NOTA TÉCNICA

VIGILÂNCIA EM MASSA E PROTEÇÃO DE DADOS: IMPLICAÇÕES DO USO DO SISTEMA CÓRTEX NO BRASIL

2024

AIRES

RAIES

REALIZAÇÃO

AI Robotics Ethics Society na PUCRS – **AIRES na PUCRS**

Rede de Inteligência Artificial Ética e Segura – **RAIES**

AUTORIA

Rafaela Weber Mallmann – Presidente do capítulo da AIRES na PUCRS
http://lattes.cnpq.br/0724129228002795

Camila Palhares Barbosa – Pesquisadora RAIES
http://lattes.cnpq.br/3838152756530280

Ana Corcovado – Diretoria AIRES
http://lattes.cnpq.br/2431654446344602

Bernardo Ferreira – Diretoria AIRES
https://lattes.cnpq.br/1150870853634759

Roberta Scalzilli Silva – Diretoria AIRES
http://lattes.cnpq.br/4110110385591421

Iara Cunha Passos – Pesquisadora AIRES
http://lattes.cnpq.br/1548598214531431

Aline Santos Barbosa – Bolsista RAIES
http://lattes.cnpq.br/8576397640518649

Paulo Marcelo Pinheiro Pasetti – Bolsista RAIES
http://lattes.cnpq.br/7149655503079342

Yasmim Aparecida Silva Almeida – Pesquisadora AIRES
https://www.linkedin.com/in/yasmim-aparecida-4a5bb4326/

AIRES na PUCRS:

AI Robotics Ethics Society na PUCRS

https://www.airespucrs.org/

airespucrs@airespucrs.org

RAIES:

Rede de Inteligência Artificial Ética e Segura

https://www.raies.org/

raies@raies.org

VIGILÂNCIA EM MASSA E PROTEÇÃO DE DADOS: IMPLICAÇÕES DO USO DO SISTEMA CÓRTEX NO BRASIL

APRESENTAÇÃO

A AI Robotics Ethics Society (AIRES) na PUCRS é uma organização de estudantes sem fins lucrativos que busca contribuir com a pesquisa científica e educar líderes futuros da IA em princípios éticos, a fim de assegurar que a IA seja criada de forma ética e responsável. Juntamente à AIRES, a Rede de Inteligência Artificial Ética e Segura (RAIES) é uma intersecção de pesquisadores, empresas, universidades e instituições nacionais e internacionais, a fim de promover o desenvolvimento de uma Inteligência Artificial ética e segura.

A RAIES busca por soluções que capacitem desenvolvedores e empresas que produzam aplicações através de sistemas inteligentes a instituir políticas que estimulem o desenvolvimento de IA ética e segura. Deste modo, alinhando os interesses da sociedade brasileira com os interesses da indústria, almejamos garantir que "Inteligência Artificial" se torne "Inteligência Artificial Benéfica e Para Todos".

É a partir desses objetivos que as duas organizações se uniram a fim de desenvolver esta Nota Técnica a respeito do uso do sistema Córtex.

A plataforma de Monitoramento Córtex[1] é alimentada com um sistema de vigilância que conta, entre outras informações, com imagens captadas em tempo real por 35,9 mil câmeras espalhadas em locais públicos em todo o Brasil, sendo rodovias federais, ruas e avenidas, entradas e saídas de estádios

1 Disponível em: https://apublica.org/2024/10/vigilancia-55-mil-agentes-podem-monitorar-alvos-sem-justificativa/. Acesso em: 27 out. 2024.

de futebol, entre outros pontos estratégicos. A funcionalidade denominada “cerco eletrônico” consegue monitorar ao vivo os veículos que transitam por esses locais que contém câmeras a partir da “leitura” das placas dos automóveis.

O sistema foi criado com o intuito de ser utilizado como ferramenta do setor de inteligência do Ministério da Justiça e Segurança Pública (MJSP) em Brasília. O problema central envolvido em sua utilização é que não há necessidade de motivação dos usuários ao consultarem informações no Córtex, pois as consultas ocorreriam visando atividades de manutenção da segurança pública. Apenas haveria auditoria em caso de suspeita de irregularidades nas consultas.

Desde 2019, o Ministério da Justiça e Segurança Pública tem expandido e aprofundado o uso da Plataforma Córtex, desenvolvida “em prol da integração das forças de segurança pública no combate às mais diversas modalidades de prática criminal”[2], mas que em prática tem permitido o amplo monitoramento e vigilância no âmbito civil. Em 2022, a Associação Data Privacy Brasil de Pesquisa, em conjunto com outras ONGs defensoras da privacidade e segurança de dados, encaminharam ao Ministério Público Federal um ofício solicitando um inquérito acerca das potenciais irregularidade da plataforma, especialmente, da violação da privacidade, da transparência, e ameaça a direitos e liberdade fundamentais protegidas constitucionalmente. Com a expansão do uso da Córtex, no dia 9 de outubro de 2024, a agência de notícias Pública divulgou uma matéria denunciando a existência, no âmbito do Ministério da Justiça e Segurança Pública (MJSP), de uma “plataforma de dados capaz de monitorar pessoas e veículos nas ruas em tempo real e sem autorização judicial”[3]. A matéria reacendeu o debate necessário sobre o uso de plataformas de inteligência artificial (IA) para automatização da segurança pública através do monitoramento massivo dos cidadãos, sem parâmetros le-

2 Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/operacoes-integradas/destaques/plataforma-de-monitoramento-cortex#:~:text=O%20Minist%C3%A9rio%20da%20Justi%C3%A7a%20e,diversas%20modalidades%20de%20pr%C3%A1tica%20criminal.. Acesso em: 29 out. 2024.

3 Disponível em: https://apublica.org/2024/10/vigilancia-55-mil-agentes-podem-monitorar-alvos-sem-justificativa/. Acesso em: 28 out. 2024.

gais e transparentes, além da ausência de um debate e mapeamento sobre os possíveis malefícios éticos de seu uso.

A Plataforma de Monitoramento Córtex é operada como uma ferramenta de "inteligência" do MJSP, o que dá respaldo jurídico para que seja operada sem análise do Judiciário ou vínculo a processos judiciais ou inquéritos da polícia. Contudo, na realidade, essa plataforma é disponibilizada para mais de 180 órgãos, inclusive de fora do Sistema Único de Segurança Pública (SUSP), e é atualmente operada por 55 mil usuários civis e militares. Há esforços na promoção do uso da plataforma no reforço da segurança pública, de modo que esse número cresce à medida que novos acordos são celebrados. O cadastro das entidades que podem ter acesso à ferramenta se dá mediante barganha de informações para incremento da própria plataforma: uma prefeitura que disponibilize informações sobre bilhetagem do transporte público, por exemplo, pode ter acesso à plataforma e, nela, obter informações do Sistema Único de Saúde (SUS), emissão de notas fiscais ou das câmeras de monitoramento em tempo real de rodovias e espaços públicos de outra cidade ou outro estado do Brasil. Este exemplo ilustra a abrangência e a natureza diversa dos dados concentrados e disponibilizados na plataforma. Uma vez que seu uso não é discriminado e não há transparência sobre a coleta e distribuição de informações, qualquer cidadão pode ser um "alvo" de qualquer um dos 55 mil usuários com acesso à plataforma (de inteligência).

Não há controle efetivo nem necessidade de relatar o motivo da vigilância, por quanto tempo foi realizado o monitoramento e o resultado da ação por parte do usuário. A concentração e a possibilidade de cruzamento dos dados disponíveis representam um poder desmedido sobre cidadãos comuns, na medida em que os "alvos" não sabem que estão sendo vigiados por outros cidadãos com acesso privilegiado aos dados sensíveis por meio de uma ferramenta criada e disponibilizada, sem a devida cautela e controle, pelo poder público. Aqueles cidadãos que possuem registro de automóvel em seu nome, cadastro no SUS, a carteira de trabalho assinada ou empregam funcionários, que registram seu CPF em no-

tas fiscais ou usam um bilhete único de transporte público, entre outras ações simples, podem estar sendo monitorados através do sistema. Isso implica, portanto, que praticamente qualquer pessoa no Brasil pode estar sendo monitorada no presente momento, tornando-se um sistema massivo de vigilância e controle.

CONTEXTUALIZAÇÃO

Atualmente, o campo da Inteligência Artificial (IA) lida com questões de impacto social relevantes. O debate sobre a utilização de ferramentas, como a de reconhecimento facial (FR), abre uma discussão técnica e pública quanto à sua utilização devido aos altos índices de malefícios, especialmente com comunidades vulnerabilizadas, que podem vir a ocorrer durante seu manuseio. Entender a história do campo da IA, suas atuais conjecturas, apresentar as devidas explicações de seus métodos, etapas de desenvolvimento e aplicação na sociedade são peças-chave para que direitos possam ser respeitados e responsabilidades possam ser atribuídas a quem lhes constroem e mantêm ativas.

Historicamente, o campo de pesquisa da IA possui como marco o ano de 1956, quando um pequeno grupo de cientistas se reuniu para o Projeto de Pesquisa de Verão de Dartmouth sobre Inteligência Artificial. O encontro inicial, idealizado por John McCarthy, na época professor de matemática da faculdade, propunha, através de suas próprias palavras, "prosseguir com base na conjectura de que cada aspecto do aprendizado ou qualquer outro recurso da inteligência pode, em princípio, ser descrito com tanta precisão que uma máquina pode ser criada para simulá-lo"[4]. E para alcançar o objetivo estipulado seria "feita uma tentativa de descobrir como fazer com que as máquinas usassem a linguagem, formassem abstrações e conceitos, resolvessem tipos de problemas reservados aos seres humanos e se aprimorassem[5]". Ou seja, se tentaria estabelecer

4 Disponível em: https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth.
5 Disponível em: http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf.

uma estrutura para entender melhor a inteligência humana de forma a tornar as máquinas mais inteligentes.

Naquela época, os problemas reconhecidos dentro do campo de IA durante o projeto de pesquisa consistiam em:

- Criar computadores automáticos capazes de simularem ações feitas por máquinas;
- Padronizar regras de raciocínio e regras de conjectura para manipular palavras de forma a programar computadores para se utilizar de um idioma;
- Aprimorar o trabalho teórico e experimental realizado por pesquisadores da época de como organizar uma rede neural hipotética de modo a produzir conceitos;
- Como medir a eficiência de um cálculo a partir do estabelecimento da teoria de complexidade da função;
- Comprovar a ideia de que máquinas realmente inteligentes realizariam atividades de autoaperfeiçoamento;
- Tentar classificar e descrever os métodos que a máquina utiliza para formar abstrações;
- Se a diferença entre o pensamento criativo e o pensamento competente e sem imaginação implica certa aleatoriedade e ou abstração não prevista, como guiar computacionalmente a geração de uma intuição (tomada de decisão) que possa vir a ser eficiente?

Desde seu início, 68 anos atrás, a evolução da IA – que começou com o desenvolvimento e pesquisas de sistemas simbólicos baseados em regras e avançou para o aprendizado de máquina (ML) e as redes neurais – percorreu um longo caminho até se integrar a vários setores econômicos, políticos e sociais com processamento de linguagem natural (PNL) e visão computacional avançadas. Resumidamente, o campo da IA foi

aperfeiçoando a maneira como tenta treinar e simular a forma de raciocínio humano.

Atualmente, a IA geralmente se refere a "máquinas que respondem a estímulos consistentes com as respostas tradicionais dos seres humanos, dada a capacidade humana de contemplação, julgamento e intenção"[6]. Para a produção de sistemas autônomos que procuram replicar um comportamento inteligente, torna-se fundamental que programadores projetem algoritmos, sequências de instruções usados em sistemas de sistemas de IA para tomar decisões usando dados[7]. O que já aponta que o desenvolvimento de qualquer IA ainda necessita de intervenção humana.

A Aprendizagem de Máquina (ML), um subconjunto da IA, é usada na maioria dos aplicativos. Composta por uma série de algoritmos que aprendem com grandes quantidades de dados, para encontrar padrões e fazer previsões, ela executa uma função e melhora progressivamente com o tempo. A Aprendizagem Profunda - Deep Learning (DL) é um subconjunto da ML no qual os modelos fazem suas próprias previsões independentemente de humanos, depois que os modelos são criados. Na DL, os algoritmos são estruturados em camadas e modelados de acordo com a rede neural biológica do cérebro humano. A DL possibilita que o programa de computador realize ações por conta própria. É chamada de "aprendizagem profunda", porque tem camadas (profundas) que a ajudam a aprender a partir dos dados.

Dentre as formas de entrada de dados existentes na Plataforma Córtex, destacamos duas nesta Nota Técnica: i. o reconhecimento óptico de caracteres ou leitor óptico de caracteres (OCR); ii. e o reconhecimento facial (RF). Por exemplo, a utilização de OCR é um método comum de digitalização de textos impressos e a RF, onde os algoritmos de DL aprendem a reconhecer especificidades únicas em rostos de indivíduos como o nariz em um nível e os olhos em outro nível. Ainda, com o tempo, a promessa é de que o sistema melhore seu desempenho[8].

6 Disponível em: https://www.brookings.edu/research/what-is-artificial-intelligence/. Acesso em: 28 out. 2024.
7 Disponível em: https://haas.berkeley.edu/equity/resources/playbooks/mitigating-bias-in-ai/. Acesso em: 28 out. 2024.
8 Disponível em: https://towardsdatascience.com/ai-machine-learningdeep-learning-explained-simply-7b553da5b960. Acesso em: 28 out. 2024.

Para além do que se tenta argumentar pelo Conselho Nacional do Ministério Público - de que “o sistema Córtex foi identificado como uma plataforma importante e eficiente para a fiscalização de política pública de segurança”[9] - a utilização desta tecnologia, que utiliza métodos como o OCR e, especialmente, o FR na sociedade para produzir conteúdos direcionados e personalizados de indivíduos, trabalha com dados, ou seja, fatos brutos que incluem nossas narrativas bem como nossas histórias. Somando-se a isso, a estruturação e tomadas de decisão estipuladas pelo Córtex são selecionados matematicamente, o que faz com que debates sobre os desafios éticos e impactos sociais sejam recorrentemente abordados, de forma simples e direta, para que tendências futuras possibilitem que a inovação gere sistemas mais bem delimitados e mais responsáveis.

PROBLEMAS ÉTICOS RELACIONADOS AO USO DO SISTEMA CÓRTEX

A situação, do ponto de vista ético, é potencialmente perigosa em vários sentidos. As pessoas desconhecem o fato de que estão sendo vigiadas, o que impede a autonomia e consentimento dos usuários para obtenção de informações, violando a Lei Geral de Proteção de Dados (LGPD). Na prática, órgãos de fora do SUSP permitem o acesso a usuários não necessariamente especializados em segurança, o que viola os princípios de transparência e responsabilidade (accountability) necessários para uma plataforma de IA ética e segura.

Além disso, a alegação de que se trata de ações em favor da segurança pública, não são suficientes para justificar o uso em benefício e do não-malefício centrado no humano (Human centeredness), que é amplamente considerado pela literatura como um pilar do uso ética dos sistemas de inteligência arti-

9 Disponível em: https://www.cnmp.mp.br/portal/todas-as-noticias/15672-cnmp-mpf-e-ministerio-da-justica-firmam-acordo-para-acesso-a-plataforma-integrada-de-operacoes-e-monitoramento-de-seguranca-publica. Acesso em: 28 out. 2024.

ficial. Assim, a falta de transparência no processo e o caráter sigiloso da operação levantam sérias questões éticas sobre democracia, direitos e liberdades fundamentais e garantia do uso justo e não discriminatório por essas ferramentas. O acúmulo de um volume significativo de informações sensíveis sobre milhões de cidadãos em um único lugar e seu potencial de controle, manipulação e abuso dessas informações, representa um risco real para a democracia. Dentre os problemas ético e normativos que o uso de plataformas de monitoramento podem suscitar, podem-se destacar como necessários de um debate amplo e público, antes da implementação sistemática de tais mecanismos, as seguintes:

Violação da Privacidade Individual - O monitoramento centralizado e massivo de dados sensíveis, como mobilidade, saúde, situação econômica e de emprego, inclusive salários, além de atividades políticas, representa violação direta do direito fundamental à privacidade. Mesmo que esse sistema seja justificado como uma medida de segurança, a ausência de limites claros e mecanismos de fiscalização pode transformar esse monitoramento em um instrumento de vigilância opressiva. A privacidade é crucial para a liberdade de pensamento e expressão.

Manipulação e Abuso de Poder - Quando o governo centraliza e controla informações sensíveis dos cidadãos, pode dispor de vias para manipular dados, distorcer a realidade e utilizá-los para fins políticos ou pessoais. Sem transparência e supervisão, esse sistema pode ser usado para perseguir dissidentes, silenciar críticas e favorecer interesses específicos, corrompendo o papel ético do Estado como protetor dos direitos e liberdades dos cidadãos. A falta de auditoria e controle externo pode abrir espaço para que agentes do governo ou indivíduos com acesso privilegiado utilizem

os dados para chantagem, corrupção ou outros fins privados, distorcendo o sistema de justiça e comprometendo a confiança pública nas instituições.

Destruição da Autonomia e Liberdade de Expressão - A liberdade de protestar, se organizar politicamente ou até mesmo se mover livremente sem ser observado pode ser suprimida, especialmente se o governo ou outros indivíduos com acesso aos dados, usarem essas informações para retaliar ou limitar essas atividades. O medo de ser constantemente observado pode resultar em sentimento de desamparo, inadequação e insignificância pessoal. Esse estado compromete o desenvolvimento de indivíduos saudáveis capazes de produzir, criar e inovar, levando-os a direcionar seus interesses e suas ações à concordância e ao ajuste do que é externamente imposto. Isso pode levar ao conformismo, à autocensura e ao controle do comportamento das pessoas, destruindo a livre iniciativa e a liberdade de expressão e enfraquecendo a sociedade civil, que é essencial para o funcionamento de uma democracia saudável.

Desigualdade e Desumanização - Um sistema em que informações sensíveis são acessíveis a alguns indivíduos, mas não a outros, pode ser utilizado para criar desigualdades. Por exemplo, pessoas com acesso aos dados podem usar informações de saúde, status financeiro ou político para discriminar, marginalizar ou controlar segmentos específicos da população, o que fere o princípio ético de igualdade de tratamento e de direitos. Tal prática desumaniza aqueles que são monitorados, transformando-os em objetos (alvos) a serem controlados, em vez de cidadãos com direitos e autonomia, além de favorecer o uso para fins pessoais.

Comprometimento da Confiança Pública - Sistemas de vigilância centralizada, especialmente quando não auditados ou quando há evidência de que informações são manipuladas, enfraquecem a confiança das pessoas nas instituições governamentais. Isso pode resultar em alienação social, onde os cidadãos veem o governo mais como um adversário do que como um protetor ou representante de seus interesses. A ausência de transparência e responsabilidade cria uma atmosfera de desconfiança e insegurança, que afeta a coesão social e a legitimidade das instituições políticas.

Enfraquecimento da ordem democrática - A ética de um Estado democrático é baseada na limitação do poder e na proteção dos direitos individuais. A publicidade e transparência de informações pertinentes ao interesse público, são centrais para manutenção da participação e cidadania. Leis de acesso à informação são voltadas para garantia própria da democracia, uma vez que servem para facilitar o acesso dos cidadãos sobre decisões e iniciativas governamentais.

O direito à privacidade e liberdade tem um caráter valorativo central na ordem democrática, contudo, historicamente, a concessão de privacidade individual muitas vezes entra em conflito com os interesses governamentais e públicos. A argumentação em prol da manutenção da segurança pública e da estabilidade institucional por vezes foi usada como base de justificação para algum tipo de controle e 'invasão' do âmbito privado individual. A supervisão da esfera privada de indivíduos, em estados democráticos, é tradicionalmente utilizada pela área política e militar contra inimigos ou suspeitos, enquanto a automatização dos sistemas de monitoramento através de plataformas como a Córtex, permitem que as formas de vigilância se tornem permanentes. Esses sistemas também podem ser usados para observar os usuários e seu

ambiente de maneiras desconhecidas para eles[10]. Dentre os perigos da vigilância constante, vale destacar o já reconhecido risco de malefícios gerados por sistemas autônomos de inteligência artificial contra populações vulneráveis, como em casos de discriminação algorítmica e tomada de decisões com vieses discriminatórios.

No caso da segurança pública e da atuação de força policial, fatores de discriminação raciais e vieses na classificação de 'perigos sociais' precisam nortear o debate ético e deliberativo, antes mesmo da avaliação sobre eficácia e rapidez no combate ao crime, garantindo que o sistema esteja alinhado a princípios de justiça e de não-discriminação. Como aponta Mike Zajko[11], historicamente, os programas para governar os pobres submeteram essas populações a altos níveis de vigilância de forma a reproduzir sua marginalização, assim, o uso da IA ao passo que dá continuidade à vigilância de pessoas pobres e racializadas que já são usualmente vitimadas pelo controle policial, também tem ferramentas que permitem sua utilização em escala e dimensões sem precedentes, o que tem sido chamado pela literatura de "meta-vigilância"[12]. A ética de uma sociedade livre depende do equilíbrio entre segurança, liberdade e verdade, e a plataforma Córtex nos desafia a refletir sobre os limites aceitáveis para o acesso e o controle estatal sobre dados pessoais. Tais questões éticas precisam estar na base das tomadas de decisão sobre a custódia de informações sensíveis. Para que tais ferramentas possam ser justificadas e centradas no desenvolvimento humano, sustentável e benefício social, é preciso haver o alinhamento das práticas de escavação, armazenamento e produção de resultados de dados e informações com as normas e limites legais estabelecidos, observando boas práticas em ressonâncias com princípios éticos.

10 Bartneck, C. et al. (2021). Privacy Issues of AI. In: An Introduction to Ethics in Robotics and AI. SpringerBriefs in Ethics. Springer, Cham. https://doi.org/10.1007/978-3-030-51110-4_8

11 Zajko, Mike. "AI as automated inequality: statistics, surveillance and discrimination." Handbook of Critical Studies of Artificial Intelligence. Edward Elgar Publishing, 2023. 343-353.

12 Kılıç, M. (2024). Socio-political Analysis of AI-Based Discrimination in the Meta-surveillance Universe. In: Kılıç, M., Bozkuş Kahyaoğlu, S. (eds) Algorithmic Discrimination and Ethical Perspective of Artificial Intelligence. Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application. Springer, Singapore. https://doi.org/10.1007/978-981-99-6327-0_2

DIREITOS FUNDAMENTAIS VIOLADOS NO USO DO SISTEMA CÓRTEX E A LEI GERAL DE PROTEÇÃO DE DADOS

Averiguando a relação entre o sistema Córtex e a violação aos direitos fundamentais da Constituição Federal Brasileira, verifica-se que existem duas áreas centrais violadas: a privacidade, por meio da violação aos dados, que pode ser encontrada no que foi disposto no art. 5ª, incisos X e XII, e a liberdade, disposta no próprio *caput* do art. 5º[13]

O art. 5º inciso X da Constituição Federal trata sobre a *inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas*. Além disso, assegura o direito a indenização por danos morais ou materiais decorrentes da violação desses direitos. A falta de consentimento e o acesso aos dados de movimentação dos veículos, registros de saúde e outras informações privadas sem autorização judicial afetam diretamente a intimidade e a vida privada, sendo uma vigilância invasiva.

Ainda, o inciso XII dispõe sobre a inviolabilidade do sigilo "*da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal*".

A relação do Córtex com a violação da privacidade por meio da violação de dados corresponde ao monitoramento sem autorização judicial, ou seja, o sistema permite que mais de 55 mil agentes monitorem os cidadãos em tempo real sem necessitar de uma justificativa, ou até mesmo consulta prévia. Com isso, o direito à privacidade é violado já que os indivíduos são monitorados sem consentimento ou sequer ciência do fato.

O Córtex coleta dados que contam com informações pessoais, como relacionados à saúde (registros do SUS), dados financeiros obtidos através da Relação Anual de Informações Sociais (RAIS) e ainda informações não especificadas sobre autori-

13 Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 out. 2024.

dades em geral qualificadas como Pessoas Expostas Politicamente (PEPs). A coleta de informações confidenciais e o uso indiscriminado de dados sem transparência ou controle, expõem os cidadãos à invasão de privacidade.

Ao realizar uma análise detalhada, observa-se que os direitos fundamentais relacionados à proteção de dados pessoais, livre acesso, transparência, segurança, prevenção e não discriminação, assegurados pela Lei Geral de Proteção de Dados, estão conectados ao direito à privacidade, embora sejam considerados direitos autônomos. Essa relação é evidenciada no artigo 5º, inciso X, da Constituição Federal, e esses direitos podem ser vistos como extensões do direito à privacidade.

Ademais, o direito à proteção de dados pessoais é reconhecido não somente como um direito humano, mas também como um direito fundamental. Embora suas origens estejam ligadas ao direito à privacidade, sua relevância cresceu a ponto de se tornar um direito independente, sendo reconhecido tanto no sistema global das Nações Unidas quanto no ordenamento jurídico europeu. Sua base legal está consubstanciada no artigo 5º, inciso LXXIX da Constituição Federal, promulgada através da Emenda Constitucional n.º 155 no ano de 2022[14].

Assim, é fundamental que o tratamento de dados pessoais esteja alinhado aos princípios de finalidade pública, busca pelo interesse público e atuação conforme as competências legais, além do cumprimento de suas responsabilidades. No que se refere ao exercício das competências ou responsabilidades legais, cada órgão público possui sua autorização legal para realizar o ato e desempenhar sua função[15], uma vez que lhe é conferida uma parcela da autoridade soberana do Estado para exercer funções legais, de interesse público e administrativas, conforme previsto pela legislação.

Desse modo, os órgãos públicos possuem a autoridade para tratar dados pessoais visando atender finalidades de interesse

14 SARLET, Ingo Wolfgang. Fundamentos Constitucionais: o direito fundamental à proteção de dados. In: BIONI, Bruno [et al.]. (org.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 21-59.

15 CAVALCANTI., Themistocles Brandão. Teoria dos atos administrativos. São Paulo: Revista dos Tribunais, 1973. 345 p.

público. Contudo, é essencial disponibilizar informações claras e detalhadas sobre a fundamentação legal, os objetivos, os métodos e os procedimentos envolvidos nessas atividades, por meio de canais de fácil acesso, a fim de evitar disparidades na disseminação de informações entre os cidadãos e o Estado[16].

Enquanto a transparência é frequentemente negligenciada na sociedade de vigilância, a saber, em que as tecnologias de vigilância são amplamente usada para monitorar as atividades cotidianas das pessoas[17], as tecnologias de coleta e processamento de dados avançam, possibilitando que governos e outras organizações monitorem e controlem os cidadãos em uma escala inédita. Isso não apenas compromete a privacidade e a liberdade pessoal, mas também fomenta um cenário favorável a abusos de autoridade e violações de direitos fundamentais.

Assim, o compartilhamento desmedido de dados entre órgãos governamentais pode resultar na elaboração de perfis minuciosos dos cidadãos, ampliando a exposição de informações pessoais a diversos agentes interessados em influenciar ações por meio de algoritmos. A consequência imediata dessas práticas é a violação da autodeterminação dos indivíduos e o comprometimento de seus direitos à liberdade e à privacidade[18].

Nessa linha, é pertinente a avaliação da conformidade do tratamento de dados pessoais pelo Córtex, considerando que o referido sistema tem gerado impactos significativos, conforme demonstrado no capítulo anterior. Ao tratar do uso de dados pessoais dos cidadãos para atividades de segurança pública, segurança nacional e investigação criminal, em seu art. 4º, § 1º, da regulamentação, estabelece que esse possível uso deve ser regido por uma legislação específica e deve in-

16 BOTELHO, M. C.; CAMARGO, E. P. do A. O Tratamento de dados pessoais pelo poder público na LGPD. Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE), [S. l.], v. 9, n. 3, p. 549–580, 2022. DOI: 10.25245/rdspp.v9i3.1034. Disponível em: https://portal.unifafibe.com.br:443/revista/index.php/direitos-sociais-politicas-pub/article/view/1034. Acesso em: 20 out. 2024.

17 MACHADO Arlindo. A Cultura da Vigilância.. Artepensamento IMS, 1991. Disponível em: https://artepensamento.com.br/item/a-cultura-da-vigilancia. Acesso em: 28 out 2024.

18 PAIVA, Marcella da Costa Moreira de; RAMADA, Paula Cristiane Pinto; PIRES, Telson. Sociedade da informação e vigilância. In: MARTINS, Plínio Lacerda et al. Proteção de Dados. Rio de Janeiro: Instituto de Direito Público e Privado, 2021. p. 85-98. Disponível em: http://ppgdin.uff.br/wp-content/uploads/sites/5/2021/03/Livro-Estudos-do-Grupo-de-Prote%C3%A7%C3%A3o-de-Dados-Pessoais-%E2%80%93-CNPQ.pdf. Acesso em: 21 out. 2024.

cluir medidas proporcionais e estritamente necessárias para atender ao interesse público, respeitando o devido processo legal, os princípios gerais de proteção e os direitos do titular. Ocorre que, até o momento da redação desta Nota Técnica, denota ser inexistente.

Nesse contexto, a troca irrestrita de bancos de dados entre diferentes entidades governamentais viola o princípio da finalidade, que estabelece que o tratamento deve ser realizado para objetivos legítimos, específicos, claros e comunicados ao titular, sem a possibilidade de um tratamento subsequente que seja incompatível com as finalidades previamente definidas.

Este conflito está constante na Portaria n.º 218, ao regulamentar o uso e as funcionalidades do referido sistema, estabelece em seu art. 22, a permissão para o compartilhamento de dados por parte do órgão ou ente federado[19]. A ausência de transparência na utilização do sistema evidencia um uso indiscriminado e desregulado, que representa um grande risco à privacidade. Isso se deve ao fato de que a ocorrência de irregularidades em decorrência da falta de critérios legais e de responsabilidade na utilização do sistema, não dispõe de métricas públicas referentes ao seu uso.

Portanto, a existência do Sistema Córtex fortalece a insegurança jurídica no país ao utilizar de vácuo normativo frente à regulamentação própria de dados com enfoque na segurança pública para desenvolvimento de panóptico de vigilância visando monitoramento desenfreado de dados, sob primazia da segurança pública em colisão ao princípio da proporcionalidade, previsto expressamente na Constituição Federal. Isto, resta evidente pela diminuição da capacidade do titular de manter controle sobre suas próprias informações e escolher como configurar sua esfera particular diante da magnitude do poder estatal.

19 BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº 218, de 29 de setembro de 2021. Dispõe sobre a implementação e operação do Córtex – Plataforma Integrada de Inteligência e de Operações de Segurança Pública. Diário Oficial da União, Brasília, DF, 1 out. 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 . Acesso em: 29 out. 2024.

No contexto da Lei de Acesso à Informação (LAI), instituída pela Lei nº 12.527/2011[20] garante a qualquer cidadão o direito de acessar informações públicas, promovendo a transparência e o controle social. A LAI estabelece que a informação é um direito de todos, com exceções limitadas a casos que possam comprometer a segurança da sociedade ou do Estado. A Lei Geral de Proteção de Dados (LGPD), por sua vez, regula o tratamento de dados pessoais, exigindo que este seja realizado com transparência e consentimento, salvo exceções. A conformidade do Sistema Córtex com a LAI é crucial para assegurar a transparência na gestão pública. Isso implica que os dados coletados e analisados devem ser acessíveis ao público, exceto quando classificados como sigilosos, conforme as disposições da LAI. Eventual negativa de acesso deve ser devidamente justificada, respeitando os prazos estabelecidos pela lei.

O direito à liberdade (art. 5º caput) é violado quando esse monitoramento sem critérios estabelecidos leva ao abuso de poder, já que incluem vigilância também de indivíduos que não estão inseridos no escopo inicial na Portaria que o concede. Não há uma fiscalização efetiva do sistema Córtex e a falta de transparência é visível quando as auditorias são acionadas apenas por suspeitas de mau uso, o que demonstra falta de mecanismo preventivos para garantir o uso ético e responsável do sistema.

20 VALENTE, R, FREITAS, C. Programa de vigilância do MJ permite a 55 mil agentes seguir “alvos” sem justificativa. Em: Pública, 2024. Disponível em: https://apublica.org/2024/10/vigilancia-55-mil-agentes-podem-monitorar-alvos-sem-justificativa/?utm_source=republicacao&utm_medium=uol&utm_campaign=cortex1. Acesso em: 28 out de 2024.

A LEI DE ACESSO À INFORMAÇÃO

Um dos principais desafios é garantir a transparência no uso do Córtex, evitando abusos que comprometam o direito à informação. A aplicação do princípio da proporcionalidade é fundamental, assegurando que a vigilância em massa seja necessária e adequada aos objetivos de segurança pública, sem infringir direitos fundamentais. Embora a LAI preveja exceções ao acesso à informação, estas devem ser aplicadas com cautela, evitando que a segurança pública seja utilizada como justificativa para a opacidade.

A conformidade do Sistema Córtex com a LAI depende da natureza das informações que ele processa[21]. Dados pessoais sensíveis e informações que possam comprometer a segurança do Estado podem justificar a negativa de acesso, desde que fundamentada. É essencial que qualquer negativa seja documentada e que o cidadão tenha a possibilidade de recorrer, garantindo assim a transparência e o direito à informação. A implementação do Córtex deve, portanto, ser acompanhada de mecanismos que assegurem a transparência em sua operacionalização, respeitando os direitos fundamentais e promovendo a *accountability* na administração pública. Isso inclui a necessidade de auditorias regulares, relatórios públicos sobre o uso do sistema e a promoção de canais de comunicação entre os cidadãos e a administração pública. Portanto, a adequação do Sistema Cortex à LAI é essencial para garantir que os dados coletados e analisados sejam, sempre que possível, acessíveis ao público.

O monitoramento de segurança pública pela plataforma Córtex, foi objeto do processo nº 08198.006307/2024-41[22], que resultou na negativa de acesso às informações solicitadas por um cidadão, decisão corroborada pelo Ministério da Justiça

21 BRASIL. Superior Tribunal de Justiça. Documento MON, n. 202403061793, de 29 de agosto de 2024. Disponível em: https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=266887009&num_registro=202403061793&data=20240829 . Acesso em: 29 out. 2024.

22 BRASIL. Controladoria-Geral da União. Parecer SEI nº 08198.006307/2024-41. Recurso de 3ª Instância 615. Disponível em: https://buscaprecedentes.cgu.gov.br/BuscaAvancada/BuscaAvancada?idAnexo=119003&idAws=AnexosRecurso%2F201298%2F9c0aa374-f626-49b6-8c61-b56f6b9e0de0&fileName=SEI_08198.0063072024-41_Parecer___Recurso_de_3%C2%AA_Instancia_615.pdf&handler=DownloadFile. Acesso em: 29 out. 2024.

e Segurança Pública (MJSP) e pela Controladoria-Geral da União (CGU). O cidadão demandou dados sobre o total de alvos móveis monitorados, mas o MJSP argumentou que a divulgação desse número poderia comprometer a eficácia das operações de inteligência, uma vez que forneceria informações valiosas a potenciais adversários. A negativa de acesso foi fundamentada na Portaria nº 880/2019 e na Lei nº 12.850/2013, que preveem a proteção de informações sensíveis e o sigilo em investigações contra organizações criminosas. A CGU, ao analisar o pedido, considerou as justificativas apresentadas suficientes para proteger a segurança pública, reafirmando que a transparência deve ser equilibrada com os riscos à segurança das operações. Assim, a decisão enfatiza a importância da preservação das estratégias de segurança em detrimento da divulgação de dados que possam pôr em risco a eficácia das ações governamentais.

O SISTEMA MONUV QUE ALIMENTA O CÓRTEX

Um dos sistemas que alimentam o Córtex é o Monuv, da startup Bitsea Tecnologia em Software S.A., que oferece serviço de gestão de câmeras de segurança para empresas de segurança em uma plataforma de *cloud computing*. A empresa se estabelece sob o conceito de "segurança pública colaborativa"[23], no qual, segundo eles, "empresas de segurança, tecnologia e poder público se unem para resolver o problema de segurança pública do Brasil"[24]. No portfólio da empresa, afirmam que "estudos mostram que onde esse modelo é implantado os crimes reduzem em pelo 50% já no primeiro mês", contudo, não há informação de quais estudos e qual metodologia utilizada.

Com a proposta de ofertar softwares que funcionem em qualquer câmera de segurança, pois armazenam os dados em nuvem, criam uma rede que articula prédios privados, empresas de

23 Disponível em: https://suporte.monuv.com.br/pt-BR/articles/9449857-seguranca-publica-colaborativa-monuv. Acesso em: 27 out. 2024.

24 Disponível em: https://monuv.com.br/. Acesso em: 29 out de 2024.

segurança e órgãos de segurança pública, municipais, estaduais e federais. O Monuv armazena, processa e analisa os dados coletados em plataformas na nuvem, com isso a empresa de segurança não precisa investir em câmeras com maior tecnologia e, consequentemente, mais caras. Além disso, integra com vários sistemas de segurança amplamente utilizados no mercado: Moni, Sigma, Gear, Commbox, entre outros.[25]

Segundo material disponibilizado no site da empresa[26], para participar do sistema de segurança pública colaborativa, o cliente (empresas de segurança), precisa adquirir câmeras e postes (pelo menos 5 postes com 3 câmeras cada, sendo que um deles precisa ter câmeras com o software LPR da Monuv, de leitura de placas) e ter contatado uma autoridade de segurança pública da região para formalizar o apoio e integração de recursos. Dessa forma, a empresa auxilia os órgãos de segurança pública, contribuindo com uma malha de recursos tecnológicos e aumentando a base de dados do Córtex e outros sistemas: colaboram também com o Detecta, da Polícia Militar do estado de São Paulo, Hélios, da Polícia Militar do estado de Minas Gerais, e Smart Sampa, da Prefeitura de São Paulo. Consideram que mais de 40.000 câmeras e postes já integram a rede de segurança pública-privada, o que denota a amplitude e expansão do sistema de monitoramento e vigilância[27].

Os serviços ofertados pela empresa incluem: detecção de veículo suspeito, detecção de intrusão, detecção de pessoa suspeita, detecção de presença, detecção preventiva de ameaças (com o Anomal.IA)[28] e leitura de placas de veículos (LPR)[29]. Segundo material da empresa, a IA ofertada tem uma precisão superior a 98% e reduz em até 100x os falsos alarmes de central de monitoramento - salientamos que mesmo que seja possível um modelo de IA atingir mais de 98% de precisão, não significa que essa precisão seja para todos os cenários.

25 Disponível em: https://suporte.monuv.com.br/pt-BR/collections/9930797-integracoes-e-api. Acesso em: 29 out. 2024.
26 Disponível em: https://monuv.com.br/?utm_source=base_conhecimento. Acesso em: 29 out. 2024.
27 Disponível em: https://suporte.monuv.com.br/pt-BR/collections/9930797-integracoes-e-api. Acesso em: 29 out. 2024.
28 Disponível em: https://suporte.monuv.com.br/pt-BR/articles/9740841-como-configurar-o-anomal-ia. Acesso em: 29 out. 2024.
29 Disponível em: https://suporte.monuv.com.br/pt-BR/articles/2880723-como-funciona-a-leitura-de-placas-da-monuv-lpr. Acesso em: 28 out. 2024.

Conforme Jennifer Jill Fellows e Lisa Smith, uma vasta literatura no campo de ética da inteligência artificial têm debatido os efeitos e os potenciais vieses associados aos usos desses sistemas, que "incorporam tanto implicitamente quando explicitamente com certos objetivos, vieses, ideologias, e visões de mundo que são ditados pelos humanos que as produzem"[30]. Assim, embora os empresas e organizações do "capitalismo e vigilância", isto é, aqueles que se beneficiam e lucram com a vasta coleta de dados por sistemas de IA, projetam discursos de "eficácia", "avanço tecnológico" e "desenvolvimento", é importante assumir que tais tecnologias não são plenamente objetivas e neutras. Joy Buolamwini e Timnit Gebru , por exemplo, demonstraram que há uma disparidade substantiva na precisão do reconhecimento facial na identificação de indivíduos de pele clara e de pele escura.

O reconhecimento de mulheres pretas tem uma precisão de cerca de 34,7%, enquanto a margem de erro para homens de pele clara é 0,8%[31]. Tais estudos mostram como qualquer sistema de vigilância deve estar atento às formas de classificação, como gênero, raça, idade e classe, voltando-se para garantia de uso justo e não-discriminatório. Especialmente se tratando de segurança pública, que é intermediada por empresas privadas que visam lucro como a Monuv, a promessa de "detecção de pessoa suspeita" pode exacerbar o monitoramento e policiamento da população preta, ampliando as práticas discriminatórias e o punitivismo contra a população marginalizada. Questões como quais são os critérios utilizados para caracterizar um indivíduo ou ação "suspeita", podem ser mitigadas pelos princípios de transparência, não-malefício e não-discriminação. Para isso, contudo, as informações de monitoramento e critérios de classificação precisam ser acessíveis ao público. Como argumenta Steeves, "a privacidade é um ponto crítico na sociedade da vigilância precisamente porque a vigilância obje-

30 FELLOWS, Jennifer Jill; SMITH, Lisa (ed.). Gender, Sex, and Tech!: An Intersectional Feminist Guide. Toronto: Canadian Scholars/Women's Press, 2022. p. 185-186.

31 Joy Buolamwini, Timnit Gebru Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a.html?mod=article_inline&ref=akusion-ci-shi-dai-bizinesumedeia. Acesso em: 29 out de 2024.

tifica o eu, derruba os limites entre os papéis sociais e nega as condições necessárias para a intersubjetividade"[32].

O nomal.IA, por exemplo, utiliza algoritmos de aprendizado de máquina (machine learning) para realizar um "monitoramento preventivo". Garantem que o sistema aprende o comportamento de um local entre 3 e 7 dias e com isso é capaz de identificar ameaças. Entretanto, a eficácia em uma rápida aprendizagem do comportamento, não desvela quais tipos de informações estão incluídas na análise e classificação, por exemplo, se o local monitorado contém diversidade, e os riscos caso a resposta seja negativa. Como afirmam Mulligan, D. K., Regan, P. M., & King, J., "o ponto principal aqui é a impossibilidade de extrair o comportamento dos indivíduos, incluindo os participantes da pesquisa, da sociedade que construiu sua compreensão do que é não apenas possível, mas desejável"[33]. No caso do LPR, todos os veículos que passarem pelo local em que a câmera está instalada terão a placa, cor do carro e horário em que foram registrados pelo sistema armazenados[34].

Embora não haja informação de quais dados dos serviços ofertados pela Monuv são enviados para o Córtex, informam que "todas as leituras de placas feitas pela Monuv são automaticamente enviadas ao Córtex" e que "a principal função do Córtex é centralizar e analisar informações provenientes de diversas fontes, incluindo câmeras de vigilância, dados de leitura de placas de veículos (LPR), e outros sistemas de segurança, para auxiliar na prevenção e investigação de crimes". Sobre modelos de reconhecimento facial, a Monuv informa que não realizam esse tipo de serviço, "por questões de privacidade e ética", mas não informa se são enviados imagens ou dados de pessoas para sistemas como Córtex, que podem utilizar esses modelos.

32 Steeves, V. (2009). Reclaiming the social value of privacy. Lessons from the identity trail: Anonymity, privacy and identity in a networked society, 191–208.

33 Mulligan, D. K., Regan, P. M., & King, J. (2020). The Fertile Dark Matter of Privacy takes on the Dark Patterns of Surveillance. Journal of Consumer Psychology, 30(4), 767-773. Disponível em: https://doi.org/10.1002/jcpy.1190. Acesso em: 29 out. 2024.

34 Disponível em: https://suporte.monuv.com.br/pt-BR/articles/9449857-seguranca-publica-colaborativa-monuv. Acesso em: 28 out. 2024.

A diferença desses sistemas de monitoramento baseados em IA para sistemas tradicionais de câmeras de segurança é que os tradicionais armazenavam os dados localmente, em gravações por um período limitado, monitorados em tempo real por uma equipe de segurança ou, numa eventualidade (um roubo, uma invasão, etc), a gravação poderia ser cedida a órgãos de segurança pública. No caso de sistemas de armazenamento em nuvem e processamento por IA, todos os dados são coletados e armazenados, cruzados com outras bases e outros sistemas, sendo que na maioria das vezes quem está sendo filmado não está ciente para onde os seus dados estão sendo enviados e para o que estão sendo utilizados[35].

Na Política de Privacidade e Proteção de Dados Pessoais da Bitsea, identificamos alguns problemas em relação à conformidade com a LGPD e seus princípios[36], em especial:

1. Princípio da Finalidade

A LGPD determina que as atividades de tratamento de dados pessoais devem respeitar princípios, incluindo o da finalidade. Esse princípio exige que o tratamento de dados ocorra exclusivamente para objetivos legítimos, específicos e informados ao titular, proibindo qualquer uso posterior incompatível com os propósitos inicialmente informados.

No contexto da empresa Bitsea, foram identificadas algumas preocupações relacionadas ao cumprimento desse princípio. Embora a empresa cite finalidades gerais, como segurança e gerenciamento de dados, falta clareza sobre a necessidade de coleta de dados sensíveis, como informações biométricas, para alcançar tais objetivos. Essa ausência de transparência pode prejudicar a confiança dos usuários, uma vez que as finalidades para o uso de dados não estão claramente explicadas. A

35 Disponível em: https://suporte.monuv.com.br/pt-BR/articles/9636105-cortex-ministerio-da-justica-e-seguranca-publica-do-brasil. Acesso em: 28 out. 2024.

36 Art. 6º da Lei 13.709, de 14 de agosto de 20218. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 out. 2024.

Bitsea também não especifica por quanto tempo os dados serão armazenados, o que levanta preocupações adicionais. Manter dados sem prazo de eliminação compromete o princípio da finalidade e sugere que o tratamento pode estar sendo realizado além do necessário, possivelmente violando a LGPD.

2. Princípio da Necessidade

A LGPD determina que o tratamento de dados pessoais deve ser limitado ao mínimo necessário para alcançar a finalidade proposta, atendendo ao princípio da necessidade. A Bitsea, entretanto, não esclarece adequadamente por que coleta dados sensíveis, como biometria, para finalidades como segurança e gerenciamento de usuários, levantando dúvidas sobre a proporcionalidade e relevância dessas informações. A empresa também não demonstra considerar alternativas menos invasivas para atingir seus objetivos, sugerindo possível coleta excessiva de dados e falta de conformidade com a LGPD.

3. Princípio da Transparência

A falta de observância ao princípio da transparência na Bitsea implica o descumprimento de outros princípios fundamentais da LGPD, como qualidade, segurança, prevenção, não discriminação e responsabilização. A ausência de informações claras sobre a precisão dos equipamentos utilizados para coletar dados sensíveis, especialmente biométricos, compromete a qualidade e exatidão desses dados e pode gerar problemas de segurança, como falsos positivos em reconhecimento facial. Essa falta de transparência não apenas suscita dúvidas éticas e legais, mas também mina a confiança dos usuários, revelando possíveis falhas na conformidade com a LGPD.

Consequências do Descumprimento dos Princípios da LGPD

A ausência de uma demonstração clara de que o tratamento de dados realizado pela Bitsea é compatível com as finalidades informadas aos titulares pode acarretar sérias consequências. A falta de justificativa para a coleta de dados sensíveis e a ausência de informações sobre a precisão dos dispositivos utilizados indicam um possível desrespeito [MP1] aos princípios da LGPD, expondo os titulares a riscos de privacidade e discriminação. Esse desalinhamento pode resultar em sanções legais e impactar negativamente a credibilidade da empresa.

Para assegurar a conformidade, recomenda-se que a Bitsea minimize a coleta de dados, detalhe as finalidades específicas e estabeleça prazos de retenção claros, além de garantir a precisão dos dispositivos de coleta e fornecer livre acesso aos titulares de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

RESPONSABILIZAÇÃO DO ESTADO NO USO INDEVIDO DE DADOS PELO CÓRTEX

Em nossa análise, não foi localizado precedente que atribua responsabilização direta ao Estado por violação de privacidade ou uso indevido de dados pessoais por meio do sistema Córtex. Entretanto, destacam-se decisões judiciais em que a plataforma Córtex foi utilizada em operações policiais, sem que a legalidade da plataforma em si fosse questionada de forma direta, como ocorre nos seguintes precedentes:

Habeas Corpus n. 226790 / RJ, Ministra Carmen Lúcia, DJe Publicação: 26/04/2023 (STF): Efetuada uma consulta ao sistema de monitoramento de OCRs do Córtex base nacional, sendo verificado que o automóvel do denunciado teria registrado passagens em dois locais próximos aos lo-

cais da abordagem e onde o veículo da vítima foi abandonado, conforme a informação sobre a investigação[37].

Habeas Corpus n. 937605, Ministro Rogério Schietti Cruz, DJe de 29/08/2024 (STJ): O sistema Córtex foi mencionado como ferramenta de investigação, sendo utilizado para rastrear a movimentação de veículos e alterar placas[38].

Habeas Corpus n. 890189, Ministro Joel Ilan Paciornik, DJe de 16/04/2024 (STJ): Neste caso, a plataforma Córtex foi utilizada para localizar veículos suspeitos em uma investigação de crimes graves. O tribunal não questionou o uso do Córtex[39].

Recurso em Habeas Corpus n. 194260, Ministro Ribeiro Dantas, DJe de 06/03/2024 (STJ): A investigação policial contou com o suporte do Córtex para a obtenção de informações relacionadas a movimentações de veículos e sua ligação com crimes investigados[40].

No entanto, o uso da plataforma Córtex foi questionado por alegadas violações das normas processuais penais, nos autos do **Habeas Corpus n. 895233[5], relatora Ministra Daniela Teixeira, DJe de 07/03/2024 (STJ)**, no qual a defesa alegou que

37 BRASIL. Supremo Tribunal Federal. Despacho nº 1398957. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/despacho1398957/false . Acesso em: 29 out. 2024.

38 BRASIL. Superior Tribunal de Justiça. Documento MON, n. 202403061793, de 29 de agosto de 2024. Disponível em: https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=266887009&num_registro=202403061793&data=20240829 . Acesso em: 29 out. 2024.

39 BRASIL. Superior Tribunal de Justiça. Documento MON, n. 202400385707, de 16 de abril de 2024. Disponível em: https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=238871388&num_registro=202400385707&data=20240416. Acesso em: 29 out. 2024.

40 BRASIL. Superior Tribunal de Justiça. Documento MON, n. 202400638183, de 6 de março de 2024. Disponível em: https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=232081205&num_registro=202400638183&data=20240306 . Acesso em: 29 out. 2024.

a extração de dados de um celular foi feita sem a devida autorização judicial, contrariando o Protocolo Córtex e as normas de custódia de prova (Lei n.º 13.964/2019). Em que pese o STJ tenha negado o pedido da defesa, a questão foi discutida quanto à regularidade do processo de coleta e preservação de provas digitais.

Além disso, a análise da **Nota Técnica nº 29/2024/FIS/CGF/ANPD**[41], data de 11/09/2024, emitida pela Autoridade Nacional de Proteção de Dados (ANPD), relacionada ao acordo de cooperação entre o Ministério da Justiça e Segurança Pública (MJSP) e a Confederação Brasileira de Futebol (CBF), suscita importantes questionamentos sobre a proteção de dados pessoais no contexto da segurança pública e da efetividade de iniciativas como o Projeto Estádio Seguro. Este projeto, que visa combater o racismo e a violência nos estádios brasileiros por meio do compartilhamento de dados, levanta preocupações sobre a privacidade dos torcedores e a utilização adequada das informações pessoais. O compartilhamento e o tratamento de dados pessoais, conforme proposto, possui como objetivo identificar indivíduos envolvidos em ilícitos que possam comprometer a segurança nos eventos esportivos. Contudo, a premissa de que a tecnologia e a vigilância podem, por si só, resolver problemas complexos de violência e discriminação nos estádios é questionável.

A análise realizada pela ANPD, ao considerar a legalidade das operações de tratamento de dados dentro desse projeto, levanta outro ponto crucial: a necessidade de garantir que a implementação do projeto respeite os direitos dos titulares. A prática de compartilhar informações sensíveis deve ser acompanhada de mecanismos robustos que assegurem a transparência e a responsabilidade das entidades envolvidas. O caráter modular da Plataforma Córtex, que será utilizada para cruzar dados de vendas de ingressos com informações de pessoas procuradas pela justiça, também gera preocupações sobre a efetividade e a segurança do sistema. A proposta de que os clubes organiza-

41 BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 29/2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nota-tecnica-29_2024.pdf . Acesso em: 29 out. 2024.

dores não terão acesso ao conteúdo dos códigos de bloqueio é um passo positivo em direção à proteção da privacidade dos torcedores. No entanto, a eficácia do sistema depende da robustez das medidas de segurança adotadas e da capacidade de evitar abusos.

Embora se considere que o tratamento de dados pessoais no âmbito deste projeto se enquadre nas competências legais do Ministério da Justiça e Segurança Pública (MJSP) e atenda às finalidades de interesse público, conforme o artigo 23 da LGPD. No entanto, a Lei nº 14.597, de 14 de junho de 2023, que institui a Lei Geral do Esporte, não pode ser interpretada como uma autorização para a transmissão de dados pessoais de torcedores coletados pelos clubes de futebol a esse órgão, com o intuito de implementar o projeto. Essa interpretação se justifica pelo fato de que a norma não define critérios, procedimentos ou limites para o compartilhamento de dados pessoais com órgãos do Poder Público.

Assim, é de responsabilidade do MJSP garantir que o tratamento de dados no âmbito do projeto Estádio Seguro esteja em estrita conformidade com os parâmetros estabelecidos pela LGPD. Além disso, é proibido o uso desse tratamento para finalidades de segurança pública ou para atividades de investigação e repressão de infrações penais, dada a falta de regulamentação específica para tais fins. Essa proibição está alinhada com o disposto no artigo 4º, inciso III, alíneas “a” e “d” da LGPD, que definem as situações em que essa lei não se aplica.

CONSIDERAÇÕES FINAIS

O objetivo desta Nota Técnica foi esclarecer os impactos da utilização do Sistema Córtex para a sociedade, principalmente, no que diz respeito aos problemas éticos e jurídicos envolvidos. Buscamos deixar claro que não há um posicionamento contra o uso das tecnologias para otimizar questões envolvendo a segurança pública e o bem-estar da população, entretanto, é necessário haver uma regulamentação e uma fiscalização sobre a forma como ocorre a utilização dos dados coletados e o cruzamento deles com outros sistemas, bem como sobre as pessoas que possuem acesso a eles. A transparência e acessibilidade oportunizam que a população compreenda como suas informações pessoais estão sendo utilizadas, ao mesmo tempo em que a fiscalização e a regulamentação oportunizam um rigor e maior cuidado no tratamento desses dados.

A tecnologia precisa ser uma aliada no desenvolvimento social, econômico e humano, e não piorar desigualdades e formas de opressão pré-existentes. Por isso o cuidado com a proteção de dados não diz respeito apenas aos desenvolvedores das tecnologias que utilizamos, mas a todos os usuários e indivíduos envolvidos no processo de criação, utilização, aplicação, coleta e análise desses dados que estão disponíveis a partir do uso do Córtex. Sabemos que cada vez mais as informações pessoais estão sendo comercializadas e utilizadas de forma desregulamentada, resultando em vazamentos que movimentam o mercado financeiro ilegal. O Córtex não pode ser uma plataforma que contribua para esse tipo de situação, e deve basear sua aplicação em princípios éticos para que a sua utilização ocorra de forma segura.

AIRES na PUCRS

Presidente
Rafaela Weber Mallmann

Diretoria
Ana Corcovado
Bernardo Ferreira
Roberta Scalzilli Silva

RAIES / PUCRS

Coordenador do Projeto
Nythamar Fernandes de Oliveira

Vice Coordenador do Projeto
Paulo Caliendo

Equipe RAIES
Aline Santos Barbosa
Bernardo Ferreira
Camila Palhares Barbosa
Evandro Pontel
Jair Tauchen
James William Santos
Marcelo Pasetti
Nicholas Kluge Corrêa

AIRES

RAIES