dossiê

VIGILÂNCIA & VIGILANTISMO

conceitos, legislação brasileira e organizações atuantes

Realização

LAUT CENTRO DE ANÁLISE DA LIBERDADE E DO AUTORITARISMO

Somos uma instituiçªo independente e apartidÆria de pesquisas interdisciplinares, comprometida em produzir e disseminar conhecimento sobre a qualidade do estado de direito e da democracia. Nosso objetivo
Ø monitorar as manifestaçıes do autoritarismo e de repressªo às liberdades para fundamentar a mobilizaçªo da sociedade civil e a defesa das liberdades.

Gestªo

Conrado Hübner Mendes (Diretor Presidente), Rafael Mafei Rabelo Queiroz (Diretor Vice-Presidente), Adriane Sanctis (Diretora e Gerente de Pesquisa) e Carolina C.B. Cooper (Gerente de estratØgia e operaçıes).

Maio de 2022

Apoio

FORD FOUNDATION

A realização desta publicação foi possível devido ao apoio da Fundação Ford

Responsáveis pelo projeto

Pesquisa e redação:
Anna Carolina Venturini, Pedro Ansel, Marina Slhessarenko Barreto, Yuri Marcelo Oliveira e Ana Silva Rosa

Edição
Iara Crepaldi

Revisão
House of Words

Projeto Gráfico
Atonal Studio

Diagramação
Raul Sanches Gonzalez

Sugestão de Citação
Venturini, A. C.; Ansel, P.; Barreto, M.S.; Oliveira, Y.M.; Rosa, A. S. (2022). *Vigilância & vigilantismo: conceitos, legislação brasileira e organizações atuantes.* São Paulo. Centro de Análise da Liberdade e do Autoritarismo (LAUT)

CABF CB8B CF8F

Índice

Introdução

O tema da vigilância e do vigilantismo tem sido cada vez mais discutido no Brasil e no mundo, principalmente por conta dos desenvolvimentos tecnológicos que permitem a captura de dados biométricos e também por conta da crescente coleta de dados pessoais. Todos os dias dividimos uma quantidade imensa de informações sobre nossos hábitos e comportamentos com empresas privadas, donas de tecnologias digitais como celulares, tablets, aplicativos e muitas outras.

As pessoas também são monitoradas constantemente pelo Estado. Desde muito antes de existirem celulares e computadores, o Estado produz registros cadastrais sobre sua população, sobre quando nascemos, onde, qual é a nossa renda anual e se utilizamos serviços públicos. Ademais, o Estado pode promover diretamente o monitoramento da população pelas atividades de policiamento, inteligência e até de espionagem. No entanto, esse controle sobre os nossos dados nem sempre é autoritário e abusivo. Para que existam políticas públicas adequadas às demandas da população, é necessário que uma série de dados coletados pelos entes públicos seja analisada por pesquisadores e especialistas para a formulação de políticas públicas baseadas em evidências.

A vigilância e o vigilantismo são fundamentais para pensarmos sobre a democracia e o Estado de Direito hoje. Em sistemas não democráticos e autoritários, o poder ligado ao uso de tecnologias de vigilância pode afetar o desenvolvimento democrático e levar a graves abusos dos direitos humanos. São recorrentes os casos em que ativistas de oposição, defensores de direitos humanos e jornalistas são colocados sob vigilância governamental e têm suas comunicações lidas, às vezes de forma legítima e outras de forma ilegal.

A coleta de um grande número de dados por parte do Estado também traz questões relevantes relacionadas à segurança de seu armazenamento, a finalidade da coleta e o tratamento dos dados e os riscos da centralização de dados em bancos únicos. Por conta disso, muitos países começaram a revisar

suas leis sobre vigilância, privacidade e proteção de dados pessoais, com o objetivo de garantir mais segurança às pessoas e ao compartilhamento de seus dados e informações pessoais pelo Estado e por empresas privadas.

Além disso, quando falamos de tecnologia, é impossível não pensar em discriminação. Nos últimos anos, muitas pesquisas têm mostrado como as tecnologias automatizadas e inteligências artificiais reproduzem vieses, estereótipos e acabam sendo discriminatórias. A falta de diversidade no setor de tecnologia é notável e amplamente pesquisada. Muitos estudos mostram a sub-representação de mulheres e minorias nas áreas de ciência, tecnologia, engenharia ou matemática, seja no ensino superior ou no mercado de trabalho. E a ausência de pessoas com diferentes identidades, trajetórias e experiências gera efeitos nas tecnologias que são desenvolvidas. Isso porque a maioria delas depende de programação, isto é, de uma pessoa que irá desenvolver o código — chamado de algoritmo — necessário para que aquilo funcione. Há um número crescente de organizações que dependem de algoritmos para auxiliar na tomada de decisões, mas se a indústria de programação e inteligência artificial for composta apenas por um grupo — de homens brancos — isso pode levar a um viés nos sistemas.

Com isso em mente, o presente dossiê apresenta conceitos fundamentais sobre a temática e os dados de como a vigilância e o vigilantismo têm se manifestado no Brasil. Além disso, este documento pretende oferecer um panorama inicial sobre o ecossistema de organizações que atuam nesses temas, no Brasil e no mundo. Os dados apresentados são resultado de mapeamentos não exaustivos feitos pelos pesquisadores do LAUT a partir de notícias e publicações a respeito das temáticas.

Esse panorama contém seis partes, incluindo esta introdução. A segunda parte apresenta o conceito de vigilância, dados sobre projetos de lei ligados à questão da proteção de dados pessoais e casos emblemáticos de vazamentos de dados pessoais de brasileiros. A terceira parte se dedica à questão do reconhecimento facial, de como essa tecnologia tem sido adotada no país e como ela tem sido abordada em projetos de lei relacionados a dados biométricos, inteligência artificial e reconhecimento facial. Na parte quatro, abordamos o vigilantismo e como ele se manifesta dentro e fora do ambiente digital, incluindo casos de vigilantismo que foram destaque na imprensa brasileira. A quinta parte traz um mapeamento de organizações do Brasil e do mundo que abordam a temática da vigilância e do vigilantismo de forma direta ou indireta. Por fim, a última parte traz exemplos de organizações não governamentais que têm utilizado tecnologias digitais para auxiliar a população e suprir, em certa medida, a ausência ou inação do poder público.

Vigilância dentro e fora dos ambientes digitais

O que é vigilância? Como pode afetar nossas liberdades e resultar em discriminações e outras violações de direitos? Entenda o conceito e como suas manifestações se fazem presentes em nosso dia a dia.

Vigilância

Refere-se a atividades de monitoramento e fiscalização exercidas por agentes públicos ou privados. No campo da segurança pública temos como exemplo de vigilância o patrulhamento policial que objetiva garantir o direito constitucional dos cidadãos à segurança e à ordem pública. Empresas privadas estão aptas a realizar atividades de vigilância, desde que devidamente homologadas pelo poder público, geralmente oferecendo serviços de segurança privada para outras organizações e pessoas, nos termos da **Lei nº 7.102/1983**. Instituições da sociedade civil, como organizações não governamentais (ONGs) e conselhos — estaduais, federais e municipais — também podem assumir o papel de fiscalizadores. A vigilância dentro dos limites legais deve respeitar principalmente o direito à privacidade das pessoas que estão sendo vigiadas.

Vigilância Digital

A vigilância digital está relacionada ao ato de vigiar as condutas dos indivíduos nos ambientes digitais (redes sociais, sites, aplicativos e outras plataformas conectadas à internet). Grande parte da vigilância digital é viabilizada por meio da coleta dos chamados rastros digitais, informações que deixamos para trás ao clicarmos em um anúncio publicitário ou quando fazemos um cadastro para ter acesso a alguma plataforma online, por exemplo. Muitos dos dados produzidos como resultado de

nossas atividades nos meios virtuais são os chamados dados pessoais, informações que podem nos identificar direta ou indiretamente, como CPF, número de telefone e até localização.

Atualmente, é cada vez mais comum que empresas atuantes em diferentes setores coletem dados pessoais. Espalhados por cerca de 440 milhões de dispositivos digitais em uso no Brasil, os dados são usados para mapear hábitos de consumo com o objetivo de desenvolver produtos mais atrativos para os públicos-alvo das empresas. De forma análoga, o poder público também mantém vigilância constante sobre os cidadãos por meio do processamento de dados pessoais que circulam na internet. Porém, em vez de objetivar formas de aumentar suas receitas como as empresas, utiliza os dados para viabilizar ações como distribuição de benefícios sociais, elaboração de políticas públicas e investigações policiais.

Até 2018, não existia uma lei específica no Brasil para regular a aquisição ou compartilhamento de dados pessoais. **A Lei Geral de Proteção de Dados (LGPD)** estabeleceu, a partir de então, que "*toda pessoa natural tem assegurada a titularidade de seus dados pessoais*". Além disso, determinou outros dispositivos legais que, em tese, dão aos cidadãos um maior controle sobre a vigilância digital. O *artigo 5º* da LGPD também definiu os tipos de dados pessoais: (a) o *dado pessoal* é a "informação relacionada a pessoa natural identificada ou identificável", (b) o *dado pessoal sensível* é 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[1]", e (c) o *dado anonimizado* é o "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

[Linha do Tempo] Legislação sobre proteção de dados pessoais

Principais marcos legais relacionados à proteção de dados pessoais no Brasil

Novembro de 2010

Ministério da Justiça inicia 1ª **consulta pública** para discutir **anteprojeto de lei** sobre proteção de dados pessoais na internet. O texto aborda: proteção de dados no setor público e privado, regras para troca de informações de clientes entre instituições financeiras e regulamentação da proteção de dados pessoais como política para garantir o direito à privacidade e a liberdade dos cidadãos. Também visa à criação do Conselho Nacional de Proteção de Dados Pessoais.

1 Pessoa natural é todo ser humano capaz de direitos e deveres na ordem civil, segundo o Código Civil Brasileiro (Lei 10.406/2002).

Agosto de 2011

Marco Civil da Internet (Projeto de lei nº 2126/2011) é enviado ao Congresso Nacional. PL prevê princípios, garantias, direitos e deveres para uso da internet no Brasil, estabelecendo que todos os envolvidos na transmissão dos dados são obrigados a tratá-los de forma igualitária e sem discriminações. A "constituição da internet", como ficou conhecido o projeto, reconhece princípios constitucionais como liberdade de expressão, privacidade e direitos humanos nos ambientes virtuais.

Novembro de 2011

Lei de Acesso à Informação (**LAI**) — Lei nº 12.527/2011 — é sancionada. Institui como princípio fundamental o acesso a documentos públicos, permitindo que qualquer brasileiro solicite dados referentes à administração pública, em nível federal, estadual ou municipal, incluindo todos os poderes (Executivo, Legislativo e Judiciário). Também acaba com a possibilidade de sigilo eterno que protegia a publicação de documentos oficiais e determina que entidades públicas divulguem proativamente um rol mínimo de informações sobre suas atividades por meio da internet. É importante destacar que, enquanto a LAI regula o acesso a informações e documentos públicos, a legislação do *habeas data* (art. 5º, LXXII da **CF 1988** e **Lei n.º 9.507/1997**) dispõe sobre o acesso a informações privadas de cidadãos coletadas pelo Estado, com o objetivo de garantir os direitos fundamentais à privacidade, intimidade e informação.

Junho de 2012

É apresentado o Projeto de Lei nº 4060/2012 para regulamentar o tratamento de dados pessoais, com o objetivo de criar legislação específica sobre a temática. Tratamento de dados pessoais representa o cruzamento de dados e informações de uma pessoa ou de um grupo para direcionar políticas públicas, decisões comerciais e de consumo, bem como a atuação de órgão público. O cruzamento envolve o agrupamento de informações armazenadas em bases de dados de diferentes instituições. O PL prevê como regra que o tratamento dos dados pessoais seja condicionado à permissão de seus titulares.

Dezembro de 2012

Entra em vigor a **Lei Carolina Dieckmann (Lei nº 12.737/2012)**, que agrega ao **Código Penal Brasileiro** a tipificação de crimes e delitos cibernéticos por meio de invasões a dispositivos eletrônicos (artigos 154-A e 154-B). A lei foi motivada por um episódio de grande repercussão na mídia: a atriz Carolina Dieckmann teve o computador pessoal invadido e fotos íntimas suas foram divulgadas na internet.

Agosto de 2013

Marco regulatório sobre proteção de dados pessoais é apresentado no Senado, sob o formato do **Projeto de Lei nº 330/13**. O **PL** versa sobre regras para coleta de dados no Brasil, tendo como fundamento os princípios da dignidade da pessoa humana, da proteção da privacidade, da garantia da liberdade e da inviolabilidade da imagem das pessoas. Também estabelece que dados pessoais não podem ser utilizados com intuito de prejudicar cidadãos.

Abril de 2014

Aprovação do **Marco Civil da Internet**, 1º lei brasileira a estabelecer direitos, garantias, princípios e deveres para **uso da internet no país**. Lei nº **12.965** prevê que a internet deve respeitar o princípio da neutralidade de rede, ou seja, todas as informações em rede devem trafegar de maneira isonômica, independentemente de seu conteúdo, origem, destino, serviço ou aplicação. Estabelece a liberdade de expressão como princípio básico para o funcionamento da internet e a"inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação" (Art. 7º, inciso I).

Janeiro de 2015

Ministério da Justiça realiza nova **consulta pública** para discutir a proteção de dados pessoais armazenados dentro ou fora do Brasil. A consulta, inspirada nos moldes do Marco Civil da Internet, visa afundamentar o direito à fiscalização por parte de cidadãos e cidadãs sobre como terceiros coletam e utilizam os seus dados. Também traz para o debate público a delimitação dos conceitos de dados pessoais (informações que possibilitam a identificação de indivíduos), dados anônimos (que não identificam seus titulares) e dados sensíveis (informações passiveis de gerar discriminação de raça, religião, preferências políticas, entre outras), bem como diretrizes para protegê-los.

Maio de 2016

Câmara dos Deputados inicia a tramitação do **Projeto de Lei nº 5276/2016**. PL é resultado do **debate público** promovido pelo Ministério da Justiça e versa sobre aumento da proteção de dados, embasado na "garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural''.

Maio de 2018

PLC nº 53/2018, considerado base para a LGPD, é aprovado na Câmara. Tem origem na anexação de outros três PLs que tratam do tema da proteção de dados pessoais: **PL nº 5.276/2016**, **PL nº 4.060/2012** e **PLS nº 330/2013**. Nova proposta para a proteção de dados no Brasil tem influência direta da recém-aprovada **General Data Protection Regulation (GDPR)**, de 25 de maio de 2018, que traçou as diretrizes da **proteção de dados na União Europeia**.

Julho de 2018

PLC 53/2018 é **aprovado por unanimidade no Senado**. Visa a regulamentar a proteção, transferência e utilização de dados pessoais. Também prevê a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão vinculado ao Ministério da Justiça, para auxiliar no controle e fiscalização da circulação de dados. Dispõe, ainda, sobre punições, multas e suspensão do exercício de atividades de empresas caso haja infrações relativas ao tratamento de dados e informações.

Agosto de 2018

LGPD – Lei Federal 13/709/2018 – é sancionada pelo então presidente Michel Temer e publicada no Diário Oficial da União com prazo de 18 meses para entrar em vigência. Esse marco legal, que regulamenta transferência, uso e proteção de dados pessoais no Brasil, é constituído em consonância com parâmetros internacionais de proteção de dados. Estabelece a titularidade de cidadãos brasileiros sobre seus dados nos meios físicos e digitais, de modo que o tratamento de dados pessoais e sensíveis por instituições públicas e privadas passa a ser condicionado à autorização dos titulares, exceto em casos como cumprimento de dever legal ou criação de políticas públicas. Também fixa o compromisso da transparência em relação às operações efetuadas com dados pessoais dos titulares. Em caso de descumprimento da LGPD, estão previstas sanções administrativas como multas e bloqueio de atividades relacionadas ao tratamento de informações.

Junho de 2019

É criada a Subcomissão de Biometria e Privacidade no âmbito da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara.

Julho de 2019

Proposta de Emenda Constitucional **(PEC) 17/2019**) é apresentada no Senado. Seu objetivo é inserir a proteção de dados pessoais, inclusive nos meios digitais, na Constituição de 1988, reconhecendo a proteção de informações pessoais como direito fundamental no ordenamento jurídico brasileiro.

Outubro de 2019

Governo federal emite o **Decreto 10.046/2019**, regulamentando o compartilhamento de dados entre órgãos da administração pública federal, e cria o **Cadastro Base do Cidadão (CBC)**, construído a partir de bases de dados de distintos órgãos governamentais. O Cadastro cruza dados dessas bases e informações pessoais como CPF, nome, data de nascimento, filiação etc. O argumento utilizado para sua criação é o papel que desempenharia na construção de melhores políticas públicas.

Setembro de 2020

Após uma série de adiamentos, a LGPD entra em vigor. A tramitação do texto conta com a participação ativa de organizações da sociedade civil e amplia o alcance das diretrizes de proteção de dados estabelecidas pelo Marco Civil da Internet. Com a vigência da **LGPD**, instituições públicas e privadas são obrigadas a adequar suas práticas de armazenamento, disponibilização e coleta de informações na internet às novas normas legais. Órgãos do Poder Judiciário também tiveram que adotar medidas para que seus tribunais se adequassem às disposições dessa legislação.

Novembro de 2020

ANPD é efetivada. Novo órgão da administração pública federal passa a ser responsável pela implementação, fiscalização e regulamentação do cumprimento da LGPD. Dentre as principais **competências da ANPD** estão: promoção da cooperação com autoridades de proteção de dados pessoais de outros países, fornecimento de informações para a população sobre normas e políticas públicas de proteção de dados pessoais e medidas de segurança, bem como fiscalização e aplicação de sanções em caso de descumprimento da lei. Presidente Jair Bolsonaro escolhe **três militares para ocupar a direção da ANPD**.

Março de 2021

No âmbito da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI), é apresentado o **requerimento 8/2021**, solicitando a "realização de Audiência Pública para atualizar o debate acerca da questão das tecnologias de reconhecimento facial para aplicação em segurança pública e em outros sistemas de facilitação do dia a dia no Brasil".

Maio de 2021

Ministério da Justiça realiza pregão virtual para adquirir o **software de espionagem Pegasus**. Esse programa de computador usado para espionagem permite acessar celulares e computadores pessoais e coletar dados neles armazenados sem consentimento de proprietários. Descoberto em 2016, é um spyware — tecnologia de espionagem para, supostamente, coibir ação de criminosos e terroristas. Nos últimos anos, porém, governos de países como México, Índia e Arábia Saudita foram flagrados utilizando esse programa para invadir celulares e monitorar conversas de opositores políticos. O processo de licitação, no valor de R$ 25,4 milhões, conta com participação ativa do vereador **Carlos Bolsonaro** (Republicanos), que foi a Israel em 2019 tratar do tema com representantes da empresa fornecedora da tecnologia. Os órgãos beneficiados seriam a Agência Brasileira de Inteligência (Abin) e o Gabinete de Segurança Institucional (GSI). O pregão eletrônico da licitação acaba suspenso pelo Tribunal de Contas da União (TCU).

Julho de 2021

Diretor Geral da Polícia Federal (PF) assina contrato para compra e implementação do sistema **ABIS – Solução Automatizada de Identificação Biométrica**, que permitiria identificação de pessoas com coleta, armazenamento e cruzamento de dados da impressão digital e reconhecimento facial. Segundo a PF, o sistema ABIS poderia proporcionar a unificação de dados das Secretarias de Segurança Pública (SSPs), possibilitando a polícias estaduais acesso à base biométrica nacional. Diversas entidades **acionam a ANPD**, com o argumento de que o sistema traria risco à privacidade dos indivíduos e à proteção de informações.

Agosto de 2022

Entra em vigor a aplicação de sanções em caso de descumprimento da LGPD, que estabelece que as instituições devem justificar a coleta de dados pessoais e solicitar autorização de uso para o proprietário das informações. Sanções são aplicadas pela ANPD e variam de acordo com o grau de impacto e a gravidade da infração à lei, podendo incluir advertência, multas diárias, multas simples de até 2% do faturamento das empresas, multas de publicização da infração, bloqueio ou eliminação de dados pessoais, suspensão e até a proibição parcial ou total das atividades da empresa violadora.

Fevereiro de 2022

É promulgada no Congresso Nacional a **Emenda Constitucional (EC) 115**, que altera a Constituição para incluir a proteção de dados pessoais no rol de direitos fundamentais e estabelece a competência privativa da União para legislar sobre questões de proteção e tratamento de informações pessoais. Assim a proteção de dados pessoais se torna, oficialmente, um direito constitucional ("Art. 5º, inciso LXXIX — é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.").

[Linha do Tempo] Casos de vazamentos de dados

Casos de vazamentos de dados no Brasil que ganharam destaque na imprensa

Julho de 2007

Por conta dos Jogos Pan-Americanos, a extinta Secretaria de Estado de Segurança do Rio de Janeiro adquire o **sistema de interceptação telefônica Guardião**, que permite o acesso a dados gerados por voz a partir de terminal telefônico — a chamada escuta telefônica. **Depois do Pan, o sistema é adquirido por diversas superintendências da PF e pelo Ministério Público** (MP) de alguns estados para ser utilizado, principalmente, em operações de combate à corrupção.

Junho de 2011

PF investiga **suspeito de violar e-mail de Dilma Rousseff**, que teria acessado boletins médicos e documentos sigilosos do Superior Tribunal Militar (STM) que estavam no correio eletrônico da presidente. A partir da invasão do site do Partido dos Trabalhadores (PT), durante corrida presidencial do ano anterior, o cibercriminoso (quem usa conhecimentos em programação para invadir sistemas) teria conseguido acesso ao e-mail de Dilma Rousseff e copiado cerca de 600 mensagens. O conteúdo seria vendido para a imprensa e partidos políticos de oposição à ex-chefe do Poder Executivo. Governo federal informa ter dificuldades para confirmar se e-mails de fato foram extraídos ilegalmente.

Setembro de 2013

Imprensa divulga **documentos vazados por Edward Snowden** revelando que o governo brasileiro foi alvo de espionagem da Agência de Segurança Nacional dos Estados Unidos (NSA, em inglês). Considerado o maior sistema de espionagem do mundo, a NSA monitorou números de telefones, e-mails e IPs (identificação de computadores) para interceptar conversas da chefe do executivo brasileiro e de seus principais assessores. Um dos softwares utilizados na empreitada de vigilância foi o "DNI selectors", capaz de rastrear as ações de usuários na internet. Nos documentos não constam quais informações foram interceptadas nem os interesses dos EUA em tal ação.

Dezembro de 2017

Empresa Netshoes reporta **megavazamento de dados de clientes**. Falhas na segurança cibernética da plataforma permitiram que criminosos virtuais se apropriassem e divulgassem listas com informações de quase dois milhões de usuários cadastrados. Entre os dados expostos constavam nomes completos, produtos adquiridos, CPFs, e-mails e datas de nascimento. Segundo o Ministério Público do Distrito Federal e dos Territórios (MPDFT), responsável pela apuração do caso, foi um dos **maiores incidentes de segurança** de dados registrados no Brasil.

Abril de 2018

Facebook anuncia que **empresa de consultoria se apropriou indevidamente dos dados** de mais de 87 milhões de usuários; 443 mil eram brasileiros. Com a autorização do Facebook, a empresa Cambridge Analytica circulou na rede social um teste psicológico, no qual os dados referentes a traços de personalidade eram coletados sem autorização — e ofereceu as informações coletadas ilegalmente para auxiliar na campanha presidencial de Donald Trump, apontando quais usuários do Facebook teriam perfis compatíveis para receber e divulgar as bandeiras do candidato Republicano em seus perfis na rede social.

Maio de 2018

Comissão da Verdade do estado de São Paulo revela que reitorias das principais instituições de ensino superior do país contribuíram com o regime militar. Segundo **documento produzido pela Comissão**, a **Universidade Federal de Santa Catarina (UFSC) e a Universidade de São Paulo (USP) repassavam informações sobre posições ideológicas de alunos e professores para o Serviço Nacional de Informações (SNI)**. Além de entregar relatórios sobre alunos e docentes, a espionagem contava com a atuação de membros do governo federal infiltrados nos ambientes universitários. Comissão também apontou indícios da atuação de espiões do regime militar nas Universidades Federais da Bahia, do Espírito Santo e do Rio Grande do Norte, além da PUC-SP e da Universidade de Brasília.

Fevereiro de 2019

Pacote anticrime do ministro Sérgio Moro estabelece legalmente a figura do agente policial disfarçado, cuja ação está situada entre campanha policial e infiltração policial. Além de relativo grau de expertise, o agente disfarçado deve possuir habilidade para atuar descaracterizado de forma a permitir a coleta de provas de um crime e a investigação de autoria, sem interferir no curso causal da ação criminosa.

Setembro de 2019

Documentos sigilosos da PF mostram que **agentes de segurança pública se infiltraram em reuniões de movimentos sociais e nos protestos de junho de 2013**. Nomes dos líderes dos movimentos sociais foram identificados, assim como dados dos cidadãos que participaram dos atos, seus comentários nas redes sociais e carros. E os infiltrados se camuflaram nos grupos “black blocks”, manifestantes em geral vestidos de preto e mascarados conhecidos por realizar ações diretas nos protestos. Apesar desse tipo de atuação das autoridades ser completamente invasiva e potencialmente violadora das liberdades de expressão e manifestação, a **PF respondeu aos jornais na época que “agiu legalmente e cumprindo seu trabalho”**.

Junho de 2020

Imprensa revela **caso de vigilância digital comandado pela Agência Brasileira de Inteligência (Abin)**. O órgão central do Sistema Brasileiro de Inteligência (SISBIN) realizou uma manobra administrativa considerada ilegal na tentativa de obter os dados da carteira nacional de habilitação (CNH) de mais de 76 milhões de brasileiros. Na ocasião, a ABIN solicitou ao Serviço Federal de Processamento de Dados (SERPRO), a maior empresa pública de serviços de tecnologia do país, que extraísse do banco de dados do Registro Nacional de Carteira de Habilitação (Renach), informações dos veículos, números de telefones, endereços, filiação, telefones, dados dos veículos e fotos dos portadores de CNH do país, quase 40% da população brasileira. Informações

seriam entregues ao governo federal. Ação movida no **Supremo Tribunal Federal (STF)** alega que a Abin violou o direito à privacidade, à proteção de dados pessoais e à autodeterminação informativa, além de afrontar a dignidade da pessoa humana.

Julho de 2020

A Secretaria de Operações Integradas (SEOPI), órgão do Ministério da Justiça e Segurança Pública criado pelo ex-ministro Sérgio Moro, é acusada de ter **monitorado dados pessoais de 579 servidores públicos federais, estaduais e professores universitários listados como antifascistas** e críticos ao governo Jair Bolsonaro. O órgão teria produzido dossiê com nomes e, em alguns casos, fotografias e endereços de redes sociais das pessoas monitoradas e distribuído um relatório às administrações públicas federal e estaduais. O partido Rede Sustentabilidade questiona no STF as investigações sigilosas conduzidas pela Seopi. Tribunal classifica a prática como "abuso da máquina estatal" o recolhimento de informações "de servidores com postura política contrária ao governo" e, assim, determina a suspensão de qualquer ação dessa natureza pelo governo federal.

Agosto de 2020

Rede Sustentabilidade e PSB questionam no STF a interpretação que parecia ser um poder legal da **Agência Brasileira de Inteligência** (ABIN) de requisitar compulsoriamente informações sensíveis e dados sigilosos, como sigilo fiscal, relatórios do COAF e sigilos telefônicos, por exemplo. **No julgamento, a Corte decidiu que só podem ser fornecidos dados e conhecimentos específicos à Abin** quando for comprovado o interesse público da medida, afastando qualquer possibilidade de que esses dados sirvam a interesses pessoais ou privados. Também decidiu ser imprescindível a instauração de procedimento formal e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

Novembro de 2020

Superior Tribunal de Justiça (STJ) informa que seu sistema de informática foi alvo de ataque cibernético. De acordo com investigação, falha no sistema de segurança na rede do STJ teria permitido que criminosos cibernéticos bloqueassem o acesso de magistrados e funcionários aos arquivos da corte. Como medidas de segurança, e-mails institucionais foram tirados do ar e pessoas que trabalhavam no tribunal foram orientadas a não utilizar seus computadores. O ataque cibernético ocorreu no momento da realização de sessões de julgamento, que tiveram de ser suspensas até a área técnica restabelecer a segurança

Junho de 2021

Governador do Rio de Janeiro **sanciona lei que determina implantação de câmeras de vídeo e áudio em uniformes de policiais e em aeronaves** das forças de segurança. Aprovação gera discussões, já que o **governador Cláudio Castro vetou trechos importantes**, como os que estabeleciam prazos para instalação dos equipamentos, determinavam a disponibilização de registros de áudio e vídeo no ato do registro de ocorrência, com objetivo de atestar a inviolabilidade do material, e, ainda, que garantiam o acesso ao material a "todo e qualquer cidadão" envolvido diretamente na ação.

Janeiro de 2021

Megavazamento de dados de 223 milhões de brasileiros é noticiado. **Bases de dados** contendo informações como nomes completos, datas de nascimento, CPFs, gênero e endereços residenciais de pessoas vivas e falecidas foram negociados por criminosos digitais em fóruns da *dark web* (zona da internet onde as atividades são mais difíceis de serem rastreadas). Os crackers também ofereciam listas contendo informações como escolaridade, benefícios do Instituto Nacional do Seguro Social (INSS), programas sociais, renda e avaliações de crédito. Parte dos dados foi oferecida gratuitamente e 37 pacotes de dados estavam sendo vendidos. PF prendeu dois suspeitos do crime.

Agosto de 2021

Rede interna da Secretaria do Tesouro Nacional é alvo de *ransomware*, ataque virtual no qual um computador tem seus dados criptografados, impedindo que possam ser acessados. Em geral, criminosos exigem resgate (*ransom*) para liberar os dados. Em nota, o Ministério da Economia esclareceu que, apesar do ataque, nenhum tipo de dano nos sistemas do Tesouro Nacional havia sido identificado pelos especialistas.

Dezembro de 2021

Site do Ministério da Saúde (MS) sofre **ataque virtual**. Página é retirada do ar e, no lugar, lê-se apenas a seguinte mensagem do grupo que assumiu a autoria do ataque: "os dados internos dos sistemas foram copiados e excluídos. 50 TB de dados está em nossas mãos. Nos contate caso queiram o retorno dos dados". O **Portal Covid e o Portal Conecte Sus também são derrubados** pelos criminosos virtuais. PF e GSI são acionados para apurar o caso.

Vigilância e tecnologias de reconhecimento facial

No Brasil e em diversos países, as tecnologias de reconhecimento facial e seu uso para vigilância ou combate a fraudes têm levantado intensas discussões, em decorrência da multiplicação de casos de discriminação algorítmica que vem ocasionando erros e a punição de pessoas inocentes.

Destacamos abaixo conceitos fundamentais para a compreensão desse debate, bem como os principais usos das tecnologias de reconhecimento facial que mapeamos no Brasil e projetos de lei que têm por finalidade regular o uso dessas tecnologias e da inteligência artificial no país.

Algoritmos

Os **algoritmos** podem ser entendidos como sequências de códigos (regras, instruções, operações ou raciocínios) que devem ser seguidas para resolver um problema ou atingir um determinado objetivo, uma espécie de receita. Os algoritmos estruturam tudo que é feito em computadores e, consequentemente, no mundo virtual. Em geral, esses códigos são escritos por desenvolvedores da indústria da tecnologia, que estabelecem todos os passos para o funcionamento de softwares e equipamentos como computadores, celulares, câmeras de monitoramento, entre outros. Recentemente, vêm sendo alvo de críticas, por afetar a qualidade das esferas públicas e o equilíbrio de poderes tanto no setor privado quanto no público. Além disso, são passíveis de crítica pela falta de transparência de seus mecanismos, o que reforça a possibilidade de manipulações. No setor privado, por exemplo, oportunizam a criação de bolhas de reprodução de opiniões e posicionamentos – a exemplo dos clusters em torno de assuntos de esquerda versus direita em redes sociais – e publicidade direcionada. Portanto, são elementos fundamentais não só para o funcionamento dos sistemas de vigilância, mas também para a existência de qualquer software e tecnologia digital.

Discriminação algorítmica e inteligência artificial (IA)

A discriminação algorítmica ocorre quando existe distinção na abordagem de conteúdos digitais em razão de vieses assumidos pelos algoritmos (em razão da forma como seus códigos foram elaborados). Esse tipo de discriminação tem sido frequentemente atrelado à inteligência artificial, um ramo de pesquisa da ciência da computação que busca, por meio de mecanismos computacionais, a construção de máquinas capazes de executar tarefas que normalmente exigem inteligência humana, como a resolução de problemas cotidianos. É importante destacar que a inteligência artificial é uma categoria ampla, a qual não se confunde com o aprendizado de máquina (ou "**machine learning**" em inglês), pois esse é apenas um dos seus recursos. Softwares com machine learning são programas que podem melhorar automaticamente de acordo com o número de dados por eles processados.

Uma vez instruídos por seus programadores/desenvolvedores com critérios de importância, os algoritmos de IA podem segregar ou evidenciar informações. As formas mais frequentes de **discriminação algorítmica** são o racismo e o sexismo; estudos apontam que isso se dá pelo fato da indústria da tecnologia ser composta, majoritariamente, por homens brancos, fazendo com que os critérios de importância com os quais os algoritmos são produzidos assumam, muitas vezes, premissas sexistas e racistas para classificar informações no mundo digital. Em 2018, a gigante da tecnologia Amazon criou um algoritmo de inteligência artificial que selecionava currículos para vagas de emprego, mas a empresa acabou tirando a tecnologia de circulação após perceber uma forte tendência em desclassificar mulheres dos processos seletivos. Por sua vez, a preferência por selecionar rostos de pessoas brancas em fotos contendo pessoas negras e brancas fez com que a rede social Twitter descontinuasse, em 2020, o algoritmo que realizava recortes automáticos de fotos antes de serem postadas pelos usuários.

Tecnologias de reconhecimento biométrico

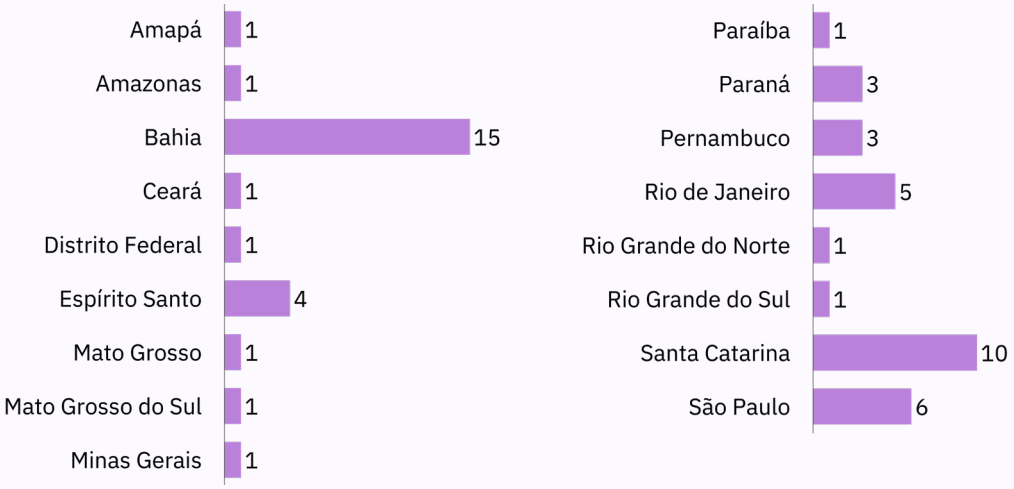
A biometria pode ser definida como a análise de características físicas, morfológicas e comportamentais para fornecer a identificação de um indivíduo, partindo do princípio que tais características são singulares e imutáveis ao longo do tempo. As tecnologias de reconhecimento biométrico respondem a métodos automatizados para verificar ou reconhecer a identidade de uma pessoa com base na metrificação de suas características físicas, dentre elas, a curvatura dos lábios, a distância entre os olhos, o formato das impressões digitais e até a disposição dos vasos sanguíneos que irrigam a retina. Nem sempre percebemos, mas o nosso cotidiano é permeado por essas tecnologias; as mais comuns são a leitura da impressão digital (utilizada para emissão de documentos como RG e CNH) e o reconhecimento facial.

As tecnologias de reconhecimento facial permitem que o rosto de uma pessoa seja digitalizado e associado automaticamente a um banco de dados. Nos últimos anos, o reconhecimento facial tem sido usado para o desbloqueio de aparelhos celulares, para a liberação do ingresso de uma pessoa em edifícios, para o controle de acesso em escolas e para o registro de ponto de funcionários, bem como para a localização de pessoas foragidas da justiça, por meio de câmeras espalhadas pelo espaço público e conectadas às autoridades policiais. Além disso, essas tecnologias têm sido utilizadas no transporte público sob o argumento de evitar fraudes. Importante destacar que nem todas as câmeras de videomonitoramento instaladas em cidades e edifícios possuem a tecnologia de reconhecimento facial – estas são câmeras específicas que só recentemente vêm sendo instaladas em espaços públicos, privados e meios de transporte.

As tecnologias de reconhecimento facial têm levantado intensas discussões no campo da Segurança Pública pelo mundo, em decorrência da multiplicação de casos de **racismo algorítmico** que vêm ocasionando erros de reconhecimento facial de pessoas negras e levando inocentes à prisão. Também são apontadas como responsáveis pela propagação do racismo estrutural. De acordo com **O Panóptico**, projeto do Centro de Estudo de Segurança e Cidadania – **CESeC**, cerca de 90% das prisões no Brasil com base nestas tecnologias têm como alvo a população negra.

Em um mapeamento não exaustivo realizado a partir de notícias da imprensa brasileira, identificamos iniciativas do poder público e de agentes privados focadas na implementação de tecnologias de vigilância baseadas em reconhecimento facial em diferentes áreas. Essas iniciativas estão localizadas em 56 cidades, de 17 estados do país. Nota-se que a Bahia é o estado com maior número de iniciativas (15), seguida de Santa Catarina (10) e São Paulo (6).

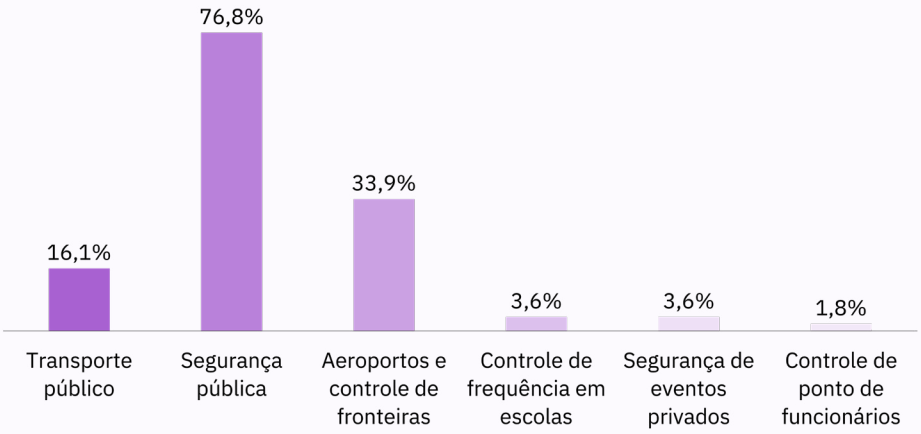
[Gráfico] Distribuição das 56 iniciativas por estados da federação



Com relação à distribuição das áreas de interesse na implementação do reconhecimento facial em cada estado, é possível notar um número maior de estados investindo nessas tecnologias nas áreas de segurança pública[2] e em aeroportos e controles de fronteira[3]. Na segurança pública, por exemplo, o estado com maior proporção de iniciativas nessa área é a Bahia, com 34,9%, seguida de Santa Catarina, com 23,3%. Já no transporte público[4], o estado que se destaca é São Paulo, com 22,2% das iniciativas, enquanto os demais estados adotantes apresentam 11,1% cada. O estado de São Paulo também se destaca na área de aeroportos e controle de fronteiras, já que apresenta a maior proporção de municípios com esse tipo de tecnologia sendo implementada em seus aeroportos (21,1%).

Ao olharmos a distribuição das iniciativas nas diferentes áreas, nota-se a predominância da área de segurança pública (76,8%), seguida dos aeroportos e controle de fronteiras (33,9%) e do transporte público (16,1%). Ademais, verifica-se a aplicação das tecnologias de reconhecimento facial para controle de frequência em escolas, para controle de ponto de funcionários e para segurança em eventos privados como festivais e estádios[5].

[Gráfico] Distribuição das 56 iniciativas que visam à implementação das tecnologias de reconhecimento facial por área de atuação



2 Nessa área, o uso mais comum é para a localização de pessoas consideradas "foragidas" e identificação de suspeitos de crimes. As câmeras de vigilância com tecnologias de reconhecimento facial são espalhadas por espaços públicos e conseguem digitalizar o rosto de uma pessoa e associá-la automaticamente a um banco de dados de autoridades de segurança pública.

3 Uso para viabilizar 100% do processo deembarque por meio da biometria facial, bem como identificar pessoas suspeitas do cometimento de crimes ou condenadas pela justiça, bem como identificar placas de carros que cruzam as fronteiras.

4 O uso mais frequente nessa área tem sido para confirmar a identidade das pessoas que utilizam o transporte público e têm direito a gratuidade ou isenção de tarifa, de modo a identificar casos de fraudes no uso do benefício.

5 Vide os casos do Mineirão (Belo Horizonte, MG) e da Oktoberfest (Blumenau, SC) mencionados na linha do tempo a seguir.

Nota-se que as primeiras iniciativas de reconhecimento facial no país foram implementadas em 2011 (11%), percentual que cresceu para 16% em 2016 e para 37% nos anos de 2021 e 2022.

[Linha do Tempo] Tecnologias de reconhecimento facial no Brasil

Casos de implementação e proposição dessas tecnologias no Brasil e questionamentos sobre seu uso por pesquisadores e pela sociedade civil

Abril de 2011

Um dos primeiros sistemas de reconhecimento facial foi implementado no Brasil, por meio de projeto piloto realizado em duas prestadoras de serviço de transporte público de ônibus na cidade de Ilhéus (BA). Ao todo, 139 veículos receberam a tecnologia, com o objetivo de detectar possíveis fraudes envolvendo beneficiários de cartões de gratuidade. O software captava a imagem dos rostos de passageiros que entravam no ônibus e as comparava com as fotos cadastradas no banco de dados das pessoas que possuíam direito à gratuidade, gerando provas materiais para o bloqueio dos cartões em caso de uso indevido do benefício.

Agosto de 2011

A Secretaria de Turismo de Santa Catarina, em parceria com a Polícia Militar, apresentou projeto para monitorar o espaço público, a fim de combater a violência contra turistas por meio da instalação de câmeras ligadas a sistemas de reconhecimento facial em sete municípios litorâneos: Balneário Camboriú, Laguna, Itapema, Navegantes, Palhoça, Bombinhas e Penha. Esse sistema é capaz de capturar imagens em tempo real, analisar as características faciais das pessoas e compará-las com as de autores de crimes ou foragidos da justiça, acionando a polícia imediatamente em caso de reconhecimento.

Setembro de 2012

Empresas de ônibus passaram a implementar **tecnologias de reconhecimento facial em toda a frota da cidade de Caruaru** (PE), para detectar se cartões de estudantes ou de idosos eram realmente dos titulares dos benefícios. Além do reconhecimento facial, foi divulgado que os 130 ônibus que atendem a cidade vão contar com o Sistema de Gestão Inteligente de Transporte, que proporciona comunicação online entre os veículos, e com uma unidade de monitoramento chamada Central de Controle Operacional, via comunicação 3G e navegação GPS.

Setembro de 2013

Prefeitura de Cascavel (PR) firmou acordo com a operadora de ônibus ValeSim e a **Transdata Smart**, desenvolvedora de soluções de automação, **para instalação de sistema de reconhecimento facial em 159 ônibus da frota que atende o município**. Esses dispositivos de biometria visam a evitar fraudes envolvendo beneficiários que pagam meia passagem ou possuem gratuidade. A medida foi tomada após aumento de 40% no uso de cartões de idosos e estudantes nos ônibus da cidade. Em 2019, também foi **anunciada a ampliação** da integração da frota, após implantação de biometria facial e rastreamento da frota, que são soluções de ITS (Intelligent Transport Systems).

Junho de 2014

140 **ônibus do transporte público municipal em Limeira (SP) ganharam sistema de biometria facial**, com a finalidade de evitar usos irregulares dos cartões de gratuidade para passageiros idosos ou de descontos para estudantes. O contrato para instalação do sistema foi firmado entre as concessionárias responsáveis pelo transporte e a empresa fornecedora da tecnologia, sem custos para o município.

Agosto de 2016

A Confederação Nacional de Transportes divulgou que um novo sistema de vigilância, baseado em reconhecimento facial e controlado pela Receita Federal, passou a operar em 14 aeroportos brasileiros: Confins (Belo Horizonte-MG), Curitiba (PR), Florianópolis (SC), Porto Alegre (RS), Brasília (DF), Fortaleza (CE), Foz do Iguaçu (PR), Galeão (RJ), Guarulhos (SP), Viracopos (Campinas-SP), Manaus (AM), Recife (PE), Salvador (BA) e São Gonçalo do Amarante (RN). O objetivo é identificar passageiros que apresentem risco potencial de estarem praticando irregularidades aduaneiras, crimes ou infrações.

Abril de 2017

Escolas municipais de Jaboatão (PE) passaram a utilizar sistemas de reconhecimento facial para controlar a frequência de alunos[6], ao custo de R$ 3.000 por unidade de ensino. Além da presença dos estudantes, o sistema também monitoraria a merenda escolar e se os alunos faziam ou não suas atividades.

---

6 Na **França** e na **Suécia**, tribunais e as autoridades de proteção de dados se manifestaram contra ouso de reconhecimento facial para controlar o acesso e frequência em escolas.Essas medidas foram consideradas desproporcionais, uma vez que violam as normas de proteção de dados de estudantes que não são capazes de consentir livremente.

Julho de 2017

Município de Macapá (AP) implementou sistema de reconhecimento facial em 243 ônibus de linhas intermunicipais e urbanas, para evitar fraudes, após Sindicato das Empresas de Transporte de Passageiros do Amapá (Setap) constatar que 25% dos passageiros que utilizavam cartões de meia tarifa não tinham direito ao benefício. Câmeras instaladas nos veículos comparavam fotos dos passageiros com as fotos cadastradas nos cartões. Em caso de imagens não compatíveis, beneficiários seriam chamados para inspeção presencial. Se fossem identificadas fraudes, o benefício seria bloqueado imediatamente.

Setembro de 2017

Em Cuiabá (MT), a Agência de Regularização de Serviços Delegados (Arsec) deu autorização para empresas administradoras do transporte coletivo no município **implantarem dispositivos para leitura de biometria facial nas catracas dos ônibus**. Ao custo médio de R$ 5.000 cada, foram instalados em 60 ônibus, com o objetivo de coibir irregularidades na utilização de gratuidades ou redução de tarifa pelos passageiros.

Abril de 2018

Escolas municipais de **Nova Venécia (ES) testaram tecnologias de reconhecimento facial nos alunos**. Após cadastro dos estudantes nos leitores de reconhecimento biométrico, o sistema foi utilizado, principalmente, para eliminar a necessidade de fazer chamadas, monitorar frequência (avisando aos responsáveis via SMS sobre presença ou ausência de alunos) e calcular de forma mais precisa a produção de merenda escolar, evitando desperdícios.

Maio de 2018

Serviço Autônomo Municipal de Trânsito e Transporte de Blumenau (SC), em parceria com empresa de ônibus, **iniciou testes de sistema de reconhecimento facial no transporte público da cidade**. Esse sistema fotografa usuários dos cartões que cruzam a catraca e realiza a comparação para detectar se as fotos convergem com imagens dos beneficiários cadastrados no sistema de transporte público. Se houver fraude, o cartão é bloqueado.

Agosto de 2018

Comissão de Dados Pessoais do Ministério Público do Distrito Federal e dos Territórios (MPDFT) abriu **inquérito civil público para investigar as empresas CredDefense**, **Certibio e Acesso Digital**, por suspeita de venda ilegal de dados biométricos. Durante as investigações, **Certibio**, que oferece serviços de segurança digital por meio de cruzamento de dados pessoais e reconhecimento facial, afirmou utilizar banco de

dados com 70 milhões de cadastros de brasileiros que pertenciam ao Serviço Federal de Processamento de Dados (Serpro). Contudo, o Serpro não tinha autorização legal para fazer transações com empresas privadas envolvendo dados pessoais.

Outubro de 2018

Prefeitura de Cariacica (ES) testou tecnologia de reconhecimento facial para monitorar se pessoa flagrada por videomonitoramento possui restrições na Secretaria de Estado da Segurança Pública (SESP). Se a restrição fosse confirmada, a polícia seria imediatamente acionada para a localização do suspeito e possível prisão. Porém, entre 2019 e 2020, nenhum valor foi gasto com esse programa, segundo o **Portal da Transparência**.

Dezembro de 2018

O secretário de Segurança Pública Maurício Barbosa e o governador da Bahia Rui Costa (PT) lançaram o **projeto "Vídeo-Polícia - Mais inteligência na Segurança"**. A iniciativa implementou sistema de videomonitoramento inteligente para subsidiar ações policiais a partir do uso de tecnologias de reconhecimento facial, identificação de placas de carros e compartilhamento de dados entre autoridades policiais. Também estabeleceu instalação de 300 câmeras de reconhecimento facial pelo estado ao custo de mais de R$ 18 milhões.

Dezembro de 2018

Prefeitura de Campinas (SP) apresentou o projeto Cidade Segura, em parceria com a Huawei e o Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD). Com foco em segurança pública, a iniciativa instalaria 30 câmeras de vigilância integradas a sistemas de reconhecimento facial para identificar criminosos e pessoas desaparecidas, e dar suporte ao gerenciamento do trânsito e à atuação da Defesa Civil. À época, seis delas entraram em funcionamento na cidade.

Dezembro de 2018

Sindicato das Empresas de Transportes Urbanos de João Pessoa (Sintur-JP) anunciou instalação da biometria facial em 100% da frota de ônibus na capital após contrato com a Transdata – que já forneceu, por exemplo, tecnologia para frota de Cascavel. O objetivo foi impedir fraudes envolvendo passageiros com direito a meia tarifa e gratuidade. Desde a instalação do sistema em 2019, a Sintur tem **registrado** número vultoso de fraudes.

Março de 2019

Foi registrada a **primeira prisão por reconhecimento facial no Brasil**. Durante a passagem de um bloco de carnaval em Salvador (BA), no circuito Barra-Ondina, câmeras ligadas a software de reconhecimento facial, instaladas pela Secretaria de Segurança Pública da Bahia (SSP-BA), identificaram um jovem de 19 anos como suspeito de ter cometido homicídio e acionaram a polícia, que efetuou sua prisão. O estado informou que investiu mais de R$ 18 milhões nesse tipo de tecnologia.

Março de 2019

Campinas (SP) começou a testar câmeras de reconhecimento facial semelhantes às que ajudaram a prender um foragido da justiça durante o carnaval de em Salvador (BA). As câmeras foram implantadas no Terminal Central e no centro da cidade.

Junho de 2019

A **Secretaria de Administração Prisional (Seap) implantou sistema de reconhecimento facial no Presídio Floramar**, em Divinópolis (MG), a fim de verificar com mais agilidade se os presos que davam entrada na unidade forneciam dados verdadeiros às autoridades no momento da prisão. Seap informou que o mesmo sistema de reconhecimento facial se estenderia às 197 unidades prisionais do estado.

Setembro de 2019

Prefeitura de Vila Velha (ES) expandiu e modernizou videomonitoramento no município com a aquisição de 200 novas câmeras, que foram posicionadas estrategicamente, de acordo com o mapa da violência da cidade. Em abril de 2022, a **imprensa revelou** que a prefeitura já havia feito testes sobre o uso da tecnologia de reconhecimento facial.

Outubro de 2019

Sistema de monitoramento apoiou a prisão de três pessoas durante megaevento em Blumenau (SC). Polícia foi acionada após confirmação da existência de mandados de prisão não cumpridos por meio do sistema de reconhecimento facial, que funcionava em conjunto com câmeras instaladas no Parque Vila Germânica, onde ocorreu a tradicional Oktoberfest.

Novembro de 2019

Sistemas de reconhecimento facial instalados em dois bairros cariocas (Copacabana e no Maracanã) ajudaram a prender 63 pessoas em quatro meses no Rio de Janeiro (RJ), segundo levantamento da imprensa. A tecnologia fornecida pelas empresas Oi e Huawei foi usada em parceria entre a Polícia Militar e a Polícia Civil do Rio de Janeiro para a realização das prisões. O sistema capturou imagens dos rostos de pessoas e as

comparou com 49 mil fotos de pessoas com mandado de prisão não cumprido, que compõem o banco de dados mantido pela Polícia Civil. Ao identificar pelo menos 93% de semelhança entre os rostos, acionava a polícia para realizar a abordagem.

Dezembro de 2019

Programa **Fronteira Tech foi inaugurado em Foz de Iguaçu (PR)**, com a instalação de 70 câmeras de reconhecimento facial. Segundo a Receita Federal, a finalidade era reprimir a criminalidade, não só identificando pessoas suspeitas, mas também veículos roubados que cruzavam a ponte da Amizade (entre Brasil e Paraguai). O governo federal investiu, aproximadamente, R$ 5 milhões.

Fevereiro de 2020

Governo do **Amapá passou a cadastrar a biometria facial dos servidores do estado**, a fim de automatizar a produção da folha de ponto. Ao passar pelo equipamento, o colaborador teria o rosto reconhecido, além de identificar local e horário em que o ponto fora registrado. As informações seriam inseridas diretamente na folha de pagamento; e o comprovante, enviado para e-mails dos funcionários.

Fevereiro de 2020:

A Secretaria de Segurança Pública da Bahia (SSP-BA) anunciou a captura de 42 foragidos da justiça durante o carnaval de Salvador com ajuda de sistema de reconhecimento facial. Também informou que, além da varredura feita pelo sistema, algumas prisões foram feitas com base no aplicativo Face check, que compara digitais de suspeitos abordados pela polícia a impressões digitais do banco de dados da Secretaria.

Março de 2020

A Universidade Federal da Paraíba (UFPB) apresentou novo esquema de segurança no campus I, no bairro do Castelo Branco, em João Pessoa. Seriam instaladas 98 novas câmeras com sistemas de reconhecimento facial, além de aplicativo com botão do pânico para atuar junto com o sistema. Alunos, servidores e demais funcionários cadastrados no app poderiam acionar o recurso caso se sentissem ameaçados dentro do campus e passar sua localização para a segurança da universidade.

Junho de 2020

O **prefeito de Curitiba Rafael Greca (União Brasil) anunciou, em parceria com o Instituto das Cidades Inteligentes (ICI), a instalação de 500 câmeras de videomonitoramento** integradas à tecnologia de reconhecimento facial e a radares de trânsito, para formar um cerco digital de segurança ao redor da cidade. Os equipamentos foram distribuídos em pontos estratégicos, de acordo com o mapa do crime da capital paranaense, como

parte do programa Muralha Digital – que tinha correspondências, por exemplo, com o **Muralha Eletrônica** implantado em outras cidades, como Vila Velha (ES). O sistema passou a operar em Curitiba em **janeiro do ano seguinte**.

Julho de 2020

O projeto **cidade inteligente foi anunciado pela prefeitura de Macapá (AP)**. Orçado em R$ 5 milhões, incluía uso da inteligência artificial entre outras tecnologias para auxiliar no desenvolvimento da cidade. Previu uso de algoritmos de aprendizado de máquina integrados a câmeras de videomonitoramento, que realizariam o reconhecimento facial dos cidadãos para auxiliar o trabalho dos órgãos de Segurança Pública.

Agosto de 2020

Sistema de reconhecimento facial da Secretaria da Segurança Pública e Defesa Social (SSPDS) auxiliou a Polícia Civil do Ceará a prender um homem acusado de integrar organização criminosa. Durante as investigações, policiais chegaram à fotografia da companheira de um foragido da justiça federal. A imagem foi submetida à função de reconhecimento facial no aplicativo Portal do Comando Avançado (PCA), que tinha mais de de oito milhões de perfis cadastrados. Com a localização da residência da mulher identificada, a Polícia Civil conseguiu prender o acusado, que lá se escondia das autoridades .

Outubro de 2020

Governo federal realizou o primeiro teste do projeto piloto Embarque + Seguro no aeroporto de Florianópolis (SC). Criado pela Secretaria Nacional de Aviação Civil do Ministério da Infraestrutura e desenvolvido pelo Serviço Federal de Processamento de Dados (Serpro), possibilitaria o embarque com base no reconhecimento facial, sem necessidade de apresentação de documentos. Após captação de imagens dos passageiros, um sistema unificado checaria e validaria suas identidades a partir do cruzamento da biometria facial com informações de diferentes bases de dados governamentais. Foi realizado teste com 12 pessoas em um único voo. A expectativa era de que todos os aeroportos do país receberiam o sistema em até três anos.

Março de 2021

Governo estadual do Rio de Janeiro, em parceria com Consórcio Integrado de Segurança Pública da Baixada Fluminense (CISPBAF), anunciou um **centro de monitoramento para vigiar 17 municípios do estado**. Municípios da **Baixada Fluminense**, além das cidades de Itaboraí, São Gonçalo, Mangaratiba e Angra dos Reis, teriam ruas vigiadas por câmeras com softwares de reconhecimento facial e leitura de placas de automóveis. A previsão de investimento era de aproximadamente R$ 15 milhões. A verba para a compra dos equipamentos foi disponibilizada pela **Assembleia Legislativa do Estado do Rio de Janeiro (Alerj) em 2019**.

Abril de 2021

Prefeitura de Manaus anunciou a instalação de 180 câmeras de vigilância de alta definição na cidade até o final daquele ano, com funções de reconhecimento facial e leitura de placas de veículos. As primeiras 41 câmeras foram compradas com recurso federal, por meio do Financiamento à Infraestrutura e ao Saneamento (Finisa), após licitação ganha pela Motorola Solution Ltda, responsável pela instalação e manutenção dos equipamentos.

Maio de 2021

Governo federal iniciou testes de sistema de monitoramento com reconhecimento facial no aeroporto de Belo Horizonte (MG), dentro do projeto Embarque + Seguro. Testes foram iniciados em outubro de 2020, para viabilizar 100% do processo de embarque por meio da biometria facial. O projeto fazia parte do Programa de Transformação Digital do governo federal, iniciativa coordenada pela Subsecretaria de Gestão Estratégica, Tecnologia e Inovação (SGETI), subordinada à Secretaria Executiva no Ministério da Infraestrutura. A tecnologia foi desenvolvida pelas empresas Biomtech, Wolpac e Azul/Pacer.

Julho de 2021

O governador da Bahia Rui Costa (PT) apresentou plano de **expansão do Projeto Vídeo Polícia**: Itabuna, Ilhéus, Guanambi, Teixeira de Freitas, Porto Seguro, Eunápolis, Itamaraju, Valença e Barreiras, Feira de Santana, Alagoinhas, Santo Antônio de Jesus, Jequié e Vitória da Conquista fariam parte da lista de 77 municípios baianos que contariam com sistemas de rastreamento de placas de veículos e reconhecimento facial. O projeto, orçado em aproximadamente R$ 665 milhões, previa cinco anos da prestação de serviço pelo consórcio formado pela Oi SA e Avante SA, que vencera a licitação. Segundo o **Intercept**, com mais essa ação, Costa vinha fazendo da Bahia um "laboratório de vigilância com reconhecimento facial".

Agosto de 2021

Aeroporto Leite Lopes, em Ribeirão Preto (SP), iniciou testes para realizar o embarque de passageiros usando tecnologia de reconhecimento facial, como parte do programa do governo federal Embarque + Seguro 100% Digital. Com a adoção desse sistema, passageiros não necessitariam mais apresentar documentos de identificação nem cartão de embarque para viajar, uma vez que todo o processo passa a ser feito pelo reconhecimento da biometria facial.

Agosto de 2021

Plano de metas para a segurança pública em São José (SC) previu ampliação do videomonitoramento para todos os bairros da cidade, inclusive com auxílio de câmeras capazes de realizar o reconhecimento facial e com instalação de totens (sistema de segurança digital) em todas as praças públicas do município. Em fevereiro de 2022, a **prefeitura** reportou uma melhora na localização e identificação de autores de roubo, furto, arrombamento, agressão, tráfico ou consumo de drogas, o que foi atribuído ao trabalho da Central de Videomonitoramento com as tecnologias de identificação biométrica.

Fevereiro de 2022

Polícia Civil **prende foragido da Justiça com ajuda de câmeras de reconhecimento facial instaladas no Mercado do Produtor de Juazeiro (BA)**. A Autarquia Municipal de Abastecimento (AMA), órgão que administra o mercado, acionou a polícia assim que o sistema de monitoramento, que conta com 53 câmeras, identificou um homem que tinha mandado de prisão preventiva decretada por suspeita de praticar um homicídio em Pernambuco. Policiais civis imediatamente mandaram uma equipe ao local efetuando a prisão do suspeito.

Fevereiro de 2022

Dispositivo chamado **"infraestrutura hiperconvergente" (Hyper-Converged Infrastructure - HCI - em inglês)** foi anunciado como medida de combate ao crime em Vitória (ES). Seriam instaladas 150 câmeras com leitores de biometria facial para monitoramento urbano da capital capixaba, ao custo de R$ 15 milhões aos cofres públicos. A ferramenta seria capaz de localizar carros em situação irregular circulando, pessoas com mandado de prisão não cumprido e suspeitas de práticas de crimes em tempo real. Também poderia localizar pessoas com mandados de prisão em aberto, suspeitas de práticas de crimes ou que estivessem portando armas e objetos perigosos, além de veículos em circulação irregular pela cidade.

Março de 2022

Prefeitura do Recife previu lançar edital para Parceria Público-Privada com o objetivo de instalar 108 relógios contendo anúncios publicitários, informações como hora, qualidade do ar e temperatura, além de câmeras de vigilância de reconhecimento facial. Em audiência pública, vereadores e membros da sociedade civil se opuseram ao edital devido a preocupações com violação do direito à privacidade, racismo algorítmico e falta de transparência sobre funcionamento da tecnologia e finalidade das câmeras. O edital previa a concessão de 20 anos de prestação de serviços com a empresa ganhadora da licitação.

Março de 2022

Juizado do Torcedor de Minas Gerais, em conjunto com empresa de tecnologia Biomtech, **inaugurou câmeras de reconhecimento facial no estádio do Mineirão, em Belo Horizonte**. O objetivo era coibir a prática de atos ilícitos, como entrada sem pagar e envolvimento em brigas. Pessoas flagradas cometendo ato ilícito no estádio passariam por um cadastramento de biometria facial. Assim, seria possível garantir o cumprimento de medidas de afastamento do estádio determinadas pela justiça, por meio de reconhecimento facial capaz de detectar pessoas com restrições de entrada cadastradas em suas bases de dados. Com a adoção do sistema, **três pessoas foram detidas**.

Março de 2022

Justiça impediu funcionamento do sistema de reconhecimento facial do Metrô de São Paulo, após decisão judicial favorável a Ação Civil Pública movida pelas Defensorias Públicas de São Paulo e da União, pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) e por organizações da sociedade civil, em agosto de 2018. Entidades alegaram que reconhecimento no metrô violava direitos dos cidadãos e não respeitavam exigências legais para coleta de dados pessoais previstas na LGPD, no Código de Usuários de Serviços Públicos, no Estatuto da Criança e do Adolescente, na Constituição e em tratados internacionais. A Via Quatro, administradora do metrô, afirmou que o sistema fora instalado para fins estatísticos de estimação do fluxo de passageiros.

[Linha do Tempo] Projetos de Lei do Congresso Nacional sobre reconhecimento facial, dados biométricos e inteligência artificial

PLs em tramitação que tratam das temáticas envolvidas no uso dessas tecnologias entre 2017 e 2021

Dezembro de 2017

PL 9.414 torna obrigatória instalação da leitura de impressão digital e facial nos meios de transportes públicos coletivos, a fim de inibir fraudes de benefícios (isenções e reduções de tarifa) concedidos pelo poder público no acesso ao transporte público por cidadãos.

Março de 2018

PL 9.736 torna obrigatória a presença de sistemas de reconhecimento facial em presídios de todo o país. Inclui na Lei de Execução Penal a identificação por método biométrico de reconhecimento facial de todas as pessoas custodiadas em estabelecimentos penais.

Dezembro de 2018

PL 11.140 determina que, além de detidos, servidores públicos, prestadores de serviços e visitantes deverão ser identificados pelo sistema biométrico para ter acesso aos estabelecimentos penais.

Agosto de 2019

PL 4.612 prevê a regulamentação do desenvolvimento e uso de tecnologias de reconhecimento facial e emocional para identificação de pessoas, além de analisar ou prever seus comportamentos. É justificado pela necessidade de regular uma nova área de expansão tecnológica.

Fevereiro de 2020

PL 329 prevê a obrigatoriedade de pagamento eletrônico nas viagens por aplicativos de transporte particular, além de registro facial ou biométrico dos passageiros. Visa a reduzir a violência contra os motoristas de aplicativo e prevê a necessidade de identificação dos antecedentes criminais de passageiros para viagens por apps.

Fevereiro de 2021

PL 572 cria o Banco Nacional de Dados de Reconhecimento Facial e Digital, formado a partir dos registros faciais de menores de 18 anos coletados no ato do registro de identidade. Visa a facilitar buscas de crianças e adolescentes desaparecidos.

Outubro de 2021

PL 3.714 prevê alteração no Código de Processo Penal para que o reconhecimento facial por fotografia seja obtido, preferencialmente, de órgãos oficiais (poder público) e que seja usado em todas as fases de uma ação criminal. É justificado pela quantidade de erros em julgamentos que utilizam fotografias como prova única e principal dos julgados, não raro resultando em decisões injustas.

Março de 2022

PL 745 altera a Lei nº 13.812/2019 sobre a Política Nacional de Busca de Pessoas Desaparecidas que criou o Cadastro Nacional de Pessoas Desaparecidas e alterou o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), para dispor e regulamentar o uso de dados de reconhecimento facial de menores. É justificado como resposta ao alto número de menores desaparecidos anualmente no país.

Vigilantismo e digilantismo

Já abordamos como as pessoas são vigiadas tanto pelo Estado quanto por empresas privadas e os riscos que isso gera para os indivíduos e para a democracia. No entanto,também é preciso colocar nessa matriz de riscos a atuação direta de grupos paraestatais, de indivíduos que, diante da falta de ação ou mesmo a partir do fomento pelo poder público, resolvem agir diretamente, à margem da lei, quando se sentem ameaçados. Esses grupos e indivíduos atuam para resolver alegados problemas de segurança, de emprego, ou mesmo exacerbando incompreensões particulares sobre o diferente, sobre o outro. Grupos vulneráveis acabam sendo os alvos preferenciais desse tipo de atuação. E o "fazer justiça com as próprias mãos" resulta em violência física ou psicológica de pessoas.

Ações vigilantistas são recorrentes no Brasil, já que a violência é vista como pedagógica por parte da população e a política de segurança do Estado acaba deixando espaço para que grupos atuem à margem da lei e indivíduos sintam a necessidade fazer justiça com as próprias mãos.

Destacamos abaixo conceitos fundamentais para a compreensão do debate sobre vigilantismo, seja no ambiente físico ou no ambiente virtual.

Vigilantismo

Está ligado ao exercício de controle sobre a vida de pessoas por meio da violação de direitos básicos assegurados por leis. O primeiro ponto fundamental é a ideia de que, diante de uma resposta insuficiente a demandas sociais, de uma negligência ou por falta de recursos do Estado, grupos surgem para tentar resolver supostos problemas de forma independente e, na maior parte dos casos, de forma violenta e à margem da lei. Assim, o vigilantismo pode ser manifestado por indivíduos ou organizações sem qualquer vínculo com o poder público, por meio da imposição de regras e punições que não estão previstas nos dispositivos legais ou que estão previstas, mas deveriam ser executadas pelas autoridades competentes.

A prática de fazer justiça com as próprias mãos, que frequentemente se desdobra em assassinatos, linchamentos e outros crimes, é um exemplo categórico de vigilantismo exercido por atores privados. Grupos que utilizam a violência e mecanismos institucionais para perseguir ou intimidar, com o objetivo de controlar territórios ou promover qualquer outra forma de solapamento dos direitos dos cidadãos e cidadãs, como as milícias e facções criminosas, também podem ser enquadrados como faces do vigilantismo.

Ações vigilantistas, ainda, podem partir de autoridades estatais, como em casos em que o governo não realiza ações diretamente, mas incentiva atos violentos, a intolerância e a perseguição de pessoas e grupos por meio de discursos, por exemplo.

Digilantismo (Vigilantismo digital)

Corresponde à reprodução do vigilantismo nos meios digitais. O **vigilantismo digital**, também chamado de digilantismo ou cibervigilantismo, ocorre quando tecnologias da informação conectadas à internet são mobilizadas por indivíduos, grupos ou pelo poder público para práticas criminosas, tal como incitação ao crime, invasão de privacidade e espionagem, ou para outras ações que não são necessariamente crimes, mas que constumam causar severos danos, como no caso do linchamento virtual. Ano após ano, multiplicam-se pelo mundo casos nos quais vítimas de linchamento virtual perdem seus empregos, sofrem atentados ou cometem suicídio após terem sua intimidade ou posição politica exposta na internet, de forma a suscitar milhares de mensagens de ódio e ameaças de morte.

A ideia da justiça com as próprias mãos também está presente no vigilantismo digital e, geralmente, manifesta-se quando grupos organizados ou indivíduos cometem crimes sob o pretexto de combater outros crimes, como no caso do grupo de hackers Anonymous, que divulgou na internet uma lista com dados pessoais de supostos pedófilos. Vácuos deixados pelo poder público no que se refere à legislação, ações de segurança e ausência de infraestrutura para a fiscalização dos ambientes virtuais também estimulam o vigilantismo digital.

Tipos de ações que podem ser consideradas como vigilantismo

Destacamos abaixo situações que podem ser consideradas como vigilantismo fora e dentro do ambiente virtual, incluindo alguns exemplos a partir de casos que foram destaque na mídia.

1. Casos em que grupos paralelos, como milícias, esquadrões da morte e outros grupos vigilantistas praticam o vigilantismo como forma de manter ou reforçar seu controle sobre determinados territórios e reprimir o crime. Desse modo, punem pessoas que ameaçam o seu poder de alguma maneira (exemplo: alguém reclama de alguma taxa cobrada pelo grupo) ou violam as regras impostas àquele território (por exemplo, o não pagamento de uma taxa de segurança, o consumo ou venda de substâncias proibidas, o cometimento de algum crime ou infração). As punições variam em tipo e intensidade, envolvendo violências físicas (espancamento, linchamento público), violências contra o patrimônio (roubo de equipamentos de comércios) e até a morte. A violência exerce um caráter pedagógico ou de vingança, no sentido de reforçar a autoridade que os grupos exercem. Já nos casos dos esquadrões da morte, em geral eles buscam punir pessoas que são acusadas de cometer crimes ou vingar a morte de integrantes do grupo.

    - Nos anos 1960, começam a surgir, no Rio de Janeiro, denúncias de execuções realizadas por um grupo organizado de policiais após a morte do famoso detetive da Polícia Civil Milton Le Cocq, em 1964, durante troca de tiros com um dos suspeitos de crimes mais procurados da capital na época, Milton Moreira, o Cara de Cavalo. A morte de Le Coq marca o surgimento do mais famoso esquadrão da morte do país, a “Escuderia Le Cocq”. Criado para vingar a morte do detetive, o grupo mobilizou muitos policiais que participaram voluntariamente das diligências atrás do assassino, morto poucos dias depois com mais de 50 tiros. O esquadrão atuou entre as décadas de 1960 e 1980 e foi extinto nos anos 2000. Ao menos 1.500 pessoas foram mortas apenas no Espírito Santo.

    - Em São Paulo, o Esquadrão da Morte se estabelece na década de 1960 após o golpe militar e começa a funcionar com mais força e em conjunto com o Estado na execução de “suspeitos” e “bandidos”. Entre 1968 e 1969, o esquadrão paulista passa a agir enquanto grupo independente e atua em conjunto com a repressão política da ditadura. No livro “Rota 66 - A História da Polícia que Mata”, o jornalista Caco Barcellos aponta que as Rondas Ostensivas Tobias de Aguiar (ROTA) assumiram papel da limpeza social por meio do extermínio no estado de São Paulo. A ROTA e a sua manutenção nas polícias após o fim da ditadura representam a “institucionalização” do Esquadrão da Morte por causa da sua violência e número de mortes.

    - Na madrugada de 23 de julho de 1993, oito meninos são executados a tiros de fuzil por um grupo de policiais militares nos arredores da Igreja da Candelária, no centro do Rio de Janeiro. Os policiais militares Marcus Vinicius Emannuel Borges Vargas, Nelson Oliveira dos Santos, Marco Aurélio Dias de Alcântara e Arlindo Afonso Lisboa Júnior são condenados pelo crime, conhecido como “Chacina da Candelária”. A motivação do massacre é de se vingar de crianças em situação de rua que vivem no entorno da Candelária e, no dia anterior, atiraram pedras em uma viatura da PM-RJ dirigida por Marcus Vinicius, em protesto à prisão de Nilton e Ruço, dois meninos que viviam ali.

- 22 pessoas são assassinadas em Vigário Geral, Zona Norte do Rio de Janeiro, na noite de 29 de agosto de 1993, um mês após a Chacina da Candelária. Os executores do crime integram um grupo conhecido como “Cavalos Corredores” — pela atuação violenta de entrar em favelas correndo como cavalos e atirando a esmo —, formado por policiais militares vinculados ao 9º Batalhão da PM de Rocha Miranda, também na Zona Norte. O massacre é uma represália do grupo pelo assassinato de um policial militar, supostamente cometido por traficantes da favela de Vigário Geral. Nenhuma das vinte e duas pessoas assassinadas tem qualquer ligação com o tráfico.

- Entre 19 e 22 de agosto de 2004, dez pessoas em situação de rua, fixadas na Praça da Sé, no centro de São Paulo, são mortas com golpes na cabeça, por grupo de policiais militares e um segurança privado, a fim de silenciar possíveis testemunhas do envolvimento do grupo com o tráfico de drogas.

- Em 2005, 30 pessoas são baleadas por policiais militares nas cidades de Nova Iguaçu e Queimados, na Baixada Fluminense (RJ), em retaliação à prisão de policiais do 15º Batalhão da PM em Duque de Caxias. Insatisfeitos com a atuação do novo comandante do batalhão, os policiais atiram a esmo em diversos locais das cidades em 31 de março de 2005, matando 29 pessoas.

② Outra ação considerada vigilantista que merece destaque é o linchamento. Essas ações coletivas para punir pessoas acusadas de crimes ou violações persistem há muitos séculos. Enquanto no caso das milícias, esquadrões da morte e outros grupos justiceiros há uma vigilância para reprimir o crime, os linchamentos “típicos” são resultado de uma decisão súbita, espontânea e irracional dos linchadores. Os linchamentos se baseiam em julgamentos frequentemente imediatos, carregados da emoção do ódio ou do medo, em que os acusadores são quase sempre anônimos. Os linchadores se sentem dispensados da necessidade de apresentação de provas que fundamentem suas suspeitas e a vítima não tem tempo nem oportunidade de provar sua inocência. É um julgamento sem juiz neutro ou possibilidade de recurso. As redes sociais também têm exercido um papel na disseminação de boatos e fotos sobre supostos crimes, o que contribui para a ocorrência de linchamentos – tanto físicos quanto virtuais. Podemos destacar casos em que pessoas são acusadas de algum crime e são alvo de violência, como espancamentos (em alguns casos até à morte) e prisão de pessoas em postes, entre outros.

- Três assassinatos brutais chocam o país em 1990, no caso conhecido como **Massacre de Matupá**. Ao assaltar uma residência na cidade de Matupá (MT), três homens fazem refém uma família, após a chegada da polícia ao local. Durante negociação para a liberação dos reféns que durou mais de 15 horas, os moradores se aglomeram ao redor da casa para acompanhar. Mesmo após os assaltantes se entregarem à polícia e liberarem os reféns, a população local os captura e leva até a praça principal da cidade, onde são baleados, linchados e queimados vivos. As

imagens são gravadas pelo cinegrafista amador Leno Durrewald e divulgadas na mídia, dando repercussão nacional ao caso. Ao todo, **18 réus** indiciados pelo crime vão a júri popular.

- Em 2014, **um adolescente é espancado e preso por uma tranca de bicicleta a um poste no bairro do Flamengo, Zona Sul do Rio de Janeiro**, após ser acusado por moradores da região de ser um assaltante conhecido na região.

- Em 2015, **um homem é amarrado a um poste e espancado até a morte por um grupo de moradores**, após ser considerado suspeito de uma tentativa de assalto a um bar em São Luís, no Maranhão.

- Em 2020, nos primeiros meses da pandemia da covid-19 no Brasil, os estados começam a criar hospitais de campanha por conta do aumento do número de casos e internações. No meio da crise com governadores e do negacionismo da gravidade da situação, o presidente Bolsonaro pede que apoiadores "arranjem uma maneira" de entrar em hospitais de campanha e filmar se os leitos estão ocupados ou não. Isso desencadeia uma **série de invasões a hospitais**, apesar do risco de contágio.

3. Os casos de violência e justiça com as próprias mãos não têm apenas brasileiros como alvo. Têm se tornado cada vez mais recorrentes casos de violência contra imigrantes e refugiados. Derivam diretamente do que chamamos de xenofobia, um sentimento de hostilidade contra pessoas por conta de sua nacionalidade.

   - Em 2010, o Haiti é devastado por um forte terremoto. A catástrofe e a crise econômica motiva milhares de haitianos a migrar para outros países, e o Brasil é um dos principais destinos. No entanto, as cidades brasileiras não têm abrigos para acolher imigrantes e refugiados em situação de vulnerabilidade. Nos anos seguintes, ocorrem diversos ataques violentos a cidadãos dessa nacionalidade. Em 2015, **seis haitianos são baleados** no centro de São Paulo. Pelas informações prestadas pela Missão Paz e pelas vítimas, os feridos estavam na escadaria da igreja que oferece assistência a imigrantes, no bairro paulistano do Glicério, quando um dos responsáveis pelo ataque passou pelo local de carro, com outras três pessoas, e, antes de atirar, gritou: "Haitianos, vocês roubam nossos empregos!".

   - Situação semelhante ocorre em Roraima com imigrantes venezuelanos. A cidade brasileira de Pacaraima, na fronteira com a Venezuela, começa a receber milhares de refugiados a partir de 2016. Em agosto de 2018, após um assalto a um comerciante, **um grupo de moradores de Pacaraima incendeia barracas e pertences de refugiados venezuelanos**, acusando-os de responsáveis pelo aumento da violência na cidade. Vídeos mostram os brasileiros gritando "bota fogo" e carregando pedaços de madeira e pedras. Em março de 2021, a Polícia Federal

invade abrigo de refugiados em Paracaima e encaminha 55 mulheres e crianças venezuelanos para a deportação. Em agosto, um levantamento da imprensa revela que o Exército criou um espaço de detenção em Boa Vista, no qual indígenas venezuelanos foram confinados ilegalmente e torturados.

④ Também destacamos os casos de vigilantismo que ocorrem no ambiente virtual, os quais possuem diversos nomes e impactam a vida dos punidos de diferentes formas. Ações vigilantistas na internet podem incluir (a) atribuição pública de culpa a alguém (blaming), (b) ataques para desmascarar pessoas (debunking), (c) vergonha pública (public shaming), (d) linchamentos digitais que envolvem perseguição e ataques para destruir a reputação de alguém, o que pode impactar sua vida fora das redes, (e) busca e transmissão de dados privados de uma pessoa (endereços, placas de carro, informações das redes sociais e outras) e uso desses dados para chantagear, ameaçar, extorquir ou humilhar virtualmente pessoas, e (f) outros casos que envolvem ameaçar de morte e outras formas de assédio e violência psicológica. Muitas vezes, as práticas vigilantistas e intimidações virtuais não são levadas a sério. A professora Danielle Citron, da Universidade de Maryland (EUA), **realizou uma pesquisa sobre reações a crimes de ódio no ambiente cibernético** e constatou que muitas ameaças de morte e estupro na internet são consideradas inofensivas[7].

- É o caso da professora Débora Diniz, da Universidade de Brasília (UnB), que deixa o país com a família em **setembro de 2018**, por conta de perseguições nas redes, linchamento virtual e ameaças de morte, seguindorecomendação do **Programa de Proteção aos Defensores de Direitos Humanos** do governo. Ela é ativista pelos direitos reprodutivos de mulheres e voz ativa na esfera pública para além dos círculos acadêmicos **há quase 20 anos**. A escalada dos ataques se dá a partir de maio de 2018, especialmente após a realização de uma audiência pública no STF em agosto sobre a descriminalização do aborto nos primeiros meses de gestação. As ameaças, no entanto, **não se restringem** à professora e sua família, chegando a seus alunos, professores e à reitoria da UnB. Mesmo se autoexilando, Débora Diniz diz se sentir ameaçada e receber e-mails agressivos.

- Outro caso famoso de perseguição nas redes é o da professora da Universidade Federal do Ceará e blogueira feminista Lola Aronovich. Desde 2008, Lola possui o blog "Escreva Lola Escreva", que tem viés feminista e aborda temas variados. **Há mais de uma década, é alvo de ataques de ódio nas redes sociais** por meio de trolls misóginos e recebe ameaças à sua vida e de seus familiares. Registra boletins de ocorrência diversas vezes, mas a Delegacia da Mulher de sua cidade diz não ter condições de realizar as investigações, pois envolvem ações complexas, como quebrar o sigilo de um site hospedado no exterior. E a Polícia Federal diz que não é sua atribuição investigar esse tipo de crime. A professora também é alvo de doxing, i.e., divulgação indevida de dados pessoais pela internet.

---

7 Citron, D. (2014). Hate Crimes in Cyberspace. Cambridge, MA: Harvard University Press.

- Em março de 2021, o **youtuber Felipe Neto** é intimado pela Polícia Civil do Rio de Janeiro a prestar depoimento em investigação que o acusa de calúnia e violação à Lei de Segurança Nacional (LSN) – revogada em agosto daquele ano – por chamar o presidente Bolsonaro de genocida. Em setembro de 2020, o deputado federal José Medeiros (Podemos-MT) também requer abertura de inquérito para investigá-lo, bem como a políticos da oposição, por participação em ato político declarado antifascista. Segundo Neto, desde "o primeiro dia de governo", as ameaças a ele são constantes, sendo as requisições de abertura de inquérito apenas uma face da "perseguição absoluta" que sofre. Após entrevista ao jornal "New York Times" em 2020, em que acusa o presidente Jair Bolsonaro de péssima gestão na pandemia, o youtuber é acusado nas redes de pedofilia, o que se dá também em outras ocasiões. O influenciador também é indiciado por corrupção de menores, em razão de sua produção audiovisual.

Organizações que lidam com a temática no Brasil e no mundo

A pesquisa buscou mapear organizações da sociedade civil que trabalham com a temática da vigilância e do vigilantismo de forma direta ou indireta. A primeira etapa do mapeamento foi feita por meio de uma pesquisa e de informações colhidas em plataformas de busca na internet (Google etc) e em publicações, utilizando palavras-chave[8] ligadas à temática de vigilância e vigilantismo. Em seguida, listou as organizações que publicaram ou são citadas nos documentos encontrados. Logo, trata-se de um levantamento não exaustivo e preliminar, já que está limitado às organizações que publicam materiais nos dois idiomas utilizados na busca (português e inglês).

Identificamos 48 organizações com sede em 17 países e 5 continentes (**lista na página 51**). Não identificamos organizações localizadas em países da Oceania. O mapa abaixo mostra a localização dos países-sede.

8 Foram utilizadas palavras-chave em português como: *relatório, pesquisa, estudo + vigilância, vigilância estatal, vigilantismo, vigilantismo digital, reconhecimento facial, viés de reconhecimento facial, inteligência artificial, proteção de dados, proteção de dados pessoais, direito digital, dados biométricos, biometria, tecnoautoritarismo, monitoramento, tecnologias espiãs, softwares de espionagem, espionagem, Pegasus, viés algorítmico, racismo algorítmico, entre outras.* Também foram utilizadas as mesmas palavras em inglês: *report, research, study + surveillance, state surveillance, vigilantism, digital vigilantism, facial recognition, facial recognition bias,artificial intelligence, data protection, personal data protection, digital law, biometric data, biometrics, technoauthoritarianism, monitoring, spy technologies, spy software, espionage, Pegasus algorithmic bias, algorithmic racism* etc.

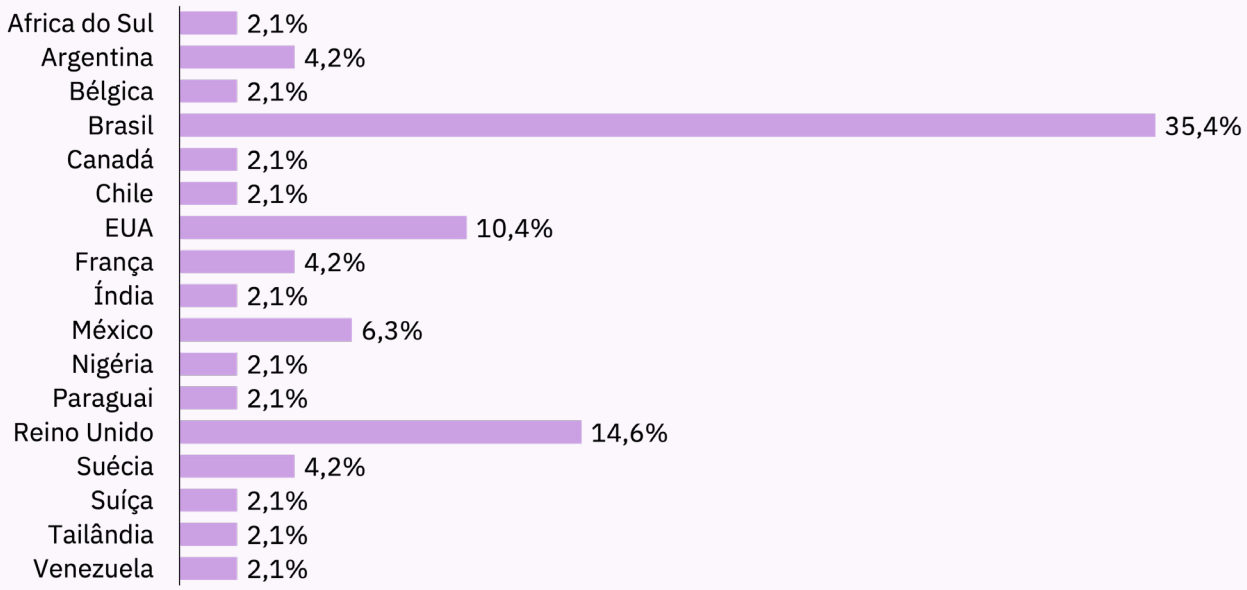
[Mapa] Países em que as organizações possuem sede

legenda: nº número de sedes de organizações presentes no país.

Ao analisar a distribuição das organizações pelos 17 países, nota-se que o Brasil concentra o maior percentual de organizações (35,4%), seguido do Reino Unido (14,4%) e dos Estados Unidos (10,4%). Isso pode ter relação com alguns fatores ligados à história do nosso país, tal como o período da ditadura militar e o **"entulho autoritário[9]"**, e à necessidade de proteção de direitos individuais e dados pessoais que são alvo de vigilância estatal e privada.

9 A expressão "entulho autoritário" foi utilizada em 1979 pela oposição ao presidente militar João Baptista Figueiredo para se referir à caótica ordem jurídica brasileira após a revogação dos atos institucionais, decretos de exceção impostos pela ditadura. Apesar da revogação dos atos institucionais, persistiam na ordem jurídica leis e instituições com a tônica autoritária da ditadura militar. É o caso da **Lei de Segurança Nacional**, que foi utilizada em anos recentes para justificar a prisão de pessoas que se manifestaram contrariamente ao governo federal.

[Gráfico] Distribuição das organizações segundo país-sede



No que se refere ao ano de fundação das organizações mapeadas, é possível notar uma dispersão no último século (1920 a 2020). Há organizações que existem há mais de 100 anos e outras criadas mais recentemente.

Chama a atenção o fato de que mais de 35% delas surgiram a partir de 2014, havendo uma concentração no ano de 2018 (12,5%). Isso pode ser explicado pelo surgimento cada vez mais veloz de novas tecnologias e mecanismos de vigilância por parte do Estado e por parte de grandes corporações nas últimas décadas.

A partir de publicações recentes dessas organizações, mapeamos as principais temáticas em que essas organizações têm atuado e que estão vinculadas de forma direta ou indireta à vigilância, ao vigilantismo e a práticas discriminatórias.

Ao analisarmos as 48 organizações, notamos que 83% delas têm realizado pesquisas ou atuado em temáticas ligadas à vigilância estatal, enquanto 77% têm se dedicado a questões relacionadas à liberdade, à privacidade e à proteção de dados pessoais.

Outro tema bastante abordado pelas organizações (62%) é o monitoramento da sociedade civil por parte do Estado e de agentes privados, o que às vezes resulta em casos de violência contra ativistas, jornalistas, defensores de direitos humanos, pessoas que se manifestam contrariamente a regimes autoritários ou a sociedade civil em geral. Para além de abordagens sobre o monitoramento da sociedade civil, há organizações que atuam de diferentes formas para a proteção de defensores de

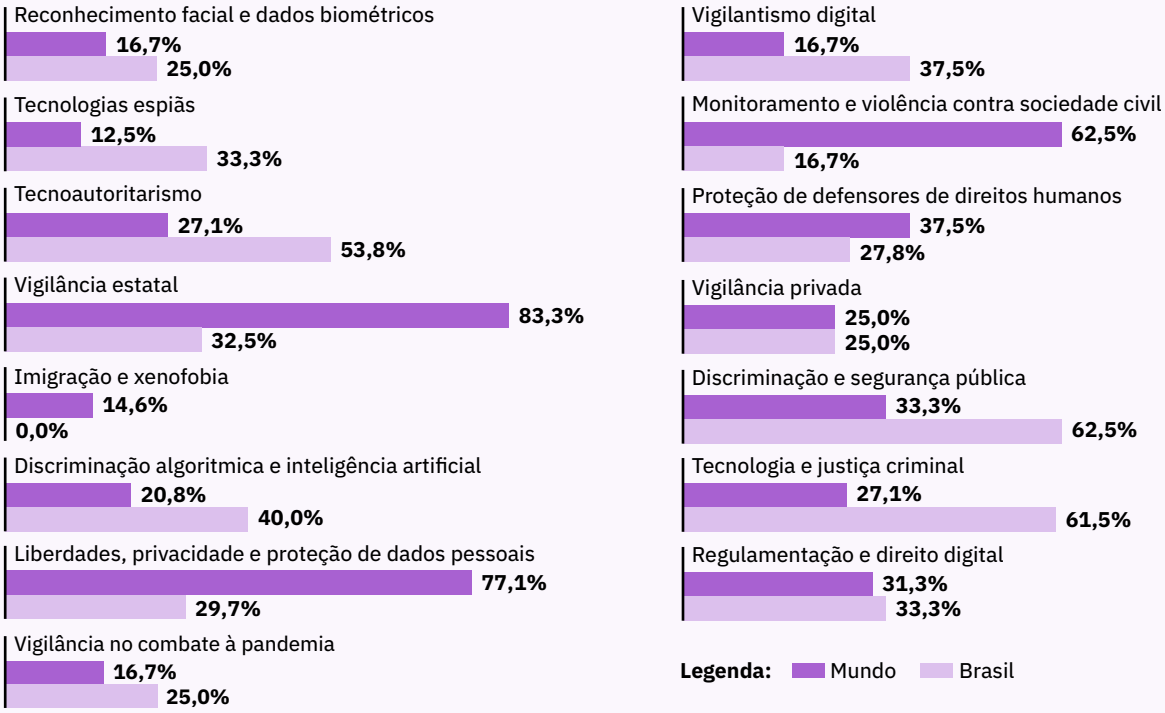
direitos humanos (37,5%). Isso se soma à temática do tecnoautoritarismo,[10] que tem sido abordada por 27% das organizações mapeadas, e à aquisição de softwares de espionagem (como o Pegasus) por estados (12,5%).

Ademais, como destacamos no item 3 deste relatório, é crescente o debate sobre a discriminação algorítmica e o uso de inteligência artificial (20,8%), as tecnologias de reconhecimento facial (16,7%) e como seu uso pode resultar em casos de discriminação na área da segurança pública (33%) e afetar as decisões judiciais no âmbito criminal (27%).

Por fim, nota-se um debate relevante sobre o direito digital e a regulamentação de novas tecnologias (31%), com o objetivo de proteger a liberdade, a privacidade e os dados pessoais dos cidadãos.

Se analisarmos a distribuição das temáticas apenas nas organizações brasileiras, percebe-se que a questão da discriminação na área da segurança pública é a de maior destaque (62,5%), seguida da discussão sobre tecnologia e a justiça criminal (61,5%) e o tecnoautoritarismo (53,8%). Também chama atenção a discussão sobre discriminação algorítmica e inteligência artificial (40%) e sobre ovigilantismo digital (37,5%).

[Gráfico] Distribuição das organizações segundo os principais temas analisados



10 Para saber mais sobre, ver: **https://laut.org.br/retrospectiva-tecnoautoritarismo-2020/.**

Quais são, onde estão e em que áreas atuam essas organizações

África do Sul

Civicus (1993)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | proteção de defensores de direitos humanos | tecnoautoritarismo | vigilância estatal.

Acesse o site ↗

Argentina

Asociación por los Derechos Civiles – ADC (1995)

Atuação: discriminação algorítmica e inteligência artificial | liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | vigilância estatal

Acesse o site ↗

Consejo Latinoamericano en Ciencias Sociales – CLACSO (1967)

Atuação: monitoramento e violência contra a sociedade civil | vigilância no combate à pandemia | vigilantismo digital

Acesse o site ↗

Bélgica

Protection Internacional (PI) – (1998)

Atuação: monitoramento e violência contra a sociedade civil | proteção de defensores de direitos humanos | vigilância estatal

Acesse o site ↗

Brasil

Centro de Análise da Liberdade e do Autoritarismo – LAUT (2020)

Atuação: discriminação e segurança pública | liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra a sociedade civil | proteção de defensores de direitos humanos | regulamentação e direito digital | tecnoautoritarismo | tecnologia e justiça criminal | vigilância estatal

Acesse o site ↗

Coalizão de Direitos na Rede (2016)

Atuação: discriminação algorítmica e inteligência artificial | liberdades, privacidade e proteção de dados pessoais | regulamentação e direito digital |tecnoautoritarismo | tecnologias espiãs | vigilância estatal | vigilância privada | vigilantismo digital

Acesse o site ↗

Coding Rights (2015)

Atuação: liberdades, privacidade e proteção de dados pessoais | tecnoautoritarismo | vigilância estatal

Acesse o site ↗

Conectas Direitos Humanos (2001)

Atuação: discriminação algorítmica e inteligência artificial | discriminação e segurança pública | liberdades, privacidade e protação de dados pessoais | monitoramento e violência contra sociedade civil | proteção de defensores de direitos humanos | regulamentação e direito digital | tecnoautoritarismo | tecnologias espiãs | tecnologia e justiça criminal | vigilância estatal

Acesse o site ↗

Data Privacy Brasil (2018)

Atuação: discriminação algorítmica e inteligência artificial | liberdades, privacidade e proteção de dados pessoais | regulamentação e direito digital | tecnoautoritarismo | tecnologia e justiça criminal | vigilância estatal | vigilância no combate à pandemia | vigilantismo digital

Acesse o site ↗

Datalabe (2016)

Atuação: discriminação e segurança pública | vigilância estatal

Acesse o site ↗

Fiquem Sabendo (2018)

Atuação: discriminação e segurança pública | liberdades, privacidade e proteção de dados pessoais | tecnologia e justiça criminal | vigilância estatal

Acesse o site ↗

Iniciativa Direito à memória e Justiça Racial – IDMJR (2018)

Atuação: discriminação e segurança pública | tecnologia e justiça criminal | vigilância estatal

Acesse o site ↗

Iniciativa Negra (2015)

Atuação: discriminação e segurança pública | vigilância estatal

Acesse o site ↗

Instituto de Defesa do Direito de Defesa – IDDD (2000)

Atuação: discriminação e segurança pública | liberdades, privacidade e proteção de dados pessoais | vigilância estatal | vigilância no combate à pandemia

Acesse o site ↗

Instituto Igarapé (2011)

Atuação: discriminação e segurança pública| liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra a sociedade civil | proteção de defensores de direitos humanos | reconhecimento facial e dados biométricos | tecnoautoritarismo | tecnologia e justiça criminal | vigilância estatal | vigilância privada

Acesse o site ↗

InternetLab (2014)

Atuação: liberdades, privacidade e proteção de dados pessoais | tecnoautoritarismo | vigilância estatal | vigilância privada

Acesse o site ↗

Instituto Vero (2020)

Atuação: liberdades, privacidade e proteção de dados pessoais | regulamentação e o direito digital | vigilantismo digital

Acesse o site ↗

Justiça Global (1999)

Atuação: discriminação e segurança pública | monitoramento e violência contra sociedade civil | proteção de defensores de direitos humanos | tecnologia e justiça criminal

Acesse o site ↗

Observatório de Favelas (2001)

Atuação: monitoramento e violência contra a sociedade civil | proteção de defensores de direitos humanos | vigilância estatal

Acesse o site ↗

O Panóptico (2018)

Atuação: discriminação algorítmica e inteligência artificial | discriminação e segurança pública | liberdades, privacidade e proteção de dados pessoais | reconhecimento facial e dados biométricos | tecnologia e justiça criminal

Acesse o site ↗

Canadá

The Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto (2001)

Atuação: discriminação algorítmica e inteligência artificial | imigração e xenofobia | liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra a sociedade civil | proteção de direitos humanos | regulamentação e direito digital | tecnoautoritarismo | tecnologias espiãs | vigilância estatal | vigilância no combate à pandemia | vigilância privada | vigilantismo digital

Acesse o site ↗

Chile

Derechos digitales (2005)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | tecnologia e justiça criminal | vigilância estatal

Acesse o site ↗

EUA

American Civil Liberties Union – ACLU (1920)

Atuação: discriminação algorítmica e inteligência artificial | discriminação e segurança pública | imigração e xenofobia | liberdades, privacidade e proteção de dados pessoais | reconhecimento facial e dados biométricos | vigilância estatal | vigilância privada

Acesse o site ↗

The Advocates for Human Rights (1983)

Atuação: imigração e xenofobia | liberdades, privacidade e proteção de dados pessoais | vigilância estatal

Acesse o site ↗

The Association for Women's Rights in Development – AWID (1982)

Atuação: liberdades, privacidade e proteção de dados pessoais | proteção de defensores de direitos humanos

Acesse o site ↗

Eletronic Frontier Foundation (1990)

Atuação: liberdades, privacidade e proteção de dados pessoais | vigilância estatal | vigilância privada

Acesse o site ↗

Human rights watch (1978)

Atuação: discriminação algorítmica e inteligência artificial | discriminação e segurança pública | imigração e xenofobia | liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | proteção de defensores de direitos humanos | reconhecimento facial e dados biométricos | regulamentação e direito digital | tecnoautoritarismo | tecnologias espiãs | tecnologia e justiça criminal | vigilância estatal | vigilância no combate à pandemia | vigilância privada | vigilantismo digital

Acesse o site ↗

França

International Federation for Human Rights – FIDH (1992)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | proteção de defensores de direitos humanos | regulamentação e direito digital | tecnoautoritarismo | tecnologias espiãs | tecnologia e justiça criminal | vigilância estatal | vigilância privada

Acesse o site ↗

TRIAL International (2002)

Atuação: imigração e xenofobia | monitoramento e violência contra sociedade civil | vigilância estatal | vigilância privada

Acesse o site ↗

Índia

India Civil Watch – ICWI (2018)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | proteção de defensores de direitos humanos | vigilância estatal

Acesse o site ↗

México

Centro de Derechos Humanos Fray Bartolomé de Las Casas (1989)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | vigilância estatal

Acesse o site ↗

Observatorio Contra a Tortura (2019)

Atuação: liberdades, privacidade e proteção de dados pessoais | vigilância estatal

Acesse o site ↗

Red en Defesa de los Derechos Digitales (2015)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | reconhecimento facial e dados biométricos | regulamentação e direito digital | vigilância estatal

Acesse o site ↗

Nigéria

Global Rights (1978)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | vigilância estatal

Acesse o site ↗

Paraguai

TEDIC – Technology, Education, Development, Investigation, Communication (2012)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | reconhecimento facial e dados biométricos | regulamentação e direito digital | vigilância estatal | vigilância no combate à pandemia

Acesse o site ↗

Reino Unido

Anistia Internacional (1961)

Atuação: discriminação algorítmica e inteligência artificial | discriminação e segurança pública | imigração e xenofobia | liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | proteção de defensores de direitos humanos | reconhecimento facial e dados biométricos | regulamentação e direito digital | tecnoautoritarismo | tecnologias espiãs | tecnologia e justiça criminal | vigilância estatal | vigilância no combate à pandemia | vigilância privada | vigilantismo digital

Acesse o site ↗

Artigo 19 – Article 19 (1987)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | proteção de defensores de direitos humanos

Acesse o site ↗

Big Brother Watch (2009)

Atuação: discriminação algorítmica e inteligência artificial | discriminação e segurança pública | liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | reconhecimento facial e dados biométricos | regulamentação e direito digital | tecnologia e justiça criminal | vigilância estatal

Acesse o site ↗

Global Partners Digital (2014)

Atuação: liberdades, privacidade e proteção de dados pessoais | proteção de defensores de direitos humanos | regulamentação e direito digital | vigilância estatal | vigilância privada

Acesse o site ↗

Minority Rights Group Internatoinal – MRG (1969)

Atuação: monitoramento e violência contra sociedade civil

Acesse o site ↗

International Bar Association – IBA (1947)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | proteção de defensores de direitos humanos | regulamentação e direito digital | tecnoautoritarismo | vigilância estatal | vigilância privada | vigilantismo digital

Acesse o site ↗

Privacy International (1990)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | vigilância estatal

Acesse o site ↗

Suécia

Civil Rights Defenders (1982)

Atuação: discriminação e segurança pública | liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | proteção de defensores de direitos humanos | regulamentação e direito digital | vigilância estatal | vigilância no combate à pandemia

Acesse o site ↗

Varieties of Democracy – V-Dem (2014)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | vigilância estatal

Acesse o site ↗

Suíça

MENA Rights (2018)

Atuação: imigração e xenofobia | monitoramento e violência contra sociedade civil | vigilância estatal

Acesse o site ↗

Tailândia

Assistance Association for Political Prisoners – AAPP (2000)

Atuação: discriminação e segurança pública | liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | proteção de defensores de direitos humanos | vigilância estatal

Acesse o site ↗

Venezuela

Comité de Familiares de Víctimas de Caracazo – COFAVIC (1989)

Atuação: liberdades, privacidade e proteção de dados pessoais | monitoramento e violência contra sociedade civil | vigilância estatal

Acesse o site ↗

Iniciativas brasileiras que usam vigilância para auxiliar a população

O vácuo gerado pela inação do Estado na solução de problemas e formulação de políticas públicas frequentemente se torna um campo fértil para o estabelecimento de ações de vigilância e vigilantismo. Como vimos acima, grupos organizados ou atores individuais aproveitam a ausência de regulação ou a regulação precária do poder público para arbitrar sobre o destino dos cidadãos, passando por cima das leis que deveriam assegurar a integridade, a dignidade e a vida em um Estado democratico de direito.

Contudo, o intenso trabalho de algumas pessoas e organizações da sociedade civil nos mostra que a vigilância pode ser utilizada para ocupar as lacunas deixadas pelo poder público de forma positiva e com o objetivo de ajudar populações vulneráveis. Por meio de iniciativas que articulam tecnologias digitais com a proteção dos direitos fundamentais, aplicativos e outras plataformas digitais vêm sendo desenvolvidos para auxiliar a população em demandas sociais que o Estado não enxerga ou não se mostra capaz de resolver. Destacamos abaixo algumas organizações não governamentais e as ferramentas tecnológicas que têm sido criadas para suprir essa ausência estatal e auxiliar a população.

Fogo Cruzado

A falta de segurança pública é um problema recorrente, ocasionado, em grande medida, pela incapacidade do Estado em lidar com o fenômeno da violência. Tão grave quanto a falta de segurança é a ausência ou imprecisão do fornecimento de informações à população sobre onde e como a violência ocorre. O descontentamento com estas lacunas geradas pelas autoridades levou a jornalista Cecília Oliveira a idealizar a plataforma **Fogo Cruzado**. Entre o final de 2015 e o início de 2016, a

jornalista passou a coletar manualmente dados sobre tiroteios na cidade do Rio de Janeiro por meio de suas redes sociais. Ao perceber o potencial da iniciativa, surgiu então a ideia de transformá-la em uma plataforma digital.

Em entrevista para o podcast Revoar, Cecília Oliveira contou que *"cobrindo segurança pública, eu percebi o quanto que falta informação para uma cobertura mais ampla, que nos permita análises mais ricas, que sejam mais próximas da realidade. Então ali, no fim de 2015, eu lembro de ter visto uma capa do jornal Voz das Comunidades, lá do Complexo do Alemão, onde era destacada uma supermanchete: o Complexo do Alemão estava há cem dias sob tiroteios. E isso não era reverberado na grande imprensa. Chegava de uma forma picada, como se fossem eventos isolados, vamos dizer assim. E naquela época, eu estava procurando informações sobre vítimas de balas perdidas para poder fazer uma matéria. E não tinha o suficiente"*.

Foi assim que nasceu o aplicativo Fogo Cruzado, que foi ao ar, oficialmente, em setembro de 2016, um mês antes do início da olimpíada sediada no município do Rio de Janeiro. O app monitora informações sobre conflitos armados disponibilizadas por usuários, parceiros, veículos de imprensa, canais de informação de autoridades policiais e, após checagem das informações, disponibiliza a localização exata destes conflitos. Os tiroteios não apenas colocam a vida das pessoas em risco, mas também geram um grande impacto na rotina das populações, já que muitos resultam no fechamento de ruas, escolas, hospitais, alteração do trajeto de linhas de ônibus e muitas outras coisas que afetam o dia a dia de milhares de pessoas. O Fogo Cruzado não só ajuda nessa vigilância sobre a ocorrência dos tiroteios, mas também destaca esses impactos e ajuda pessoas diariamente a organizarem suas rotinas, informando sobre ruas, hospitais e estações de metrô fechadas, linhas de ônibus desviadas e outras informações úteis. Atualmente, o alcance do mapeamento colaborativo da violência armada também abrange a Grande Recife (PE). Além de informar a população, esses já embasaram a criação de um projeto de lei para que diretores de escolas possam ter autonomia para suspender as aulas em casos de tiroteios, bem como contribuíram com instituições ligadas à segurança pública servindo de subsídio para o desenvolvimento de estratégias que possam tornar o espaço público mais seguro.

PenhaS

O Brasil ocupa o 5º lugar no ranking de países onde mais ocorrem feminicídios. Aqui uma **mulher é vítima de violência a cada dois minutos**, e **nove entre dez mulheres** não confiam nos órgãos oficiais de atendimento à mulher, uma combinação perigosa que evidencia a fragilidade do poder público no amparo às vítimas desse tipo de violência. As preocupações com a triste realidade brasileira, resultado do desenvolvimento das diversas formas de violência contra a mulher no país, levou o **Instituto Az Mina a lançar em 2019, no Dia da Mulher, o Aplicativo PenhaS**. É um canal para denunciar casos de violência contra a mulher e acolher vítimas e teve o nome inspirado na Lei Maria da Penha. Foi desenvolvido a partir da escuta de especialistas e de mulheres de diferentes

idades, raças e classes sociais que compartilharam suas experiências sobre as situações por elas enfrentadas cotidianamente. O aplicativo garante o total anonimato das denunciantes. Dentre os recursos do app, destacamos o compartilhamento de informações sobre direitos das mulheres, mapas das delegacias da mulher em todo o Brasil e a ajuda em encaminhar mulheres vítimas de violência aos serviços de atendimento mais próximos. A plataforma conta com um botão do pânico que alerta pessoas selecionadas pelas usuárias em caso de urgência, além de permitir a gravação de áudio para captar o som ambiente no momento em que a violência ocorre, possibilitando que as vítimas produzam provas contra seus agressores.

Serenata de amor

A transparência nos gastos públicos é um componente fundamental da democracia. A população só pode cobrar do Estado a administração mais eficiente dos recursos se tiver conhecimento sobre como o dinheiro público está sendo gasto. A Lei de Acesso à Informação (LAI) estabelece como regra a divulgação das informações referentes à gestão pública, sendo o sigilo a exceção. Mesmo assim muitas das informações referentes à administração municipal, estadual ou federal não chegam aos cidadãos, sobretudo as que envolvem o dispêndio de recursos públicos. Nesse contexto, foi criada a **Operação Serenata de Amor** em 2016. O projeto idealizado pelo programador Irio Musskopf usa a ciência de dados e o aprendizado de máquina para fiscalizar gastos públicos e compartilhar informações de forma simples para qualquer pessoa que tenha acesso à internet.

A iniciativa funciona da seguinte forma: a robô Rosie, inteligência artificial desenvolvida por Musskopf, em conjunto com outros programadores, analisa os gastos reembolsados pela Cota para Exercício da Atividade Parlamentar (CEAP) de deputados federais e senadores feitos em exercício de sua função e identifica padrões de gastos suspeitos. A movimentação financeira monitorada é repassada ao "jarbas dashboard", um site no qual os reembolsos dos parlamentares podem ser facilmente visualizados. O serenata de amor já conseguiu identificar mais de 8.000 reembolsos suspeitos. Destes, o projeto denunciou 626 reembolsos de gastos irregulares que envolveram 216 deputados diferentes e mais de R$ 378.000.

Cocôzap

O saneamento básico é um direito garantido pela Constituição, um serviço infraestrutural que, assim como outros, é compreendido como fundamental para garantir a dignidade e a qualidade de vida da população. Sua ausência está relacionada a uma série de riscos à saúde e ao aumento na taxa de mortalidade devido ao contato com o esgoto e ao consumo de água sem tratamento. É **dever legal do Estado garantir saneamento básico** para todos os cidadãos (art. 23, inciso IX, da **Constituição**), mas sabemos que na prática isso não acontece, como no caso do complexo de favelas da

Maré, um bairro com 140.000 habitantes da Zona Norte da cidade do Rio de Janeiro (RJ). Para alertar o poder público sobre a falta de saneamento básico na Maré, o laboratório de dados **Data Labe** criou o projeto **Cocôzap** que faz um trabalho de mapeamento, incidência e participação cidadã sobre saneamento básico em favelas. A equipe do projeto, em parceria com a Casa Fluminense e a Associação Redes de Desenvolvimento da Maré, trabalha desde 2018 no Cocôzap para viabilizar um canal de denúncia, debate e proposição sobre saneamento básico, abastecimento de água e coleta de lixo na Maré a partir de um número de WhatsApp.

Dessa forma, um número de celular recebe, por meio da plataforma Whatsapp, fotos, vídeos e narrativas sobre a situação do esgoto e do lixo na Maré, de modo a localizar a dificuldade da população local em acessar esses serviços que deveriam ser fornecidos pelo poder público. Uma base de dados está sendo produzida com a intenção de construir diagnósticos complementares aos indicadores oficiais de tais serviços.O objetivo do projeto é pressionar as autoridades para o estabelecimento de políticas públicas e soluções mais eficazes, baseadas em evidências coletadas por pessoas que vivem cotidianamente o impacto da ausência de serviços básicos que deveriam ser garantidos pelo Estado.

Defezap

Anualmente, a violência causada pela ação direta do Estado mata milhares de brasileiros. Dados divulgados na última edição do **Anuário Brasileiro de Segurança Pública** mostram que, de 2013 a 2020, o número de mortes em decorrência de intervenções policiais no país cresceu durante sete anos consecutivos, culminando em 6.416 pessoas mortas no último ano da série histórica, ou seja, mais de 17 pessoas por dia só em 2020, sendo 99% homens, em sua maioria negros (79%). Do total de mortes decorrentes de intervenção policial no país, quase 20% estão concentradas no **Rio de Janeiro**. Foi essa conjuntura de explosão da violência policial que influenciou a organização sem fins lucrativos **NOSSAS**, a criar o **Defezap** em 2016, um canal de denúncias de violências cometidas pelo Estado na região metropolitana do Rio de Janeiro. Por meio do número de WhatsApp, a população fluminense ganhou um aliado importante para denunciar qualquer tipo de violência perpetrada por agentes do Estado de forma totalmente anônima e segura.

O conteúdo encaminhado pelos cidadãos ao Defezap é apurado pela equipe que trabalha no projeto e posteriormente encaminhado às autoridades responsáveis. Com o sucesso da iniciativa, que já recebeu mais de 300 materiais em vídeo com denúncias concretas e encaminhou mais de 200 investigações — muitas delas com desfechos favoráveis para os moradores de favelas (as áreas mais atingidas pela violência de Estado no Rio) —, o serviço foi **incorporado pela Comissão de Direitos Humanos da Assembleia Legislativa do Rio de Janeiro (Alerj)** em 2020 e se tornou um canal oficial do poder público para denunciar violações de direitos.

2020

Realização

LAUT

CENTRO DE ANÁLISE
DA LIBERDADE E
DO AUTORITARISMO

laut.org.br

@Laut_br

@laut-org

@Laut.org

@Laut_br

Apoio

FORD
FOUNDATION