cometeram novos crimes. Os pesquisadores aduziram que seus resultados seriam melhores que a avaliação de qualquer juiz.

O algoritmo passou a ser utilizado não apenas para análise de risco de reincidência criminosa, mas também para subsidiar juízes em suas decisões sobre condenação e dosimetria de pena. Ocorre que, ao lado do grande percentual de acurácia, existe um número significativo de potencial erro – em média um de cada 3 resultados indicariam falsos negativos ou falsos positivos. Falsos negativos acontecem quando existe falha na identificação do risco de um indivíduo. Falsos positivos ocorrem quando o algoritmo incorretamente identifica uma pessoa como portadora de risco.

O instituto Propublica, organização americana independente e sem fins lucrativos, que produz jornalismo investigativo, expôs, em 2016, preconceitos raciais nos resultados obtidos por meio do programa COMPAS, utilizado nos Estados Unidos para predizer o risco de reincidência delitiva de um indivíduo[108]. A pesquisa mostrou que réus negros estavam mais suscetíveis que réus brancos de serem incorretamente julgados com maior risco de reincidência.

O COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) é um sistema de inteligência artificial que visa a fazer previsões de comportamentos a partir da captação de informações do infrator. Essa coleta pode ser feita por meios diversos:

[108] PROPUBLICA. Disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm . Acesso em 30 de junho de 2022.

preenchimento de formulário, entrevista guiada ou discussão guiada. Uma análise de eficácia do COMPAS mostrou que infratores afro-americanos tinham 77% mais chances de serem classificados com grande risco de reincidência do que infratores brancos.

Na avaliação feita pelo COMPAS, a pontuação, que revela a chance de reincidência, é dada conforme respostas a perguntas pré-definidas, que procuram saber dados objetivos e opiniões do sujeito analisado.

O Instituto ProPublica publicou o questionário de risco[109] formado por 137 perguntas utilizadas pelo sistema Northpoint, empregado para análise de risco na Flórida. Estas dizem respeito ao contexto do delito, ao histórico criminal do indivíduo, ao histórico de sua família (inclusive criminal) e de seus amigos, possível abuso de substâncias, ambiente social histórico escolar e profissional, recreação e ideias ou opiniões sobre crimes.

Não se sabe, porém, como a pontuação é atribuída a cada uma dessas respostas, o que tona difícil ao indivíduo questionar o resultado. Ademais, não há literatura que indique haver, por parte dos juízes, postura de independência em relação ao resultado apresentado pelo sistema, havendo, antes, uma confirmação da conclusão apresentada.

Caso emblemático ocorreu no condado de Barron, em Wiscoconsin[110]. Paul Zilly foi processado por furtar um cortador de grama e algumas ferramentas. Analisando seu caso, o promotor recomendou um ano de prisão no condado e acompanhamento a fim de que Zilly "permanecesse no caminho certo". O acordo judicial apresentado pelo órgão persecutor foi aceito pelo advogado de defesa e pelo réu.

Contudo, o juiz do caso, James Babler, analisou o questionário e a pontuação do de Zilly. O software da Northponit o classificou como portador de alto risco de prática de crimes violentos no futuro e, em médio prazo, risco de reincidência geral. Diante do resultado, o juiz recusou o acordo judicial firmado pelas partes e condenou o réu a dois anos de prisão estadual e três anos sob supervisão.

É possível que Babler tenha atuado sob influência do chamado "mito da neutralidade" das máquinas. Hugo de Brito Machado Segundo explica o conceito como a presunção de que os algoritmos, no desempenho de tarefas que envolvem seleções, escolhas e

---

[109] PROPUBLICA. **Risk Assessment**. Disponível em: https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html. Acesso em 20 de novembro de 2023.

[110] PROPUBLICA. **Machine Bia**s: there's software udes across the country to predict future criminals. And it's biased against black. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em: 20 de novembro de 2023.

julgamentos serão neutras por definição. Isso, adverte, é um erro, pois, "se dos dados dos quais partirem forem enviesados, os resultados possivelmente também o serão."[111]

Existe de modo disseminado ima ideia de que as tecnologias são infalíveis e objetivas por terem uma precisão matemática, sem erros ou preconceitos por parte dos programadores que calibram as máquinas. Ocorre que estas são projetadas e operadas por pessoas que ali refletem suas visões, muitas vezes enviesadas. Os processos históricos e culturais invariavelmente acabam refletidos na programação que se faz dos sistemas, comprometendo a imparcialidade e objetividade que delas se espera.

No caso concreto mencionado, o questionário usado para a análise preditiva, como pode ser observado nas perguntas elaboradas, cuida de condições que são historicamente desfavoráveis a um determinado grupo étnico e racial. Historicamente, negros estão submetidos a muitas barreiras raciais. O nível educacional, a inserção profissional e as condições econômicas são largamente inferiores em razão de processos históricos que os colocam à margem.

Simone Browne[112] mostra, ainda, como tecnologias e práticas de vigilância contemporâneas são informadas pela longa história da formação racial e pelos métodos de policiamento da vida negra desde os tempos da escravidão. A autora destaca também a existência de sistemas biométricos específicos que privilegiam a branquitude e mostram com quais corpos as tecnologias são projetadas para funcionar melhor.

Os estudos aqui elencados preteritamente, que dizem respeito a sistemas de reconhecimento facial e sua acurácia diante de peles brancas ou negras, é um claro exemplo da abordagem de Browne. A falta de precisão na identificação de rostos gera uma gama de falsos positivos, especialmente agravados quando ocorrem no contexto da segurança pública.

Mais do que números, percentuais de acerto e acurácia, deve-se tomar nota que os números indicam apenas uma probabilidade, mas não determinam o que de fato ocorrerá no futuro. Uma pessoa classificada como indivíduo com grande risco de reincidência nem sempre tornará a praticar crimes. O comportamento humano é imprevisível, mas as consequências negativas da perda de uma oportunidade, da taxação social e enquadramento em grupos marginalizados são visíveis.

---

[111] MACHADO SEGUNDO, Hugo de Brito. **Direito e inteligência artificial**: o que os algoritmos têm a ensinar sobre interpretação, valores e justiça. 2.ed. São Paulo: Editora Foco, 2023, p. 16.
[112] BROWNE, Simone. **Dark Matters**: on the surveillance of blackness. Durham an London: Duke University Press, 2015, p. 111.

4.3.2 Discriminação de gênero

As tecnologias reproduzem as formas de organização social do mundo real. Assim, em uma sociedade em que determinados grupos são discriminados e subalternizados, também o mundo construído tecnologicamente será atingido. Esse é o ponto de partida dos estudos de Safyia Noble[113], que, analisando motores de busca nos meios de comunicação, demonstra a misoginia, sexismo e racismo reproduzidos em suas sugestões. Um dos pontos centrais da autora é abordar como resultados fornecidos pelos sítios de busca podem ter efeitos deletérios quando não há construção que filtre os preconceitos e enviesamentos daqueles que os manipulam.

Essa ausência de filtros leva a que resultados e informações equivocadas ganhem destaque e espalhem desinformação, criando vieses e associações que não encontram respaldo numa análise racional. Sobre o tema, veja-se trecho preciso de George Marmelstein:

> "(...) as pessoas tendem a fazer associações automáticas entre homens negros, criminalidade, armas, ameaças, raiva, força e violência. Essas associações automáticas são ativadas de modo inconsciente e não intencional, podendo gerar falhas de percepção com sérias consequências na vida real. É possível, por exemplo, que uma testemunha interprete um comportamento de uma pessoa negra como mais ameaçadora ou confunda um objeto inofensivo com uma arma apenas por estar nas mãos de uma pessoa negra."[114]

Essa é também uma afirmação de Meredith Brounard[115]. Segundo a pesquisadora, todos possuem vieses inconscientes e os espelham na tecnologia; se os modelos de aprendizagem automática simplesmente replicarem o mundo tal como é, não se avançará rumo a uma sociedade mais justa. O fato de haver reflexo, nos sistemas criados, da forma de organização social no mundo real faz com que essas ferramentas tenham a cara de quem as projeta. A questão que se põe é que, em se tratando de tecnologia, grupos são historicamente excluídos do processo de criação.

Brounard[116] destaca como a ausência de mulheres em posições relevantes nas empresas de tecnologia compromete sua representatividade no setor. Dado que o verdadeiro

---

[113] NOBLE, Safyia Umoja. **Algorithms of Opression**: how search engines reinforce racism. New York: New YorK University Press, 2018, p.116.
[114] MARMELSTEIN, George. **Testemunhando a injustiça**: a ciência da prova testemunhal e das injustiças inconscientes. São Paulo: Editora Juspodivm, 2022, p. 48.
[115] BROUSSARD, Meredith. **Artificial unintelligence**: how computers misunderstand the world. London: The MIT Press, 2018, p. 116.
[116] *Op. cit.*, p.158.

poder pertence aos desenvolvedores e engenheiros, galgando elas postos significativos apenas em outras áreas (como marketing e recursos humanos), estariam à margem do poder de influência nos sistemas tecnológicos.

Questão semelhante atinge o grupo minoritário formado por pessoas trans – transexuais e travestis. Essa população possui luta histórica pela garantia de cidadania e reconhecimento de sua identidade social. Considerando que a identidade revela as características pessoais, é importante que o Estado identifique a forma como o sujeito se reconhece, abarcando as inúmeras identidades que podem ser construídas na complexa teia humana. Não reconhecer uma identidade é invisibilizar a pessoa, desconsiderando-a como sujeito de direitos a quem o Estado deve proteger.

Na construção da identidade individual, diversos elementos estão inseridos, entres os quais o nome, o gênero e a possibilidade de autodeterminação de um e de outro pelo sujeito, além da construção de sua própria imagem física. Essa autodeterminação somente recentemente foi reconhecida no âmbito nacional. Em 2018, o Supremo Tribunal Federal declarou, na ADI n° 4275, ser possível a alteração de nome e gênero no assento de registro civil mesmo sem a realização de procedimento cirúrgico de redesignação de sexo e sem autorização judicial.

Esse foi momento marcante para os movimentos promotores dos direitos civis, que lutam contra a discriminação e a marginalização de grupos minoritários. Em seguida, outros direitos civis foram também reconhecidos, como a possibilidade de adoção por pessoas LGBTQIAPN+ e a criminalização da LGBTfobia.

Contudo, as decisões judiciais significam apenas mais um passo no longo caminho para a naturalização da existência de toda a diversidade humana e da sua consideração nos muitos aspectos da vida estatal.

Obstáculo moderno consiste no reconhecimento da sua identidade social frente a novas tecnologias, em especial aos sistemas de reconhecimento facial. Estes trabalham sob uma lógica binária, que distingue entre os gêneros masculino e feminino, confrontando-o com outras bases que depositam nomes e informação gênero, capazes de levar a comunidade trans à invisibilidade. Estudo apontou que a taxa média de acertos de reconhecimento facial em mulheres trans é de 87,3%; em mulheres cis a precisão foi de 98,3%; em homens cisgênero, o índice foi de 97,6% de acurácia e em homens trans de 70,5%. Esse alto número de erro em

relação a pessoas transgênero pode ser explicado pela falta de representatividade nas bases de dados que fomentam sistemas, o que causa a exclusão dessa camada da população[117].

O rótulo homem-mulher com características definidas *a priori* não cabe mais no atual estágio de desenvolvimento humano e de organização jurídica. É importante, pois, que esses sistemas sejam adequados a fim de abranger todas as identidades de gênero, desconsiderando a dualidade tradicionalmente aplicada.

Questão relevante que também se coloca diz respeito aos riscos decorrentes da possibilidade de identificação e monitoramento de pessoas trans enquanto categoria social estigmatizada. Como demonstrado alhures, o Estado dispõe, e efetivamente utiliza, ferramentas que propiciam perfilhamento de indivíduos e de seus grupos a partir do cruzamento de bases de dados diversas.

Esse potencial de perfilhamento e vigilância do Estado gera natural preocupação a grupos minoritários consagradamente perseguidos. Dossiê sobre assassinatos e violência contra pessoas trans realizado em 2022[118] pela Associação Nacional de Travestis e Transexuais (ANTRA) mostra dados alarmantes. Naquele ano, houve o assassinato de pelo menos 131 pessoas trans – 130 travestis e mulheres transexuais e 1 homem trans. Esse número coloca o Brasil na liderança dos países que mais matam pessoas trans no mundo.

76% dessas mortes foram de pessoas trans negras (pretas e pardas), o que mostra que a população negra tem mais chances de ser assassinada. A abordagem interseccional, portanto, é importante, trazendo proteção completa aos grupos hipervulneráveis.

No dossiê ainda se reportam subnotificações de casos por falta de controle governamental, ausência de ações de enfrentamento à violência contra pessoas LGBTQIAPN+ e aumento de iniciativas que visam a institucionalizar a transfobia.

Do contexto exposto, uma primeira preocupação, de ordem técnica, exige enfrentamento: a adaptação dos sistemas para reconhecimento com precisão de mulheres e pessoas trans, respeitando a identidade social de todas elas.

---

[117] UOL. **Inteligência Artificial**: além do racismo, reconhecimento facial erra mais em pessoas trans. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/02/14/nao-e-so-racismo-reconhecimento-facial-tambem-erra-mais-em-pessoas-trans.htm. Acesso em: 20 de novembro de 2023.

[118] Associação Nacional de Travestis e Transexuais (ANTRA). Dossiê Assassinatos e Violências contra Travestis e Transexuais em 2022. Disponível em: https://antrabrasil.files.wordpress.com/2023/01/dossieantra2023.pdf. Acesso em: 20 de novembro de 2023.

Ao lado desse desafio, é fundamental que se reconheça o risco agravado sofrido por mulheres e pessoas trans em razão de misoginia, transfobia e estigmatização. Com essa constatação, maiores cautelas devem ser tomadas quando se cuida de perfilhamento e distinção de grupos sociais, dada a possibilidade de perseguições e mais graves restrições de direitos dos dois grupos sociais.

Outras sugestões são trazidas pela professora Fernanda Lage, para quem a modificação desse cenário impõe a criação de padrões de testes, tanto em termos da qualidade dos dados confiados quanto na detecção de viés. Deve-se, ademais, buscar um compromisso de reexaminar as políticas e incentivos existentes nas empresas de tecnologia, para atrair mais mulheres e acelerar a taxa de mudança.[119]

[119] LAGE, Fernanda de Carvalho. **Manual de inteligência artificial no direito brasileiro**. 2.ed. rev., atual e ampl. São Paulo: Editora Juspodivm, 2022, p. 140.

5. PROPOSTAS DE REGULAÇÃO ADEQUADA DO USO DE DADOS PESSOAIS NA SEGURANÇA PÚBLICA

A dinâmica social exige constante renovação da forma como o Estado cuida da segurança pública, trabalhando na prevenção e na repressão de ações delituosas, sejam estas referentes à segurança interna ou à defesa nacional. Nesse processo, o uso de ferramentas tecnológicas, que se tornam cada vez mais sofisticadas, podem – e de fato assim se mostram – ser grandes aliadas, aumentando a eficiência com que o combate ao crime é realizado.

No exercício da importante função de proteção do seio social, nem toda ação é permitida, porém. A necessidade de respeito aos direitos e liberdades individuais põe freio à ação estatal, trazendo como desafio o equilíbrio entre valores importantes, para que o nobre fim de garantia de segurança e paz social não venha atrelado a sacrifícios individuais (e coletivos) desarrazoados.

Importante instrumento inserido nas ações do Estado para execução da política de segurança pública foi, como demonstrado, a inteligência artificial para uso de dados pessoais, com o fim de realizar identificação e controle dos indivíduos que transitam sob a mira estatal. Ocorre que esse monitoramento e repressão nem sempre atingem os alvos corretos, havendo indevida invasão na esfera privada de terceiros; ou, quando os atingem, podem vir acompanhados de desequilíbrio no sacrifício de direito do próprio agente delituoso, por um excesso de ação.

Algumas vezes a questão que se põe não diz respeito a erro de identificação de alvos ou de dosagem punitiva, mas à vigilância a que todo o espectro social resta sujeito com vistas a um resultado ótimo da política de combate ao delito. Esta, por sua vez, pode, com ou sem gestão propositalmente maliciosa, mostrar-se ainda mais nociva para a coletividade do que a tolerância ao convívio com o delito, como apurado em linhas anteriores.

Se a coletividade se acha, de modo geral, exposta em todo esse processo, é certo que alguns grupos sociais bem definidos restam mais vulnerabilizados, por questões históricas e culturais que perpetuam extenso desequilíbrio de poder social.

Diante desse contexto, propõe-se uma reflexão sobre os problemas causados pelo uso de dados pessoais para exercício do poder do Estado na segurança pública e na persecução penal. A partir dessa ponderação, pode-se ter uma visão ampla que permita a elaboração de instrumentos adequados de regulação da coleta, tratamento, uso, guarda e compartilhamento

dos dados pessoais, com menor sacrifício de direitos fundamentais consagrados e a grupos sociais específicos.

Para atingimento desse fim, trazem-se as propostas a seguir.

5.1 Aplicação adequada do direito fundamental à proteção de dados pessoais

A inserção da proteção de dados no rol de direitos fundamentais revela a força que se quis dar à sua realização. Como direito fundamental autônomo, não é subordinado a nenhum outro e, em caso de interseção de contexto de aplicabilidade com outros direitos também garantidos constitucionalmente, deve ser feito o sopesamento com base nos critérios estipulados para tanto na Constituição.

Como norma constitucional, deverá sempre ser interpretada de forma a dar a maior concretude possível ao valor que lhe é subjacente, realizando o que Konrad Hesse cunha de força normativa da Constituição[120]. No processo de garantir sua estabilidade e efetividade, as normas devem ser interpretadas adequando-se às alterações do mundo real, embora sem perder seu conteúdo essencial. Essa postura revela a vontade de constituição e de realização dos valores que nela estão inscritos, por pressuposto espelhados na vontade social.

5.2 Aplicação efetiva dos princípios da proteção de dados pessoais expostos em legislação específica

Segundo Miguel Reale[121], princípios são "verdades ou juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízos, ordenados em um sistema de conceitos relativos a dada porção da realidade".

Os princípios são o lugar que sempre se deve ter em vista no momento da interpretação e da aplicação das normas diversas por juristas e cidadãos em geral.

A Lei Geral de Proteção de Dados (LGPD) enumera, no artigo 6º, dez princípios fundamentais, os quais devem ser aplicados mesmo nas hipóteses de exceção de aplicação da Lei – casos de segurança pública, defesa nacional, segurança do Estado e atividade de investigação e repressão de infrações penais (art. 4º, III, LGPD).

---

[120] HESSE, Konrad. **A força normativa da Constituição**. Trad. Gilmar Ferreira Mendes. Porto Alegre: Sérgio Fabris editor, 1991.

[121] REALE, Miguel**. Filosofia do Direito**. 11.ed. São Paulo: Saraiva, 1986, p. 60.

A LGPD não somente enumera os princípios, como traz o conteúdo básico de cada um deles, a fim de bem delimitar o seu escopo de atuação. Destes, falou-se no tópico que faz análise principiológica da proteção de dados no setor público.

Embora ainda não aprovado, o projeto de LGPD Penal acresce outros a serem aplicados nas atividades de tratamento e compartilhamento dos casos que disciplina: licitude, supremacia do interesse público e auditabilidade.

A licitude determina a atuação do Estado dentro de bases legais bem identificadas, dialogando com o princípio da legalidade, que também rege a atuação estatal. A supremacia do interesse público, agora textualmente indicada como base principiológica, determina a prevalência do interesse público sobre um interesse particular. Auditabilidade é apresentada como a tomada de medidas que viabilizem a verificação e a checagem do tratamento, bem como o controle do acesso à informação, sempre que tecnicamente possível.

A auditabilidade realiza, em alguma medida, o princípio da transparência (que não é em seu texto repetido), o qual, para sua realização, exige informações claras e precisas sobre o tratamento dos dados. Contudo, cuida-se não apenas de acesso à informação sobre o método, mas à intervenção mais direta por meio de checagem. O controle de acesso também é questão salutar, em especial para fins de aferição de responsabilidade em caso de afronta indevida a direitos dos titulares dos dados.

No que tange à supremacia do interesse público, cabe a reflexão já realizada acerca do sopesamento nos locais de interseção de valores objeto de igual envergadura.

5.3 Realização da proteção de dados como condição para o livre desenvolvimento da personalidade

Proteção de dados deve ser vista não apenas como um direito de caráter e expressão meramente individual, mas como um suporte para o livre desenvolvimento da personalidade, com efeitos diretos na organização do corpo social.

Relembra-se, neste ponto, a norma expressa na Lei Fundamental da Alemanha, que garante a todos esses direitos, desde que não violem a esfera jurídica de outros e não atentem contra a ordem constitucional ou a lei moral.

Esse direito foi uma das bases utilizadas pelo Tribunal Constitucional da Alemanha para dar suporte à evolução do conteúdo do direito à privacidade e para construção do direito à autodeterminação informativa, conforme explanado em item anterior do trabalho, para onde se remete.

A realização desse direito interfere na forma como o sujeito se identifica e interage com o mundo, de modo que dados não podem ser utilizados para que um indivíduo seja objeto de vigilância nos aspectos rotineiros de sua vida.

5.4 Previsão de instrumentos adequados de proteção

Sendo uma condição para a liberdade, eventual ofensa à proteção de dados deve ser sujeita a controle imediato, prevendo-se instrumentos que garantam sua proteção adequada, tal como o *habeas corpus*.

Importante pontuar o *habeas data* como importante ferramenta de concretização do direito à proteção de dados, cujas ações de defesa somente poderão ser tomadas quando se tem acesso a e conhecimento dos dados e do processo de seu tratamento. Lembre-se, nesse contexto, voto do Ministro Gilmar Mendes, na ADI 6387, em que este reconheceu o direito à proteção de dados como princípio implícito sustentado em triplo fundamento: dignidade da pessoa humana, força normativa da Constituição e *habeas data* como procedimento apto a dar concretização ao preceito.

5.5 Criação de formas de controle independente da ação estatal

Foi mencionada anteriormente, a ADI nº6.649, em que se discutiu a constitucionalidade de normas do Decreto nº 10.046/2019, o qual criou o Cadastro Base do Cidadão e instituiu o Conselho Central de Governança de Dados, para atividades de gerenciamento daquele.

No texto original do decreto, o Conselho era composto apenas por membros do governo, sem prever qualquer tipo de pluralidade de representação. Analisando o caso, o STF fixou tese no sentido de que o órgão deve ter "um perfil independente e plural, aberto à participação efetiva de representantes de outras instituições democráticas".

Órgão de fiscalização da atividade de tratamento de dados são de extrema importância, em especial quando se cuida da esfera de segurança pública do Estado. Nesta, os direitos costumam ser em mais larga medida flexibilizados, além de haver direitos mais sensíveis desrespeitados em caso de abuso – liberdade, não-culpabilidade, direito à honra e imagem etc.

Objeto central da atividade dessa entidade deve ser a identificação de problemas ou abusos e ofertar soluções para o tema.

Sugere-se que esse organismo seja, assim como o modelo aplicado em outros país, um colegiado evitando que interesses individuais circunstanciais atrapalhem os propósitos do órgão. No Brasil, a ANPD cumpre esse papel.

5.6 Valorização do relatório de impacto à proteção de dados pessoais

Para cada ação ou projeto do Poder Público que impacte no direito à proteção dos dados pessoais, deve-se proceder à confecção de um relatório de impacto, que avalie as possíveis consequências do uso da tecnologia para coleta e tratamento das informações pessoais do sujeito.

Esse relatório deve ser precedente à ação, mas também posterior àquela, servindo para monitoramento da atividade em curto, médio e longo prazo.

O relatório deve analisar não apenas o impacto individual, mas também o impacto coletivo, quando vislumbra-se ser este possível.

Esse relatório será particularmente relevante quando o tratamento envolver dados de pessoas em grupo de vulnerabilidade ou em ações que importem perfilhamento e vigilância estatal.

5.7 Seleção de agentes de controle e Responsabilização

Normas que garantam a possibilidade de aplicação de sanções em caso de desrespeito às normas de tratamento de dados são essenciais para inibir infração às regras protetivas.

Deve-se aplicar ao caso as normas abrangentes de responsabilidade estatal objetiva quando ficar comprovado o dano e o nexo causal entre este e o agente investido de poder estatal. Reconhece-se, porém, a possibilidade de regresso. Este deve ter em mira o agente controlador do dado que deixou de aplicar as recomendações dadas para uso da ferramenta sem prejuízo aos direitos individuais ou coletivos.

Como frequentemente as bases de dados serão operadas por muitos sujeitos autorizados – não só na atividade de tratamento, mas também no compartilhamento, recomenda-se cuidado especial no registro dos acessos realizados, garantindo-se a possibilidade de individualização da ação de cada agente no manuseio do banco detentor dos dados.

Quanto aos controladores, ainda, devem ser selecionados e capacitados com a cautela necessária, a fim de que estejam sensíveis à importância de tratamento cuidadoso dos dados pessoais, evitando-se restrições de direitos maiores que as necessárias.

5.8 Debate e escrutínio público

Uma sociedade democraticamente organizada não prescinde do debate público na formulação de políticas públicas e outras discussões de relevo do Estado. É preciso que este esteja aberto ao diálogo a fim de ter acesso às múltiplas dimensões das questões que envolvem o interesse público, alcançando nuances que apenas os grupos que es experienciam são capazes de perceber ou articular.

Essa iniciativa é especialmente relevante em relação a grupos minoritários e setores marginalizados, que carregam suas nuances próprias, incapazes de serem percebidas em sua profundidade por quem não se enquadra no mesmo grupo ou local social.

Nesse contexto, traz-se importante lição de George Marmelstein, que bem revela a delicadeza da questão posta. Conforme o autor, "(...) até as pessoas eticamente orientadas, que acreditam sinceramente na perversidade do preconceito e defendem que todos devem ser tratados com igual respeito e consideração, podem agir, inconscientemente, de forma discriminatória, o que torna o fenômeno ainda mais intrigante."[122] Assim, é preciso que os grupos excluídos tenham suas vozes ouvidas e participem com qualidade do debate público, enriquecendo-o com suas experiências próprias.

Os exemplos abordados no texto quanto ao reconhecimento facial bem ilustram as consequências da falta de representatividade e do tratamento parcial e segmentado dado sem chamamento à participação de grupos abrangentes.

5.9 Comunicação

Como corolário do princípio da transparência, é importante que a Administração informe aos indivíduos sempre que esses dados forem coletados, indicando, ainda, os fins e usos que dele forem efetivamente feitos. Bem assim, em caso de compartilhamento, deve-se indicar que órgãos ou entidades receberam os dados e as finalidades do compartilhamento.

---

[122] MARMELSTEIN, George**. Discriminação por preconceito implícito**. Salvador: Editora Juspodivm, 2021, p. 25.

Veja-se que todas as instâncias que tiverem acesso aos dados possuem ainda o dever de informar a base legal com que os recolhem, bem como a finalidade específica para que serão usados, em especial quando estiverem sendo aplicadas as hipóteses de tratamento que dispensam consentimento.

Em se tratando de segurança pública e persecução penal, é possível que, durante o tempo de apuração de infrações e para garantir a aplicação da lei penal não seja possível ou viável para os propósitos estatais a comunicação aos titulares dos dados, os quais poderão esquivar-se da persecução em sabendo de antemão a estratégia de segurança adotada. Contudo, quando cessada a fase do sigilo necessário para sucesso da operação deve-se indicar ao titular do dado a coleta, o tratamento e uso que dele foi feito.

Também é recomendável que se indique o tempo que o dado ficará armazenado com possibilidade de uso pelo Estado. Essa medida serve tanto para fins de informação precisa e clara, nos termos exigido pelo princípio da transparência na LGPD, como também para busca dos controladores para atualizações ou retificações quando a situação de fato sofra alguma modificação. Visto que o tratamento do dado normalmente servirá a alguma ação que pode repercutir no gozo de direitos, deve ser garantido ao cidadão que a informação utilizada para seu perfilhamento esteja correta e atualizada.

Ainda quanto à comunicação, sempre que forem usados sistemas que não são de amplo conhecimento do público, estes devem ser apresentados, demonstrando, ainda, o Poder Público a preocupação de demonstrar que a aplicação será feita respeitando-se as normas atinentes à proteção de dados pessoais. Nesse passo, poder-se-á unir este escopo com o debate público, permitindo-se ao corpo coletivo participar do processo de decisão sobre as melhores medidas a serem tomadas para o atendimento de determinado fim estatal.

Por fim, objetivando diminuir a burocracia que pode advir dessa medida, dado o intenso fluxo de tratamento de dados para os amis diversos fins do estado e nas diferentes instâncias, entende-se como atendida a proposta caso a comunicação se dê em formato de informe coletivo, ao qual se dê razoável publicidade ao grupo envolvido na coleta e processamento dos dados.

5.10 Cuidados na coleta dos dados

Conforme apurado em linhas anteriores, é reconhecido que não mais existem dados supérfluos, qualquer pequena informação pessoal, ainda que não pareça sensível em um primeiro momento, possui potencial de, combinadas com outras, em diversas medidas de

extensão, permitir perfilhamento do indivíduo e acesso a um ambiente íntimo e desnecessário para a maior parte das finalidades do Estado.

Por isso, é recomendável que somente se acesse os dados indispensáveis para o atendimento de certo fim, evitando-se coleta indiscriminada. Com inspiração em legislação estrangeira sobre o tema, recomenda-se que o dado recolhido seja apenas o adequado, relevante e não excessivo para a finalidade que se visa a alcançar.

Veja-se que sempre o princípio da finalidade deverá ser atendido. Ao lado deste, também a necessidade deve estar presente. No âmbito da atuação estatal na esfera da segurança pública, necessário será apenas aquele tratamento indispensável para a prevenção e para a repressão de conduta delituosa. Essa, por sua vez, deve ser real e não suposta. Não estará dentro das bases legais tratamento que visa a uma prevenção genérica ou na afirmação de repressão a um crime sobre o qual não se possui evidência de que efetivamente esteja ocorrendo.

Os direcionamentos ora propostos devem ser observados em todas as fases do tratamento de dados: coleta, armazenamento, uso, compartilhamento. Ademais, deve ser observado em todas atividades que envolvam a função de segurança do Estado. É comum que as forcas policiais sejam divididas em tipos ou categoria distintos, conforme se cuide de segurança interna ou atuação voltada à defesa nacional, policiamento comum ou unidades de inteligência. Em quaisquer dessas esferas, porém, recomenda-se a adoção dos direcionamentos citados. Aqui, abrangem-se todos os órgãos abarcados pela previsão do art. 4º, III, da LGPD.

No momento da coleta, deve-se atentar, ainda, para o nível de sensibilidade da informação, a fim de que seja a ela dado tratamento adequado no gerenciamento dos agentes responsáveis pela captação e manuseio posterior. É recomendável que os dados de uma e de outra natureza sejam taxados desde o momento da coleta, dando-se destinação de armazenamento adequado conforme a classificação.

Em relação aos dados sensíveis, destaca-se que a coleta deve ocorrer apenas de maneira excepcional. A regra deve ser a não utilização – o uso somente ser feito quando absolutamente indispensável para alcance da finalidade específica e após exercício de juízo de proporcionalidade em razão da exposição a que se sujeita o titular.

5.11 Armazenamento dos dados

O armazenamento de dados deve ser restrito àquela medida absolutamente necessária para viabilizar a ação estatal, destruindo-se aqueles que não terão utilidade, cujo uso e fim foram exauridos. Essa medida representa vantagem ao mesmo tempo ao administrado,

que vê menores as chances de acesso indevido às suas informações pessoais, e à Administração, que naturalmente possui recursos limitados para guarda de material.

No armazenamento, também é recomendável que se façam classificações das informações, a fim de evitar acesso a dados sensíveis por pessoal não autorizado.

Recomenda-se, ainda, descentralização da base de dados, para que não sejam cruzados diversos dados individuais e separadamente coletados para fins de cruzamento e identificação para fins maliciosos ou intrusivos.

O armazenamento também deve vir acompanhado da preocupação com atualizações, daí ser recomendado que, quando as informações sejam passíveis de sofrer modificações de fato, sejam constantemente checadas ou sejam armazenadas somente por tempo razoável para atender a (i) a finalidade da coleta e tratamento (ii) a razoabilidade de duração do tempo que naturalmente se espera que não haja modificação da situação de fato.

5.12 Regras para uso dos dados

Como se está a tratar de processamento de dados para fins específicos indicados na lei, estes devem ser estritamente observados. Para controle adequado, é razoável que a autoridade estatal sempre indique a base legal sobre a qual realiza o uso do dado.

Essa base deve ser indicada e respeitada também em caso de uso secundário e de compartilhamento, não devendo haver suposição de continuidade do atendimento da finalidade quando os órgãos entre os quais se intercambiam informações possuem funções assemelhadas ou parcerias firmadas para fins específicos.

Esses são os pontos considerados mais relevantes no debate a respeito do uso de dados pessoais pelo poder Público no âmbito da segurança pública e da persecução penal.

Objetivou-se mostrar que o tratamento de dados pelo Poder Público sem sustentação em normas protetivas adequadas acarreta diversos prejuízos à sociedade, como privação indevida de direitos, estigmatização e vigilância social. É o que já ocorre. Para enfrentar esse problema de maneira adequada, faz-se as sugestões supra, as quais, se atendidas, permitirão uma adequada gestão do interesse público na segurança e na persecução penal, ao lado do respeito a direitos e garantias postos.

CONSIDERAÇÕES FINAIS

O presente trabalho objetivou analisar como o uso de dados pessoais pela Administração para fins de segurança pública, defesa nacional, segurança de Estado e prevenção e persecução criminal sem procedimentos adequados pode levar a indevida restrições de direitos e à criação de um ambiente de vigilância estatal que ameaça o livre desenvolvimento da personalidade, a livre organização social e a própria ordem democrática.

Para o escopo da pesquisa, foram feitas introduções para apresentação do ambiente normativo relativo à proteção de dados no país, trazidos conceitos relevantes para entendimento do tema, como as concepções de privacidade, autodeterminação informativa, livre desenvolvimento da personalidade e proteção de dados pessoais.

Ao longo do trabalho utilizaram-se apenas casos reais para ilustração dos diversos temas, dada a riqueza da literatura já desenvolvida sobre o tema e a amplitude da aplicação dos recursos tecnológicos no combate e prevenção ao crime em todo o globo.

Os exemplos analisados demonstraram diversos casos em que o não cumprimento de determinadas normas de procedimento e a ausência de cuidado na aplicação atenta dos princípios que regem a proteção de dados causaram graves prejuízo aos seus titulares, com atingimento especial de alguns grupos particularmente vulnerabilizados, como mulheres, negros e pessoas trans.

Demonstra-se a insuficiência das normas existentes nesse campo, pelo que deve haver esforço estatal no sentido de criar regras adequadas que gerenciem a atividade estatal no campo da segurança sem sacrifício desarrazoado de direitos e liberdades individuais.

Visando a contribuir com a discussão, foram elaboradas as propostas apresentadas no capítulo 5, as quais, espera-se, possam ajudar na compreensão da gravidade do tema e das sutilezas que lhe subjazem, para que todo o potencial apresentado pelas tecnologias possa ser aproveitadas para eficiência máxima do Estado em sa atuação.

Com essa proposta, espera-se que os próprios administrados sintam-se seguros de que a atividade prestada pelo Estado o é com atenção e respeito a seus direitos, criando m ambiente seguro para tratamento desses dados, criando vigilância estatal apenas na medida necessária para o bem maior coletivo. Eis o que se espera de uma convivência harmônica dos diversos interesses sociais.

REFERÊNCIAS

ABERCROMBIE, N.; HILL, S.; TURNER, B.S. **Sovereign individuals of capitalism**. London: Allen & Unwin, 1986.

ALGORITHMIC JUSTICE LEAGUE. Disponível em: https://www.ajl.org/about. Acesso em: 20 de novembro de 2023.

ARAÚJO, Valter Shuenquener de; ZULLO, Bruno Almeida; TORRES, Maurílio. Big Data, algoritmos e inteligência artificial na Administração Pública: reflexões para a sua utilização em um ambiente democrático. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 20, n. 80, p. 241-261, abr./jun. 2020.

ARENDT, Hannah. **A condição humana**/Hannah Arendt; tradução de Roberto Raposo, posfácio de Celso Lafer. 10.ed. Rio de Janeiro: Forense Universitária, 2007.

ARGENTINA. **Habeas Data**. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790 . Acesso em: 19 de novembro de 2023.

ARGENTINA. **Proyecto de Ley de Protección de Datos Personales**. Disponível em: https://www.argentina.gob.ar/sites/default/files/2018/10/proyecto_leypdp2023.pdf . Acesso em: 19 de novembro de 2023.

ASSOCIAÇÃO NACIONAL DE TRAVESTIS E TRANSEXUAIS (ANTRA). **Dossiê Assassinatos e Violências contra Travestis e Transexuais em 2022**. Disponível em: https://antrabrasil.files.wordpress.com/2023/01/dossieantra2023.pdf. Acesso em: 20 de novembro de 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo para Tratamento de dados pessoais pelo Poder Público**. Versão 2.0. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 17 de novembro de 2023.

BIG BROTHER WATCH. **Big Brother is not only watching you – he's identifying you**. Disponível em: https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/. Acesso em: 20 de novemrbod e 2023.

BIONI, Bruno**. Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2021.

BONAVIDES, Paulo. **Teoria Geral do Estado** – 11. ed., rev. e aum. – São Paulo: Malheiros, 2018.

BRASIL, Supremo Tribunal Federal. **ADI nº 6529**. Relatora Ministra Cármen Lúcia. Julgamento em 11 de outubro de 2021. DJE nº217/2021 e DOU nº 208/2021. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15348384228&ext=.pdf. Acesso em: 20 de novembro de 2023.

BRASIL, Supremo Tribunal Federal. *BVerfGE* 35, 202, "Caso Lebach"(*Soldatenmord von Lebach*). **Boletim de Jurisprudência Internacional**: Direito ao Esquecimento. 5.ed. Brasília:

Supremo Tribunal Federal, 2018. Disponível em: https://www.stf.jus.br/arquivo/cms/jurisprudenciaInternacional/anexo/BJI5DIREITOAOESQUECIMENTO.pdf . Acesso em 11 de novembro de 2023.

BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Plataforma de Monitoramento Córtex**. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/operacoes-integradas/destaques/plataforma-de-monitoramento-cortex. Acesso em: 18 de novembro de 2023.

BRASIL. Ministério da Justiça e Segurança Pública. Portaria n°793, de 24 de outubro de 2019. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575. Acesso em: 20 de novembro de 2023.

BRASIL. **Portaria nº 218, de 29 de setembro de 2021**. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/operacoes-integradas/cortex/publicacoes/portaria-no-218-de-29-de-setembro-de-2021/view. Aceso em: 20 de novembro de 2023.

BRASIL. **Projeto de Lei n º 3069**, apresentado em 22 de dezembro de 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2228103&filename=PL%203069/2022. Acesso em: 20 de novembro de 2023.

BRASIL. Supremo Tribunal Federal. **Mandado de Segurança 21.729**. Distrito Federal. Relator: Ministro Marco Aurélio. Redator do acórdão: Ministro Néri da Silveira. DJ PP-00033. VOL-02048-01. PP-00067, 19 de outubro de 2001. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85599 . Acesso em: 11 de novembro de 2023.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 418.416-8/SC**. Distrito Federal. Relator: Ministro Sepúlveda Pertence. Redator do acórdão: Ministro Sepúlveda Pertence. Julgamento em 10 de maio de 2006. DJ 19 de dezembro de 2006. Ementário n° 2261-6. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790 . Acesso em: 11 de novembro de 2023.

BROUSSARD, Meredith. **Artificial unintelligence**: how computers misunderstand the world. London: The MIT Press, 2018.

BROWNE, Simone. **Dark Matters**: on the surveillance of blackness. Durham an London: Duke University Press, 2015.

BUOLAMWINI, Joy e GEBRU, Timnit. **Gender Shades**: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Fairness, Accountability, and Transparency, New York, NY, February 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf . Acesso em: 20 de novembro de 2023.

BUOLAMWINI, Joy. **Unmasking AI**: my mission to protect what is human in a world of machines. New York: Random House, 2023.

CHIN, Josh e LIN, Liza. **Surveillance State**: inside China''s quest to lauch a New era of Social Control. New York: St. Martin's Press, 2022.

COMISSÃO EUROPEIA. **REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO**, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434 . Acesso em 16 de novembro de 2023.

CONFERÊNCIA DAS NAÇÕES UNIDAS SOBRE COMÉRCIO E DESENVOLVIMENTO (UNCTAD). **Data protection regulations and international data flows**: Implications for trade and development. Disponível em: https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf. Acesso em: 16 de novembro de 2023.

CONSELHO DA EUROPA. **Convenção 108**. Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2 . Acesso em 16 de novembro de 2023.

CONSELHO DA EUROPA. **Guidelines on facial recognition**. Convenção 108. Disponível em: file:///Users/kelvianebarros/Downloads/020221GBR_Facial%20recognition%20Convention%20108.pdf . Acesso em: 20 de novembro de 2023.

CORTE EUROPEIA DE DIREITOS HUMANOS. **Case of Glukhin v. Russia**. Application nº 11519/20. Disponível em: https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-225655%22]}. Acesso em: 20 de novembro de 2023.

DATA PRIVACY BRASIL e INSTITUTO IGARAPÉ. **Regulação do Reconhecimento Facial no Setor Público**: avaliação de experiências internacionais. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 20 de novembro de 2023.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**, 3ª ed. São Paulo: Revista dos Tribunais, 2021.

DURKHEIM, Émile. Da Divisão do Trabalho Social. Tradução Eduardo Brandão. – 2. ed. – São Paulo: Martins Fontes, 1999.

ESTADOS UNIDOS DA AMÉRICA. **Children Online Privacy Protection Act** (COPPA). Disponível em: https://www.ftc.gov/system/files/2012-31341.pdf . Acesso em: 16 de novembro de 2023.

ESTADOS UNIDOS DA AMÉRICA. **Fair Credit Reportin** Act (FCRA). Disponível em: https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-may2023-508.pdf. Acesso em: 16 de novembro de 2023.

ESTADOS UNIDOS DA AMÉRICA. **Gramm Leach Billey Act** (GLBA). Disponível em: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf. Acesso em: 16 de novembro de 2023.

ESTADOS UNIDOS DA AMÉRICA. **Health Information Portability and Accountability Act** (HIPAA). Disponível em: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf . Acesso em: 16 de novembro de 2023.

FERRAZ JÚNIOR, Tércio. **Sigilo de dados**: o direito à privacidade e os limites da função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, p. 430-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231 . Acesso em 11 de novembro de 2023.

FOLHA DE SÃO PAULO. **Acesso ao Guardião da PF pela Abin gera polêmica**. Disponível em: https://www1.folha.uol.com.br/fsp/brasil/fc1211200805.htm. Acesso em: 20 de novembro de 2023.

FRY, Hannah. **Hello World**: How to Be Human in the Age of the Machine. Random House, 2018. *E-book*.

GARVIE, Clare. **Garbage In, Garbage Out**: face recognition on flawed data. Georgetown law – Center on Privacy & Tecnology. Disponível em: https://www.flawedfacedata.com/. Acesso em: 20 de novembro de 2023.

GOVERNO FEDERAL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Tratamento de Dados pelo Poder Público. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf . Acesso: 04 de novembro de 2022.

GROTHER, Patrick e NGAN, Mei. **Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms, NIST Interagency Report 8009**, 4 (May 26, 2014). Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf . Acesso em 19 de novembro de 2023.

HESSE, Konrad. **A força normativa da Constituição**. Trad. Gilmar Ferreira Mendes. Porto Alegre: Sérgio Fabris editor, 1991.

IBM. IBM CDEO **Letter to Congress on racial Justice Reform**. Disponível em: https://www.ibm.com/policy/facial-recognition-sunset-racial-justice-reforms/ . Acesso em: 19 de novembro de 2023.

INSTITUTO IGARAPÉ. **Reconhecimento Facial no Brasil**. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Avesso em: 20 de novembro de 2023.

INTERCEPT BRASIL. Disponível em: https://www.intercept.com.br/2020/09/21/governo-vigilancia-cortex/. Aceso em: 20 de novembro de 2023.

KLUM, Scott; HAN, Hun e JAIN, Anil K.. **Department of Computer Science and Engineering**. Michigan State University. Sketch Based Face Recognition: Forensic vs. Composite Sketches. Disponível em: https://openbiometrics.org/publications/klum2013sketch.pdf. Acesso em: 20 de novembro de 2023.

LAGE, Fernanda de Carvalho. **Manual de inteligência artificial no direito brasileiro**. 2.ed. rev., atual e ampl. São Paulo: Editora Juspodivm, 2022.

LIMA, Cíntia Rosa Pereira de e FIGUEIREDO, Mariana Ferreira. **10 anos de proteção de dados pessoais nos países ativos do Mercosul:** Breve análise da evolução do cenário legislativo entre 2013 e 2023. Migalhas de proteção de dados. Disponível em:

https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/394405/10-anos-de-protecao-de-dados-pessoais-nos-paises-ativos-do-mercosul . Acesso em: 19 de novembro de 2023.

MACHADO SEGUNDO, Hugo de Brito. **Direito e inteligência artificial**: o que os algoritmos têm a ensinar sobre interpretação, valores e justiça. 2.ed. São Paulo: Editora Foco, 2023.

MARMELSTEIN, George**. Discriminação por preconceito implícito**. Salvador: Editora Juspodivm, 2021.

MARMELSTEIN, George. **Testemunhando a injustiça**: a ciência da prova testemunhal e das injustiças inconscientes. São Paulo: Editora Juspodivm, 2022.

MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do tribunal constitucional federal alemão**. Montevidéu: Fundação Konrad Adenauer, 2005. Disponível em: https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf . Acesso: 27 de outubro de 2022.

MAYER-SCHONBERGER, Viktor e Cukier, Kenneth. **Big Data**: A Revolution that Will Transform How We Live, Work and Think. Nova Iorque: Houghton Mifflin Harcourt Publishing Company, 2013. *E-book*.

MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 32.ed. ed. rev. e atualiz. São Paulo: Malheiros, 2015.

MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. **Pensar – Revista de Ciências Jurídicas**. Fundação Edson Queiroz - Universidade de Fortaleza. V. 25, n.4. 2020. Disponível em: https://ojs.unifor.br/rpen/article/view/10828/pdf . Acesso em: 11 de novembro de 2023.

MENEZES, Joyceane Bezerra de e COLAÇO, Hian Silva. Quando a Lei Geral de Proteção de Dados não se aplica? TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 2.ed. São Paulo: Thomson Reuters Brasil, 2020.

MENEZES, Joyceane Bezerra de e COLAÇO, Hian Silva. Quando a Lei Geral de Proteção de Dados não se aplica? Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Gustavo Tepedino, Ana Frazão e milena Donato Oliva, coordenação. 2ª edição. São Paulo: Thomson Reuters Brasil, 2020.

NOBLE, Safyia Umoja. **Algorithms of Opression**: how search engines reinforce racism. New York: New YorK University Press, 2018.

O GLOBO. **Caso ABIN**: operação para investigar programa espião afasta número três da agência e prende dois servidores. Dispnível em: https://oglobo.globo.com/politica/noticia/2023/10/20/caso-da-abin-pf-faz-operacao-para-investigar-programa-secreto-que-monitorou-localizacao-de-pessoas-por-meio-do-celular.ghtml. Acesso em 18 de novembro de 2023.

O PANÓTIPO. **Reconhecimento facial cresce no Brasil**; entenda como isso afeta você. Disponível em: **https://opanoptico.com.br/reconhecimento-facial-cresce-no-brasil-entenda-como-isso-afeta-voce/**. Acesso em: 20 de novembro de 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Conselho de Direitos Humanos. **Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests**. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/154/35/PDF/G2015435.pdf?OpenElement. Acesso em: 20 de novembro de 2023.

OVD-INFO**. How the Russian state uses cameras against protesters**. Disponível em: https://en.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters#1 . Acesso em: 20 de novembro de 2023.

PARAGUAI. **Ley 1.682**. Disponível em: https://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado . Acesso em: 19 de novembro de 2023.PARAGUAI. Ley 1.682. Disponível em: https://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado . Acesso em: 19 de novembro de 2023.

PARAGUAI. **Ley 6.534.** Disponível em: https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-de-datos-personales-crediticios . Acesso em: 19 de novembro de 2023.

PARLAMENTO EUROPEU. **Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 16 de novembro de 2023.

PARLAMENTO EUROPEU. **Diretiva 2002/58/CE do Parlamento Europeu e do Conselho**, de 12 de julho de 2002. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002L0058. Acesso em: 16 de novembro de 2023.

PARLAMENTO EUROPEU. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho**, de 24 de outubro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 16 de novembro de 2023.

PARLAMENTO EUROPEU. **Fichas técnicas sobre a união Europeia** – 2023. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em: 16 de novembro de 2023.

PARLAMENTO EUROPEU. **Regulamento (UE) n.º 2018/1725 do Parlamento Europeu e do Conselho**, de 23 de outubro de 2018 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1725. Acesso em: 16 de novembro de 2023.

PROPUBLICA. **Machine Bia**s: there's software udes across the country to predict future criminals. And it's biased against black. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em: 20 de novembro de 2023.

PROPUBLICA. **Risk Assessment**. Disponível em: https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html. Acesso em 20 de novembro de 2023.

REALE, Miguel**. Filosofia do Direito**. 11.ed. São Paulo: Saraiva, 1986.

REIS, Camille Lima; CARVALHO, Fábio Lins de Lessa. O fomento às novas tecnologias na Administração Pública como direito ao desenvolvimento. **International Journal of Digital Law**, Belo Horizonte, ano 1, n. 3, p. 11-28, set./dez. 2020. Disponível em: https://journal.nuped.com.br/index.php/revista/article/view/15. Acesso em: 14 de fevereiro de 2022.

REIS, Carolina; ALMEIDA, Eduarda Costa; DOURADO, Fernando Fellows e SILVA, Felipe Rocha da. **Vigilância automatizada**: uso de reconhecimento facial pela Administração Pública. Laboratório de Políticas Públicas e Internet (LAPIN). Disponível em: https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/ . Acesso em: 20 de novembro de 2023.

RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. São Paulo: Renovar, 2008.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. São Paulo: Edipro, 2016.

SOLOVE, Daniel J. **Nothing to hide**: The false tradeoff between privacy and security. Yale University Press, 2011.

SOLOVE, Daniel J. **Understanding Privacy**. Cambridge: Harvard University Press, 2008.

SOUZA NETO, Cláudio Pereira de; SARMENTO, Daniel. **Direito Constitucional**: teoria, história e métodos de trabalho. 2ª ed., 6ª reimpr. Belo Horizonte: Fórum, 2019.

SUPREMO TRIBUNAL FEDERAL. ADI nº 6529. Relatora Ministra Cármen Lúcia. Julgamento em 11 de outubro de 2021. DJE nº217/2021 e DOU nº 208/2021. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15348384228&ext=.pdf. Acesso em: 20 de novembro de 2023.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 2.ed. São Paulo: Thomson Reuters Brasil, 2020.

THE NEW YORK TIMES. **Facial Recognition Is Accurate, if You're a White Guy**. Disponível em: https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html .Acesso em: 20 de novembro de 2023.

THE NEW YORK TIMES. **Wrongfully Accused by an Algorithm**. Disponível em: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html . Acesso em: 19 de novembro de 2023.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Processo n°1090663-42.2018.8.26.0100. Disponível em: https://esaj.tjsp.jus.br/pastadigital/abrirPastaProcessoDigital.do?origemDocumento=P&nuProcesso=1090663-42.2018.8.26.0100&cdProcesso=RI006J6T80000&cdForo=990&tpOrigem=2&flOrigem=S&nmAlias=SG5TJ&instanciaProcesso=SG&cdServico=190201&ticket=7upz7TIHKDNDY8NvtgdTSTbDmGLf%2FMwTyeWqRiDkbRjeBxdKdyk%2FYfy%2FDhiHd%2BmJjaqDc4rVoVv7L3tBqAQ1%2B3m0ArDoTWSHF595wJYaYlVPrlfAaS0eLZjx6Zjg5skxSSa%2FaaSwd

KVZgUo3VY5mVJXav8I0xIIxnkJKU8XBAhT1vZtkMsMoTCfZC2FQSIsdpu5I0oERzG8vZnF6zX%2B3tbWf0lgJ5KvdiRmS8I88YzUgGjXBWOcKra1PGlypZB9oTh9iQscDPddDS2TXZNz5czLm72Pep3dAK0DgAz9rGVLNHMpEZaJHRiQYETkAbmTR6CDVwtspJ%2FFaedoWNQ46OQ9AKp3NtW6mRHfKnVpFvfi39HTDtgExoh4Q%2BvF9LdQP257D5bGmSmuYaFSaAJWgiuW87xlBcMrqsD575oKMQBXnbdz5JEiKkCCtRSGJ5Y6mOL48iqb2SKBpZJgIZqZhb%2Bt3XFWrDOFsI9vsDyUg4OrHKC0W5GwZpoQnmdZIOPjt1UyyzpQEZ51Aml01sUfyXjtgW0Hbn8v%2FjkonbofRGZ1%2BLAzGMSi692qsEFamJgHm. Acesso em: 20 de novembro de 2023.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Processo nº 1010667-97.2022.8.26.0053. Disponível em: https://esaj.tjsp.jus.br/pastadigital/abrirPastaProcessoDigital.do?nuProcesso=1010667-97.2022.8.26.0053&cdProcesso=1H000LRDS0000&instanciaProcesso=pg&cdProcessoMaster=1H000LRDS0000&cdForo=53&baseIndice=INDDS&nmAlias=PG5JM&tpOrigem=2&flOrigem=P&cdServico=190101&acessibilidade=false&ticket=MX0UHU9QI3xhDMraFDVa7so7DbaRQP0ciU9v3jTQY9D9pp%2FukCo7Z1l9%2BNqSR0VuI5%2FThVsJM6o9i6eV%2FtdI83SvYZyB2%2BPASJuRZjyEBu8toeALcKdZXL1r8EQPkYB5adoy%2BaEbZQ7R1O9EWz0XTeIp9g7JXyGkhoHtpqOc6F6vvEakJvbzSC%2F2DAcCr59VsCS5PdXV8BTflut3i%2B0vdsEcUH2JSJgWVvm%2BYFbiYpXgh4CtIi67oGqA%2BA82XXh0vZMK76ArMaSuXQ1ry%2FK167iR2IhKLQTLE0i864b0NUzXQCMH2SniRirBgTRyR39H%2FaRdkcUcz%2BjT7bwf25RWZdxTW%2Fi7MASM1NfpXkjqXctfEET417PC91lTaHIrpJ7HI65L8He%2B7fDLT5DhFHM5oEeqJWEHgfbVr%2BZSYGwtH0E0WWOCHazJdB3w5VO1viFoOQh6A%2Frf3qKPzE%2F2kAzuEeKLRdvDt52yvJTqNZXa8Qz6ZhOZwo87m2%2B%2Fk%2FNdsmQnWL4hOSPeSnnT1SKQpn3pjO6Ta5N5Pc4aoxMnyXJLnac%2BdkcVtlP%2F0zTGPAdPRPqP . Acesso em: 20 de novembro de 2023.

UOL. **Inteligência Artificial**: além do racismo, reconhecimento facial erra mais em pessoas trans. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/02/14/nao-e-so-racismo-reconhecimento-facial-tambem-erra-mais-em-pessoas-trans.htm. Acesso em: 20 de novembro de 2023.

UOL. **Racismo Calculado**: Algoritmos de plataformas e redes sociais ainda precisam de muita discussão para fugir de estereótipos. Disponível em: https://www.uol.com.br/tilt/reportagens-especiais/como-os-algoritmos-espalham-racismo/#end-card. Acesso: 31 de outubro de 2023.

URUGUAI. **Reglamentacion de los arts. 37 a 40 de la ley 19.670 y art. 12 de la ley 18.331**, referente a proteccion de datos personales. Disponível em: https://www.impo.com.uy/bases/decretos/64-2020 . Acesso em: 19 de novembro de 2023.

WARREN, Samuel; BRANDEIS, Louis. **The Right to Privacy**. Civilistica.com. Rio de Janeiro, a.2, n.3, jul.-set./2013. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/127/97 . Acesso: 08 de novembro de 2023.

WIMMER, Miriam. O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In: BIONI, Bruno Ricardo; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (org.). **Tratado de proteção de dados pessoais**. São Paulo: Forense, 2022.

WORLD JEWISH CONGRESS e UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION (UNESCO). **Como os alemães sabiam quem era judeu?** Disponível em: https://abouthолocaust.org/pt/facts/como-os-alemaes-sabiam-quem-era-judeu . Acesso: 27 de outubro de 2022.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução George Schleinger. – 1. ed. – Rio de Janeiro: Intrínseca, 2020.