INSTITUTO IGARAPÉ
a think and do tank

# METODOLOGIA PARA ANALISAR A IMPLEMENTAÇÃO DE **TECNOLOGIAS DE VIGILÂNCIA PELO ESTADO**

# Sumário

# METODOLOGIA PARA ANALISAR A IMPLEMENTAÇÃO DE **TECNOLOGIAS DE VIGILÂNCIA PELO ESTADO**

## Introdução

O uso de tecnologias de vigilância em diferentes países na América Latina não é algo novo. Seja no contexto de grandes eventos como a Copa do Mundo, planos de cidades inteligentes ou em meio a crises de insegurança urbana ou sanitárias, essas novas tecnologias constituem a infraestrutura para um desenvolvimento baseado em práticas de vigilância e coleta massiva de dados.

Muitos países na região já possuem leis de proteção de dados porém, elas não são suficientes para lidar com a variedade de riscos e projetos sendo implementados em diversos setores. Soma-se a isso, a dificuldade de mapear e compreender quais são os usos dessas tecnologias para além das curtas reportagens sobre casos específicos.

Considerando esse cenário, desenvolvemos uma tipologia sobre o emprego de tecnologias de vigilância por Estados na América Latina. Seu objetivo é o de auxiliar formuladores de políticas, acadêmicos, empresas e organizações da sociedade civil a melhor visualizar os diferentes componentes que integram o espectro de atividades de vigilância na região. Isso inclui setores, implementadores, tipos de tecnologias, principais fontes de dados, e funcionalidade da tecnologia.

A tipologia proporciona um *framework* para o acompanhamento sistemático de implementação desse tipo de tecnologia, podendo servir como um mecanismo para garantir maior transparência do papel do Estado na compra e uso delas. Além disso, a tipologia poderá contribuir para o desenvolvimento de políticas informadas e a consolidação de um vocabulário compartilhado para lidar com os desafios associados aos riscos e oportunidades gerados com o emprego e digitalização do governo e da sociedade.

Esse documento é dividido em três partes. Na primeira parte destacamos os principais desafios que se colocam para a compreensão da vigilância na América Latina dentro de um contexto global de expansão de tecnologias aliadas ao setor público. Na segunda, descrevemos a metodologia da tipologia que desenvolvemos para analisar a implementação de tecnologias de vigilância pelo Estado. Por fim, na terceira seção apresentamos a estrutura da tipologia a qual abarca tanto elementos tecnológicos como os dados coletados e as funcionalidades das tecnologias empregadas, bem como os principais atores e setores envolvidos.

# Contexto

A expansão da digitalização, dispositivos interconectados, aplicativos e câmeras de circuito fechado em diferentes cidades no mundo não só transformaram serviços e acesso ao conhecimento, mas também abriram novos horizontes para monitoramento em massa. Nem sempre estamos cientes da presença de sistemas de monitoramento, mas um dispositivo móvel é capaz de coletar nossa localização, dados pessoais, dados bancários, dados biométricos e entre outros. O cenário torna-se mais preocupante se considerarmos que só o Brasil possui mais de 100 milhões de usuários de smartphones.[1]

Desde grandes projetos de cidades inteligentes como o SideWalk Labs[2], do Google, que foi altamente criticado por querer instalar grandes redes de câmeras e sensores na cidade de Toronto, à expansão de dispositivos móveis para mais de 7 bilhões de pessoas[3], a vigilância tornou-se não só uma funcionalidade das tecnologias do dia a dia mas uma infraestrutura de dispositivos e sistemas que vão desde aplicativos até softwares de processamento de dados biométricos. Essa infraestrutura está cada vez mais presente no nosso cotidiano.

Apesar das preocupações com projetos quase-distópicos como o sistema de pontuação social na cidade de Rongcheng[4], na China, ou com o abuso dessas tecnologias por regimes autoritários, grande parte das democracias liberais também empregam sistemas de vigilância baseados em inteligência artificial.[5] Casos de utilização massiva de sistemas de reconhecimento facial providenciados por empresas como a Clearview AI pela Immigration and Customs Enforcement (ICE), Federal Bureau of Investigation (FBI) e entre outras agências nos Estados Unidos, não são incomuns.[6] Pelo contrário, soluções tecnológicas se tornaram um elemento central na realização das diferentes atividades do Estado e sua aplicação vai desde a coleta de dados pessoais para acesso a serviços governamentais até implementação de sistemas baseados em Inteligência Artificial (IA) para fins de segurança pública.

*A vigilância tornou-se não só uma funcionalidade das tecnologias do dia a dia mas uma infraestrutura de dispositivos e sistemas que vão desde aplicativos até softwares de processamento de dados biométricos.*

1 Salva (2022).

2 O projeto SideWalk Labs foi descontinuado em maio de 2020, devido à crise sanitária. Disponível em: https://www.sidewalklabs.com/toronto; Cecco (2019).

3 O.Dea (2022).

4 Kobie (2019).

5 Feldstein (2019).

6 Lyons (2020).

Ao invés de mirar em dicotomias como autoritarismo versus democracias liberais, China versus Estados Unidos, banir ou permitir a implementação de tecnologias de vigilância, nos concentramos nos países do 'meio'. Grande parte dos casos de implementação de tecnologias de vigilância em massa ocorrem em países e cidades em contextos que não necessariamente atendem a esses polos. Esse é o caso de países no Sul Global que, apesar de nem sempre atingirem os grandes veículos de mídia e notoriedade internacional, são utilizados como locais para treinamento de determinadas tecnologias.[7] Cidades em regiões como a África, América Latina e Ásia operam como espaços de implementação exploratória, às vezes sem arcabouço legal e capacidades técnicas adequadas para garantir tanto a proteção de dados e de direitos fundamentais como a segurança de sistemas e redes que sustentam tecnologias de vigilância. De acordo com o relatório do Carnegie Endowment for International Peace, o Sudeste Asiático, Oriente Médio e Norte da África e Américas são as regiões com maior índice de adoção de sistemas de vigilância baseados em inteligência artificial.[8]

Na América Latina, o desafio prova-se ainda maior pois o entusiasmo do solucionismo tecnológico apresenta-se em contextos de crescentes clivagens econômicas, sociais e políticas. Os últimos anos foram marcados por um aprofundamento da crise econômica e política, contando, inclusive, com a ascensão de governos com tendências autoritárias em países como Colômbia, Brasil e entre outros. O impacto da COVID-19 também ampliou a desigualdade já existente na população. Somente em 2020, o PIB das economias da região caiu 9,1%, resultando no que a Comissão para América Latina e Caribe da ONU nomeou como sendo a pior crise econômica dos últimos 120 anos. A Organização Internacional do Trabalho (OIT) estima que pelo menos 47 milhões de pessoas ficaram desempregadas desde o início da crise sanitária[9] e o Banco Mundial acrescenta que a pandemia também acelerou a implementação de soluções automatizadas e virtuais, afetando tanto os operários quanto as lojas físicas ("bricks and mortar").[10] Já no que tange ao acesso aos benefícios advindos das tecnologias da informação e comunicações (TICs), a região ainda enfrenta consideráveis disparidades entre regiões urbanas e rurais, bem como de gênero no que diz respeito à posse e uso de TICs.[11] O estudo da International Telecommunications Union (ITU) aponta que somente 74% da população urbana e 50% da população rural possuem acesso à Internet em seus domicílios nas Américas (2020).[12]

Esses e outros desafios não foram suficientes para desacelerar o passo do emprego de tecnologias de vigilância baseada em inteligência artificial (IA) como soluções para setores como saúde, segurança pública, controle de fronteiras, transportes e entre outros. Pelo contrário, a crise sanitária global resultante do alastramento da Covid-19 desde 2020 provocou um entusiasmo renovado por parte de governos na adoção de soluções tecnológicas para rastreamento de contato social, fornecimento de informações e submissão de resultados de testes. Mais de 28 aplicativos para monitoramento da Covid-19 foram implementados na América

7 Taylor; Broeders (2015).

8 Feldstein (2019).

9 Disponível em: https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_760607/lang--en/index.htm

10 Beylis et all (2020).

11 Disponível em: https://www.itu.int/en/myitu/Publications/2021/04/26/09/33/Digital-trends-in-the-Americas-region-2021

12 Disponível em: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

*Criticado pela Autoridade Nacional de Proteção de Dados brasileira, o sistema se propõe a coletar, armazenar e cruzar dados biométricos de 50,2 milhões de brasileiros.*

Latina, alguns adotando uma parceria público-privada com empresas como a Google e a Apple[13], outros desenvolvendo seu próprio sistema. Tanto em um caso quanto no outro, permanece a preocupação já levantada por especialistas, acadêmicos e ativistas sobre o despreparo do setor público na implementação efetiva de soluções adequadas para rastreamento de contato – que acabam sendo caracterizadas pela falta de transparência e pela coleta indiscriminada de dados sensíveis sobre a saúde e a geolocalização de indivíduos.[14]

Igualmente preocupante é o emprego de tecnologias na segurança pública. A Polícia Federal no Brasil anunciou em 2021 a aquisição e implementação de uma nova Solução Automatizada de Identificação Biométrica (ABIS), o qual visa modernizar a instituição e unificar dados das Secretarias de Segurança Pública no país. Criticado pela Autoridade Nacional de Proteção de Dados brasileira, o sistema se propõe a coletar, armazenar e cruzar dados biométricos de 50,2 milhões de brasileiros.[15] Soma-se à lista de tendências regionais a preocupante revelação da venda e implementação do spyware Pegasus, fornecido pela empresa israelense NSO Group, e outras soluções similares em países como Colômbia, Chile, Brasil e México.[16][17]

Frente a esses desafios, apresentamos uma tipologia para auxiliar formuladores de políticas, acadêmicos, empresas e organizações da sociedade civil a melhor visualizar os diferentes componentes que compõem o espectro de atividades de vigilância. Isso inclui setores, implementadores, tipos de tecnologias, principais fontes de dados, e funcionalidade da tecnologia. A tipologia proporciona um framework para o acompanhamento sistemático de casos de implementação de tecnologias, podendo servir como um mecanismo para garantir maior transparência do papel do Estado na compra e uso de novas tecnologias. Além disso, a tipologia poderá contribuir para o desenvolvimento de políticas informadas e a consolidação de um vocabulário compartilhado para lidar com os desafios associados aos riscos e oportunidades gerados com o emprego e digitalização do governo e da sociedade.

13 Scrollini et al (2020).

14 Disponível em: https://www.camara.leg.br/noticias/777613-especialistas-criticam-o-rastreamento-de-casos-de-covid-19-no-brasil/

15 Knoth (2021).

16 Zabludovsky; Frenkel (2016).

17 Acha (2016).

# Metodologia

A tipologia é composta por uma classificação que permite o mapeamento sistemático da implementação de tecnologias de vigilância pelo Estado. Desenvolvemos um *framework* analítico com três dimensões: principal funcionalidade da tecnologia, componentes tecnológicos e implementação. Além disso, a tipologia contém os setores que implementaram as tecnologias. As dimensões e variáveis apresentadas na próxima seção foram desenvolvidas em três etapas:

**(i) Revisão de literatura** sobre conceitos, metodologias e casos direcionados para a América Latina e Sul Global e proposição de uma primeira tipologia para analisar as tecnologias de vigilância na região;

**(ii) Levantamento de casos** por meio de fontes primárias[18] e secundárias[19], como relatórios técnicos e casos reportados pela mídia ou por notícias de órgãos governamentais;

**(iii) Consolidação da tipologia** após a sistematização e revisão dos casos levantados.

No primeiro momento, realizamos uma revisão de literatura sobre tipologias e novas tecnologias e sobre o emprego de tecnologias de vigilância de forma mais ampla – enfatizando o mapeamento de estudos diretamente relacionados ao Sul Global e à América Latina. Tendo em vista que o objetivo da pesquisa era o de compreender e melhor estudar a implementação de tecnologias de vigilância pelo Estado, desenvolvemos de forma dedutiva e indutiva uma lista de categorias macro para serem refinadas ao longo do processo de mapeamento (implementador, tecnologia, atividades, efeitos/consequências). Essa lista e estrutura inicial foi inspirada tanto pela revisão de relatórios, bem como trabalhos mais empíricos como o de Gasser et al (2020)[20] em seu trabalho sobre desafios éticos na implementação de tecnologias no contexto do COVID-19 e outros mais conceituais como Koops et al (2017)[21] que visa apresentar uma tipologia para privacidade na era digital.

Com base nessa revisão, desenvolvemos um quadro de principais casos reportados e expandimos o mapeamento em veículos de mídia tanto os de maior alcance nacional quanto outros de cobertura mais local. Ao mesmo tempo, realizamos uma busca em portais de transparência em diferentes estados no Brasil para auxiliar no processo de coleta de dados primários e melhor triangular as informações reportadas pela mídia.

Em um terceiro momento, sistematizamos os elementos que mais apareceram nos mais de 300 casos mapeados. Utilizamos ferramentas de mapeamento de ideias para destacar e identificar as tendências e alinhá-las com as categorias preliminares que haviam sido dedutivamente listadas no início da pesquisa. Nessa última etapa também realizamos a junção de categorias de forma a garantir que as tendências reportadas fossem representativas das experiências da região. Reconhecemos que a tipologia é um documento vivo que deve refletir um panorama em constante mudança e adaptações. Com isso em mente, as dimensões e categorias apresentadas na próxima seção não só foram incluídas devido sua recorrência nos casos reportados, mas também devido sua relevância para a conjuntura atual.

---

18 Na análise e mapeamento dos casos no Brasil, os portais acessados foram o (1) Tribunal de Contas da União (TCU); e o (2) Portal da Transparência. À nível estadual, o (1) Tribunal de Contas do Estado (TCE); (2) o Portal da Transparência; e (3) o Portal de Compras, esse último variando de nome em cada estado. A importância dos portais de transparência como fonte de pesquisa foi a possibilidade de maior detalhamento de aquisição sobre cada caso, bem como o acesso aos documentos do processo.

19 Relatórios, artigos, e reportagens em grandes veículos de mídia.

20 Grassser et al (2020).

21 Koops et al (2017).

# A Tipologia

Nessa seção apresentamos uma tipologia para a análise e monitoramento da implementação de tecnologias de vigilância por entidades do setor público. Na primeira parte, destacamos os principais eixos norteadores das práticas de implementação e, na segunda explicamos cada um dos componentes presentes em cada eixo.

Conforme a tabela abaixo indica, a tipologia baseia-se em quatro eixos: **setores, funcionalidade da tecnologia, componentes tecnológicos e implementação.** Por meio desses pilares, torna-se possível uma visão mais complexa e minuciosa sobre o emprego de tecnologias pelo Estado, que congrega as tecnologias envolvidas (funcionalidade da tecnologia e fontes de dados), os dados coletados (tipo de dado), elementos do processo de implementação (desenvolvedores e principal implementador), bem como a identificação dos setores que têm empregado esse tipo de tecnologia.

<table>
<tr><th>Setores</th><th>Funcionalidade da tecnologia</th><th>Componentes tecnológicos</th><th>Implementação</th></tr>
<tr><td rowspan="2">• Economia<br>• Educação<br>• Inteligência<br>• Saúde<br>• Segurança Pública<br>• Transporte<br>• Eventos/ Turismo</td><td rowspan="2">• Aplicativos<br>• Câmeras Corporais<br>• Drones<br>• Integração de bases de dados<br>• Interceptação comunicacional<br>• Monitoramento de fluxos de pessoas e objetos<br>• Monitoramento geoespacial<br>• Monitoramento informacional e/ou comunicacional<br>• Monitoramento de temperatura<br>• Predição<br>• Reconhecimento Facial<br>• Reconhecimento de Placas<br>• Spyware<br>• *Videomonitoramento</td><td>Fonte de dados<br>• GPS<br>• Bluetooth<br>• Redes Sociais<br>• Sensores<br>• Terceiros<br>• Hardware<br>• Indivíduo</td><td>Desenvolvedor<br>• Cooperação Público-Privada<br>• Setor público<br>• Setor privado<br>• Não informado</td></tr>
<tr><td>Tipo de dado coletado<br>• Dados anonimizados<br>• Dados de imagem<br>• Dados pessoais<br>• Dados biométricos<br>• Dados sensíveis<br>• Dados de geolocalização</td><td>Principal implementador<br>• Agências de Inteligência<br>• Empresas<br>• Forças Armadas<br>• Governos locais<br>• Ministérios<br>• Polícia<br>• Não informado</td></tr>
</table>

## SETORES

Os setores foram definidos considerando os que apareceram no conjunto de casos mapeados. São eles: saúde, educação, transporte, segurança pública, inteligência, economia e eventos/turismo.

O setor de **saúde** inclui hospitais, casas de saúde, clínicas, profissionais de saúde. As atividades de vigilância propagadas pelo Estado no âmbito da saúde se caracterizam pela utilização de tecnologias para o monitoramento de fluxos de pessoas, efetividade de medidas de controle de emergências sanitárias e auxílio na provisão de serviços de saúde à população.

A **educação** congrega instituições que vão desde os respectivos ministérios da educação até representações locais, escolas e universidades (públicas e privadas). As atividades de vigilância se concentram no monitoramento do fluxo de pessoas e objetos em instituições de ensino. Há ainda tecnologias que permitem monitoramento de dados para a prevenção da gravidez em adolescentes, evasão escolar e identificação da probabilidade de menores de 18 anos sofrerem violações.

No **transporte** foram consideradas as áreas que movimentam pessoas e produtos. Esse setor inclui linhas aéreas, empresas de logística, cargueiros, entre outros.

Já na **segurança pública** estão as forças policiais, determinadas atividades militares e órgãos do sistema de segurança pública e justiça criminal de um país (tal como o Ministério Público no Brasil e o Ministério do Interior no Chile). A utilização de tecnologias no contexto da segurança pública configura-se pela sua implementação na prevenção e controle da criminalidade.

O setor de **inteligência** considera as agências de Inteligência e órgãos correlatos envolvidos em atividades de inteligência para fins de segurança nacional e segurança pública.

No setor **economia** foram considerados os casos de tecnologia empregados desde a produção de matéria prima até a indústria e serviços formais e informais.

E no de **eventos/turismo,** os órgãos públicos envolvidos na organização de eventos e turismo, bem como a parcerias público-privadas para eventos públicos.

## FUNCIONALIDADES

A primeira dimensão analítica refere-se às **principais funcionalidades da tecnologia**. O entendimento de funcionalidade, apesar de estar relacionado à tecnologia, não é tecnocêntrico. Partimos do pressuposto de que toda tecnologia é social e, portanto, sua funcionalidade não se restringe às configurações operacionais (ex: geolocalização), pelo contrário, reflete a função social de monitorar espaços, fraudes, corpos, informações e entre outros elementos pautados pelo contexto social, político e econômico.

Abaixo apresentamos as definições para as principais funcionalidades das tecnologias constantes na tipologia:

### *Aplicativos*

Um software ou um programa projetado para desempenhar uma série de funções coordenadas para o fornecimento de um serviço a usuários. Para fins da tipologia, o termo 'aplicativo' se refere a um grupo específico de aplicações desenvolvidas para dispositivos móveis. Nesse sentido, o aplicativo se refere aos múltiplos programas e serviços que são disponibilizados, por exemplo, em repositórios como a Apple ou Google Play Store.

## Câmeras Corporais

Pequenos dispositivos com câmeras que são apensados ao uniforme de policiais (em sua grande maioria, próximo ao ombro) e que tem por objetivo capturar evidências de áudio e vídeo de quem as usa, do seu entorno e das suas atividades. As câmeras são comumente utilizadas para documentar a prática policial e podem ser programadas para serem ativadas automaticamente, algumas oferecem *streaming* em tempo real e ainda podem contar com reconhecimento facial e entre outros softwares.[22] A frequência, funcionalidade e características tecnológicas variam de acordo com a localidade.

## Drones

Drones são Veículos Aéreos Não-Tripulados (VANT), aeronaves de pequeno ou grande porte que, conforme sugerido pelo nome, não possuem passageiros, piloto ou tripulação a bordo.[23] Os drones são controlados remotamente e, apesar de terem sido desenvolvidos para fins militares, hoje integram múltiplas atividades como fotografia, policiamento, vigilância urbana e de fronteiras e entre outras funções.[24]

## Integração de bases de dados

Grande parte das tecnologias baseadas em Inteligência Artificial dependem de múltiplas bases de dados. Para isso, faz-se necessário integrar e/ou garantir o acesso a esses dados.

## Interceptação comunicacional

Softwares e dispositivos utilizados para interceptar comunicações, sistemas informacionais e fluxos de dados. A depender do dispositivo, a interceptação poderá ser realizada por meio de ataques *Man-In-The-Middle* que buscam quebrar a criptografia de uma comunicação. Alguns exemplos são os chamados *IMSI Catchers* e *Stingrays* que se mascaram como torres de telefonia para poder monitorar telefones dentro de um determinado perímetro.[25]

## Monitoramento de fluxos de pessoas e objetos

Essa categoria se refere à utilização de tecnologias para monitoramento de fluxos de pessoas e objetos (mercadorias, por exemplo) não só para fins de segurança pública, mas em outros setores da sociedade como a economia e a saúde. Essas tecnologias servem não só para controle no contexto policial, mas para informar o setor público sobre controle de vacinação e isolamento.[26]

## Monitoramento informacional e/ou comunicacional

Quando a principal aplicação de determinada tecnologia diz respeito a captação/coleta de informações por um terceiro de modo que os interlocutores tenham ou não conhecimento desse processo. Essas ações podem estar vinculadas a um contexto de persecução criminal e associadas com o devido processo legal de modo que o objetivo da interceptação

22 Disponível em: https://www.eff.org/pages/body-worn-cameras

23 No Brasil, a Agência Nacional de Aviação Civil (ANAC) faz uma distinção entre VANT e drone. Um VANT é definido como "aeronave projetada para operar sem piloto a bordo que não seja utilizada para fins meramente recreativos. Nesta definição, incluem-se todos os aviões, helicópteros e dirigíveis controláveis nos três eixos, excluindo- se, portanto, os balões tradicionais e os aeromodelos". VANT é a terminologia oficial utilizada pela ANAC (Circular de Informações Aéreas AIC N 21/10) ao se referir a "aeronave projetada para operar sem piloto a bordo, de caráter não-recreativo com carga útil embarcada. Ou seja, nem todo 'drone' pode ser considerado um VANT, já que um Veículo Aéreo Não Tripulado utilizado como hobby ou esporte enquadra-se, por definição legal, na legislação pertinente aos aeromodelos e não na de um VANT". Ver: https://www2.anac.gov.br/anacpedia/sig_por/tr735.htm

24 Vale destacar que "drone", dentro do contexto militar, pode se referir genericamente a um veículo terrestre, marítimo, submarino ou subterrâneo, ou seja, não necessariamente restrito a um veículo aéreo. Ver: Lefeez; Chamayou (2015).

25 https://www.eff.org/pages/cell-site-simulatorsimsi-catchers

26 Não foram consideradas para essa funcionalidade a vigilância patrimonial ou de uma determinada instituição, como órgãos do governo, por não se tratar de espaços que configuram em amplo espectro a segurança pública.

é o de oferecer provas em contextos de investigações.[27] Ferramentas de monitoramento informacional ou comunicacional também podem ser utilizadas de forma legal para pesquisas ou marketing direcionado, em inglês são chamadas de "*social media listening tools*" (ferramentas de escuta de redes sociais). Essas ferramentas analisam reações, posts, interações em redes sociais e também podem facilitar a identificação de grupos de interesse por meio de filtros. Essas e outras ferramentas permitem a coleta de informações e inteligência em fontes abertas (OSINT).

## Monitoramento geoespacial

Refere-se às atividades de vigilância baseadas em geolocalização e demarcação de perímetros territoriais. O monitoramento geoespacial pode vir a incorporar tanto as atividades de monitoramento de grandes eventos como zonas de fronteiras ou até grupos e/ou indivíduos a partir de sua geolocalização.

## Monitoramento de temperatura

Softwares e dispositivos (ex: câmeras termográficas) que são utilizados para coleta e identificação de temperatura de um ambiente e/ou temperatura corporal.

## Predição

Refere-se exclusivamente ao uso de tecnologias baseadas em machine learning e IA para a realização e cálculo de tendências baseadas em predição estatística. O caso mais emblemático de tecnologias preditivas é o PredPol, empresa estadunidense especializada em policiamento preditivo.

## Reconhecimento Facial

Software utilizado para identificação e/ou verificação da identidade de um indivíduo por meio da coleta ou cruzamento de dados relacionados a sua face.[28] O software pode operar como ponto de coleta, processamento e "*match*" de registros faciais que, por sua vez, são dados biométricos. Esses registros faciais podem se restringir a imagens especificamente delimitadas ao rosto (ex: foto utilizada para a carteira de habilitação) como podem ser extraídos de imagens de ambientes nos quais a captura nem sempre é direcionada à face, como em shoppings, bancos, estádios e entre outros ambientes públicos e privados.

A detecção de faces, seja em contextos de identificação "ao vivo" ou o cruzamento de dados estritamente faciais, se baseia na utilização de Inteligência Artificial para automatizar o processo de detecção. O reconhecimento facial é uma tecnologia controversa[29] que já foi banida ou colocada em moratória[30] em diversos contextos por ser comprovadamente dotada de tendências raciais e de gênero, afetando desproporcionalmente comunidades negras, mulheres negras, minorias étnicas e entre outros grupos.[31]

---

27 No caso do Brasil, as atividades de interceptação de comunicações em sistemas de informática e telemática são regulamentadas pela Lei 9.296 de 24 de julho de 1996, mais conhecida como a "Lei da Interceptação". A Lei regulamenta o inciso XII do art. 5 da Constituição Federal, o qual prevê que a violação do sigilo das comunicações só será aplicável "salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal." A lei também estabelece requerimentos estritos para a quebra de sigilo de comunicações, ou seja, exige indícios razoáveis da autoria ou participação na infração penal bem como a ausência de outro meio para demonstrar o fato apurado. Outras leis que também integram o escopo de atividades associadas à quebra de sigilo são o Marco Civil da Internet (Art. 10, §2º) e a Lei Geral de Telecomunicações.

28 Disponível em: https://www.eff.org/pages/face-recognition

29 Fussey; Murray (2019).

30 Simonite (2021).

31 Hardesty (2018).

## Reconhecimento de Placas

É uma tecnologia utilizada para ler placas de veículos. Quando cruzados com outras bases de dados o software de reconhecimento de placas pode ser utilizado para auxiliar na recuperação de veículos roubados, identificação de motoristas com mandato de prisão em aberto, identificação de infração de limite de velocidade e entre outras atividades.[32]

## Spyware

O *spyware* é um termo utilizado para descrever quando um código malicioso (*malware*) é utilizado para espionar atividades realizadas por dispositivo móvel ou um computador. A utilização do código malicioso permite o acesso privilegiado ao atacante a atividades de um indivíduo, podendo coletar e vigiar redes sociais, serviços de mensageria privada, senhas, até acesso a conta bancária, por exemplo, sem que este esteja ciente. Diferente da interceptação realizada mediante um mandato judicial ou sob supervisão administrativa, o *spyware* é caracterizado pelo seu uso encoberto e ilegal, bem como pela desproporcionalidade de acesso que é conferida ao atacante mediante a injeção de um *malware* em um dispositivo. O *spyware* é um dos exemplos notórios do uso abusivo de tecnologias para o aparelhamento de práticas de *hacking* governamental, isto é, perseguição de dissidentes de governos, grupos da sociedade civil, ativistas, jornalistas, organizações acadêmicas e entre outros. O software Pegasus, fornecido pela empresa Israelense NSO Group ou as ferramentas acesso remoto comercializadas pelo grupo italiano Hacking Team são apenas alguns exemplos de como *spyware*s vem sendo comercializados para governos há anos. Representa um tipo específico de tecnologia que vem sendo rechaçada publicamente como inaceitável e uma violação direta aos direitos fundamentais.[33]

## Videomonitoramento

Um sistema de monitoramento alimentado por uma rede de câmeras distribuídas (sejam esses espaços públicos ou privados) conectadas a uma central que disponibiliza as imagens e vídeos por meio de monitores.[34] Um exemplo é o Centro de Operações da Prefeitura do Rio de Janeiro que reúne tanto informações situacionais para auxiliar na segurança pública, mas contém monitoramento de condições meteorológicas alarmantes para a cidade como tempestades e chuvas fortes.[35]

32 Disponível em: https://whatis.techtarget.com/definition/Automated-License-Plate-Recognition-ALPR

33 O caso do Pegasus Project, relatório publicado pela Anistia Internacional e outras organizações trouxe à luz dinâmicas que já haviam sido reportadas anteriormente sobre a utilização de spyware para perseguição de jornalistas e ativistas no México e em outros países. O Brasil, chegou próximo a adquirir a tecnologia em um pregão da Secretaria de Operações Integradas que requisitava uma ferramenta para realizar Inteligência de Fontes Abertas (OSINT). Apesar do NSO Group ter retirado sua proposta, vários países na América Latina já adquiriram soluções similares fornecidas pelo Hacking Team.

34 Disponível em: https://www.centralcftv.com/

35 Disponível em: http://cor.rio/institucional/

# COMPONENTES TECNOLÓGICOS

A utilização de tecnologias para fins de vigilância requer um olhar minucioso sobre quais **componentes tecnológicos** viabilizam a operação de determinados softwares e dispositivos, bem como a coleta de tipos específicos de dados. A lista de definições abaixo visa proporcionar um olhar desagregado sobre esses componentes, mais especificamente, sobre **fontes de dados** e **tipos de dados coletados** presentes em casos reportados de vigilantismo Estatal.

# FONTE DE DADOS

*Meios pelos quais os dados são coletados.*

## *Bluetooth*

Um padrão tecnológico de comunicação sem fio ("wireless") que permite a transmissão e recebimento de dados entre dispositivos.[36]

## *GPS*

Sigla advinda do seu nome em inglês, o Global Positioning System (GPS), é uma tecnologia que permite a navegação e georreferenciamento de objetos e pessoas via a recepção de sinais por satélite.

## *Indivíduo*

Quando o indivíduo se torna a principal fonte de dados. Isso inclui tanto o fornecimento deliberado de informações para acessar um determinado serviço quanto, por exemplo, a coleta do registro facial e entre outros dados biométricos de indivíduos de forma não consensual.

## *Redes Sociais*

Sites e aplicações por meio dos quais indivíduos e grupos podem criar, compartilhar e/ou trocar informações em uma comunidade virtual. Grande parte desses sites e aplicações são denominados de 'plataformas' pela função que exercem ao providenciarem um espaço programado para relações sociais, culturais, econômicas e comunicacionais se desenvolverem. Essas plataformas abarcam desde as mais notórias redes sociais como o Facebook e Whatsapp, por exemplo, até outras como blogs (ex: Medium).

## *Sensores*

Dispositivos que detectam e/ou respondem a um tipo de input (luz, temperatura, pressão, fumaça) e o transformam em uma medição capaz de ser processada por computadores.[37]

## *Terceiros*

Quando a fonte de dados não se restringe ao indivíduo, mas é terceirizada por meio da contratação de serviços de corretoras de dados também conhecidos como "data brokers". Esses "brokers" trabalham com a venda de diferentes tipos de dados de consumidores para que outras empresas possam gerar conhecimento com base nas informações obtidas.[38] Eles agregam, classificam, comercializam e precificam dados.[39] Para além dos corretores de dados, a fonte de dados também pode incluir bases de dados de diferentes ministérios, órgãos governamentais e entre outras entidades que depois são disponibilizadas para usos de outros órgãos ou para serviços aos cidadãos.

36 Câmara (2012).

37 Wigmore (2012).

38 Souza (2021).

39 As atividades de corretagem de dados são utilizadas para fins de marketing direcionado, por exemplo. No entanto, esse modelo de negócio é marcado por uma série de preocupações sobre o uso e coleta de dados pessoais, por mais agregados que sejam. Ver também Roderick (2014).

### *Hardware*

Quando um determinado dispositivo, tal como um computador ou dispositivo móvel (smartphone ou telefone), torna-se o principal alvo e/ou fonte de dado.

## TIPO DE DADOS COLETADOS

***Dados anonimizados***
Dado relativo a um titular que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Os dados precisam passar por um processo de anonimização, no qual perde a possibilidade de associação, direta ou indireta, a um indivíduo.[40]

### *Dados biométricos*

Dados gerados a partir de registros e cálculos de traços biológicos humanos como o corpo, rosto, impressão digital (datilograma), globo ocular e entre outros elementos.[41]

### *Dados de geolocalização*

Dados associados com o posicionamento geográfico de um determinado objeto. Esses dados podem ser coletados por meio de GPS, protocolos IP, o endereço MAC de um dispositivo, sistemas de radiofrequência e entre outros indicadores de localização.

### *Dados de imagem*

Dados associados a coleta de uma imagem e/ou vídeo (sequência de imagens).

### *Dados pessoais*

Informação relacionada à pessoa natural identificada ou identificável.[42] Os dados pessoais incluem informações diretamente associadas a um determinado indivíduo como os dados cadastrais (CPF, RG, nome, endereço).

### *Dados sensíveis*

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, quando vinculado a uma pessoa natural.[43]

## IMPLEMENTAÇÃO

As categorias abaixo refletem os dois pilares centrais para a identificação e mapeamento dos agentes envolvidos na implementação de tecnologias de vigilância pelo Estado: **desenvolvedores** e **principais implementadores**.

## DESENVOLVEDOR

As tecnologias de vigilância podem ser desenvolvidas exclusivamente pelo Estado. O **setor público** pode alocar recursos para produzir tecnologias específicas para que sejam empregadas no próprio conjunto de órgãos públicos a fim de otimizar suas atividades, por meio de agências especializadas, programas de pesquisa e desenvolvimento científico, empresas públicas ou pelos servidores das próprias secretarias.[44]

---

40 Art. 5 III LGPD (Brasil, 2012).

41 Apesar de dados biométricos serem, em sua grande maioria, dados sensíveis, destacam-se por serem objeto central de diversas tecnologias de vigilância e, por esse motivo, foram separados da definição de dados pessoais.

42 Art. 5 I LGPD (Brasil, 2012).

43 Art. 5 II LGPD (Brasil, 2012). Ver também GDPR Art. 4 1, 13, 14, 15 (Uniao Europeia, 2016).

44 Por exemplo, é emblemático o caso do desenvolvimento do chamado Sistema Tecnológico para Acompanhamento de Unidades de Segurança (Status) fomentado pela Fundação Cearense de Apoio ao Desenvolvimento Científico e Tecnológico (Funcap), em parceria com a Superintendência de Pesquisa e Estratégia de Segurança Pública (Supesp) para implementação no âmbito das atividades da Secretaria de Segurança Pública e Defesa Social do Estado do Ceará (SSPDS/CE).

Por outro lado, a tecnologia pode ser inteiramente desenvolvida pelo **setor privado**. Os entes privados podem atuar de diversas formas, entre elas: doando tecnologia e/ou auxiliando na instalação das mesmas.

Já no contexto da **cooperação p**úblico-privada o setor público e o setor privado assumem diferentes responsabilidades no processo de desenvolvimento conjunto de uma tecnologia. Durante a pandemia da COVID-19, a cooperação público-privada foi um elemento central no desenvolvimento de tecnologias para monitoramento de sintomas e rastreamento de contato com possíveis infectados.

## PRINCIPAL IMPLEMENTADOR

As **agências de inteligência** desempenham o papel de coleta, monitoramento e exploração de informações para avaliação de riscos à segurança nacional. As atividades de inteligência podem ser divididas em pelo menos, três categorias: estratégica, tática e de contra-inteligência. As agências utilizam tecnologias na condução dessas atividades, as quais incluem mas não se restringem à escuta, monitoramento de redes sociais, análise em fontes abertas, entre outras práticas.

**Empresas** podem atuar tanto com o fornecimento de tecnologia quanto auxílio na sua operacionalização em um projeto com entes públicos.

Constituídas pela Marinha, pelo Exército e pela Aeronáutica, as **Forças Armadas** podem auxiliar processos de implementação de tecnologias em situações de crise ou em projetos conjuntos com outros órgãos como as agências de inteligência e polícias. Além disso, as Forças também implementam tecnologias para explorar vulnerabilidades e auxiliar em atividades de espionagem ou hacking governamental.

Já os **governos locais**, eleitos e encarregados de administrar e prover serviços aos cidadãos em uma determinada localidade (ex: municipalidades, conselhos locais) empregam tecnologia na modernização, monitoramento e fornecimento de serviços ao cidadão. Alguns exemplos são a implementação de tecnologias de reconhecimento facial em transportes públicos e projetos de cidades inteligentes que acabam por criar um sistema de vigilância em escala.

De forma similar, os **Ministérios**, estão encarregados da administração e emprego de projetos de vigilância em escala nacional como a integração e centralização de grandes bases de dados biométricos, facilitação de registros documentais por meio do estabelecimento de portais e entre outras atividades.

Por fim, a **polícia** emprega tecnologia para repressão e investigação de crimes, controle da violência, monitoramento populacional, análise forense, dentre outras atividades.

# Considerações finais

A tipologia proporciona um *framework* para o acompanhamento sistemático de implementação de tecnologias de vigilância pelo Estado. No documento apresentamos uma classificação dos diferentes componentes que caracterizam as práticas de vigilância e implementação de tecnologias em diferentes setores tais como funcionalidades tecnológicas, fonte de dados e tipos de dados coletados além do agente implementador.

A partir do levantamento de mais de 300 casos mapeados no Brasil e na América Latina, busca-se contribuir para a consolidação de um vocabulário compartilhado que poderá auxiliar organizações governamentais e não-governamentais a analisarem o contexto de vigilância estatal que vem sendo empregado na região.

# Referências Bibliográficas

Acha, Gisela P. (2016). Hacking Team Malware para la Vigilancia en America Latina. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

Agência Câmara de Notícias (2021). Especialistas criticam o rastreamento de casos de Covid-19 no Brasil. Disponível em: https://www.camara.leg.br/noticias/777613-especialistas-criticam-o-rastreamento-de-casos-de-covid-19-no-brasil/

ANAC. VANT. Disponível em: https://www2.anac.gov.br/anacpedia/sig_por/tr735.htm

Beylis, Guillermo; Fattal-Jaef, Roberto; Sinha, Rishabh; Morris, Michael; Sebastian, Ashwini Rekha (2020). Going Viral: COVID-19 and the Accelerated Transformation of Jobs in Latin America and the Caribbean. World Bank Latin American and Caribbean Studies;. Washington, DC: World Bank. Disponível em: https://openknowledge.worldbank.org/handle/10986/34413

Brasil (2012). Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Buolamwini, Joy Adowaa (2017). Gender shades : intersectional phenotypic and demographic evaluation of face datasets and gender classifiers. Thesis: S.M., Massachussetts Institute of Technology, Prorgam in Media Arts and Sciences. Disponível em: https://dspace.mit.edu/handle/1721.1/114068

Câmara, Marlon (2012). Bluetooth: O que é e como funciona. Disponível em: https://www.techtudo.com.br/noticias/2012/01/bluetooth-o-que-e-e-como-funciona.ghtml

Cecco, Leyland (2019). 'Irrelevant': report pours scorn over Google's ideas for Toronto smart city. Disponível em: https://www.theguardian.com/cities/2019/sep/11/irrelevant-panel-pours-scorn-over-googles-ideas-for-toronto-smart-city

Central CFTV. O que é CFTV. Disponível em: https://www.centralcftv.com/

COR. Alta tecnologia a serviço da cidade. Disponível em: http://cor.rio/institucional/

EFF (2017). Body worn cameras. Disponível em: https://www.eff.org/pages/body-worn-cameras

_____. Cell-Site Simulators/IMSI Catchers. Disponível em: https://www.eff.org/pages/cell-site-simulatorsimsi-catchers

_____. Face recognition. Disponnível em: https://www.eff.org/pages/face-recognition

_____. Government Hacking and Subversion of Digital Security. Disponível em: https://www.eff.org/issues/government-hacking-digital-security

Feldstein, Steven (2019). The Global Expansion of AI Surveillance. Disponível em: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Fussey, Peter and Murray, Daragh (2019) Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. Project Report. University of Essex Human Rights Centre. Disponível em: http://repository.essex.ac.uk/id/eprint/24946

Grasser, Urs; Ienca, Marcello; Scheibner, James; Sleigh, Joanna; Vayena, Effy (2020); Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. The Lancet Digital Health, Volume 2, Issue 8, pp. e425-e434, ISSN 2589-7500,. Dispoível em: https://www.sciencedirect.com/science/article/pii/S2589750020301370

ILO/ECLAC (2020). Slow COVID-19 labour market recovery expected in Latin America and the Caribbean. Disponível em: https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_760607/lang--en/index.htm

ITU (2020). Digital trends in the Americas region 2021. Disponível em: https://www.itu.int/en/myitu/Publications/2021/04/26/09/33/Digital-trends-in-the-Americas-region-2021

ITU (2021). Measuring digital development: Facts and figures 2021. Disponível em: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

Knoth, Pedro (2021). Sistema de vigilância da Polícia Federal é questionado na ANPD. Disponível em: https://tecnoblog.net/463463/sistema-de-vigilancia-da-policia-federal-e-questionado-na-anpd/

Kobie, Nicole (2019). The complicated truth about China's social credit system. Disponível em: https://www.wired.co.uk/article/china-social-credit-system-explained

Koops, Bert-Jaap; Clayton, Bryce N., Timan, Tjerk; Skorvánek, Ivan, Chokrevski, Tomislav; Galic, Masa (2017). A Tipology of Privacy. Legal Scholarship Repository, pp. 483-575. Disponível em: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1938&context=jil

Hardesty, Larry. Study finds gender and skin-type bias in commercial artificial-intelligence systems. Disponível em: https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

Lefeez, Sophie; Chamayou, Grégoire (2015). Théorie du drone. *Socio-anthropologie* [En ligne], 28. Disponível em: http://journals.openedition.org/socio-anthropologie/1617

Lyons, Kim (2020). ICE just signed a contract with facial recognition company Clearview AI . Disponível em: https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration

O'Dea, S. (2022). Number of smartphone subscriptions worldwide from 2016 to 2027 (in millions). Disponível em: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Ogasawara, Midori (2019). Mainstreaming Colonial Experiences in Surveillance Studies. Disponível em: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13521

Roderick, Leanne (2014). Discipline and Power in the Digital Age: The Case of the US Consumer Data Broker Industry. Critical Sociology 40, no. 5. pp. 729–46. https://journals.sagepub.com/doi/abs/10.1177/0896920513501350.

Sava, Justina A. (2022). Number of smartphone users in selected countries in Latin America in 2020 (in millions). Disponível em: https://www.statista.com/forecasts/274689/forecast-of-mobile-phone-users-in-latin-america

Scrollini, Fabrizio; Baliosian, Javier; Etcheverry, Lorena; Moncecchi, Guillermo (2020). Uruguay's COVID 19 contact tracing app reveals the growing importance of data governance frameworks. Disponível em: https://blogs.lse.ac.uk/latamcaribbean/2020/08/26/uruguays-covid-19-contact-tracing-app-reveals-the-growing-importance-of-data-governance-frameworks/

Simonite, Tom (2021). Face Recognition Is Being Banned—but It's Still Everywhere. Disponível em: https://www.wired.com/story/face-recognition-banned-but-everywhere/

Souza, Ramon (2021). O que são data brokers e como eles funcionam. Disponível em: https://canaltech.com.br/seguranca/o-que-sao-data-brokers-e-como-eles-funcionam-176757/

Taylor, Linnet; Broeders, Dennis (2015). In the name of Development: Power, profit and the datafication of the global South. Vol. 64, pp. 229-237 https://www.sciencedirect.com/science/article/abs/pii/S0016718515001761?via%3Dihub

Tech Target Contributor (2011). Automated License Plate Recognition (ALPR). Disponível em: https://whatis.techtarget.com/definition/Automated-License-Plate-Recognition-ALPR

União Europeia (2016). Regulamento Geral sobre a Proteção de Dados. Disponível em: https://eur-lex.europa.eu/legal-content/pt/TXT/?qid=1559291025147&uri=CELEX:32016R0679#d1e40-1-1

Wigmore, Ivy (2012). Definition-Sensor. Disponível em: https://whatis.techtarget.com/definition/sensor

Zabludovsky, Karla; Frenkel, Sheera (2016). Nearly Every Latin American Country Is Using This Software To Spy On Their Citizens. Disponível em: https://www.buzzfeednews.com/article/karlazabludovsky/nearly-every-latin-american-country-is-using-this-software-t

# Leia também


**E CONHEÇA**
Portal Brasileiro
da Cibersegurança


**AE 58 Implementação de tecnologias de vigilância no Brasil e na América Latina**
(Outubro 2022)


**CIBERSEGURANÇA NO BRASIL: uma análise da estratégia nacional**
Louise Marie Hurel.
(Abril 2021)


**REGULAÇÃO DO RECONHECIMENTO FACIAL NO SETOR PÚBLICO**
Pedro Augusto P. Francisco, Louise Marie Hurel e Mariana Marques Rielli**.**
(Junho 2020)

# INSTITUTO IGARAPÉ
a think and do tank

O Instituto Igarapé é um think and do tank independente, dedicado à integração das agendas de segurança, clima e desenvolvimento. Nosso objetivo é propor soluções e parcerias a desafios globais por meio de pesquisas, novas tecnologias, influência em políticas públicas e comunicação. Somos uma instituição sem fins lucrativos, independente e apartidária, com sede no Rio de Janeiro, mas cuja atuação transcende fronteiras locais, nacionais e regionais. Premiada como a melhor ONG de Direitos Humanos no ano de 2018, o melhor think tank em política social pela Prospect Magazine em 2019 e considerada pelo Instituto Doar, pelo segundo ano consecutivo, como uma das 100 melhores organizações brasileiras do terceiro setor.

**O programa de Segurança Digital** do Instituto Igarapé se dedica ao desenvolvimento de pesquisas interdisciplinares, facilitação de diálogos intersetoriais e promoção de espaços de confiança e conscientização para o avanço de políticas digitais. Trabalhamos com temas como segurança digital, crimes na Internet, inteligência artificial, Internet das coisas, proteção de dados e cidades inteligentes. Construímos plataformas, pensamos criticamente sobre o impacto dessas tecnologias na sociedade e trabalhamos para abordar os desafios à proteção de direitos digitais mediante o avanço da implementação de tecnologias em nosso dia a dia. **igarape.org.br/temas/seguranca-digital**

**Instituto Igarapé**

Rio de Janeiro - RJ - Brasil
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org
instagram.com/igarape_org/

**igarape.org.br**

**Direção Criativa**
Raphael Durão - STORMdesign.com.br

igarape.org.br

INSTITUTO IGARAPÉ
a think and do tank