

RELATORIA FIB 15

28 de maio | Sala 1 Fiesta Bahia Hotel, Salvador - BA | 16:30 às 18:00

- Título da sessão: **Para além das muralhas: Vigilância Urbana e Direitos Civis**

- Proponentes e co-proponentes: Coalizão Direitos na Rede (CDR) e entidades que atuam no GT Vigilância, Plataforma Ização e Proteção de Dados da CDR. **Terceiro Setor.**

- Palestrantes:

a. **Julia Faustino Abad** (Analista da Coordenação-Geral de Políticas Temáticas da Secretaria Nacional de Direitos da Criança e do Adolescente do Ministério de Direitos Humanos e Cidadania e mestrandia em Gestão Urbana na PUC-PR). **Representante do setor governamental.**

b. **Tatiana Coutinho** (Lima ≡ Feigelson Advogados). **Representante do setor empresarial.** Sócia da área de Data Privacy e Cybersecurity e Artificial Intelligence no escritório Lima ≡ Feigelson Advogados. Especializada em Processo Civil, Governança em Tecnologia da Informação, Privacidade e Proteção de Dados Pessoais, Regulação e Novas Tecnologias e Direito Digital. Certified Data Protection Officer, Information Privacy Management, DPO EXIN, pesquisadora voluntária no Ethics4AI.

c. **Jéssica Ribeiro Cardoso** (C-Partes). **Representante do terceiro setor.** Formada em Direito, com especialização em Direito e Processo do Trabalho; membra pesquisadora do Grupo de Pesquisa C-PARTES e defensora popular de Direitos Humanos.

d. **Rodrigo José Firmino** (Pontifícia Universidade Católica do Paraná). **Representante da comunidade científica e tecnológica.** Professor titular do Programa de Pós-Graduação em Gestão Urbana na PUCPR. Doutor em planejamento urbano e regional (Newcastle University), mestre em arquitetura e urbanismo (USP), e formado em arquitetura e urbanismo (UNESP). Membro-fundador da Rede LAVITS. Pesquisa sobre: tecnologias urbanas, vigilância, urbanismos periféricos e ativismo digital.

e. **Moderador:** Pedro Diogo Carvalho Monteiro. **Representante do Terceiro Setor.** Coordenador do GT Vigilância e Novas Tecnologias no Laboratório de Políticas Públicas e Internet (LAPIN). Doutorando em Direito pela Universidade de Brasília (UNB). Mestre em Direito Penal e Liberdades Públicas na Universidade Federal da Bahia. Pesquisa temas relacionados à vigilância, sistema penal e terror racial, também tocando novas tecnologias, proteção de dados e Inteligência Artificial. Consultor na Coalizão Direitos na Rede (CDR).

f. **Relatora:** Ana Mielke. **Representante do Terceiro Setor.** Jornalista, mestre em Ciências da Comunicação pela Escola de Comunicações e Artes (USP), com pós-graduação em História, Sociedade e Cultura, pela PUC-SP. É membro do grupo de pesquisa 'Violência em tempos sombrios', ligado ao Núcleo de Estudos da Violência (NEV-USP), coordenadora executiva do Intervozes - Coletivo Brasil de Comunicação Social, membro da executiva do FNDC e da Coalizão Direitos na Rede (CDR).

- **Objetivos e Resultados**

O workshop teve por objetivo discutir os planos de ampliação das iniciativas de vigilância urbana sob a ótica dos direitos civis, com foco em como essas infraestruturas impactam a liberdade e a privacidade dos cidadãos e afetam desproporcionalmente grupos marginalizados em marcadores de raça, gênero e classe. A implementação crescente de projetos como o Muralha Paulista (SP), Câmera Interativa (BA) e Muralha Digital (PR) levanta questões cruciais sobre segurança pública e proteção dos direitos individuais, e o workshop busca promover uma reflexão aprofundada sobre esse tema, visando conscientizar sobre os efeitos dessas medidas no cotidiano dos cidadãos. Como objetivos secundários, o workshop explorou o cenário atual de utilização das tecnologias de vigilância para identificar os principais atores envolvidos, tanto do setor público quanto do privado.

A compreensão de quem são os responsáveis pelo desenvolvimento e aplicação dessas tecnologias é fundamental para traçar um panorama completo das forças em jogo e dos interesses que influenciam o aumento da vigilância nas cidades. Dessa forma, buscou-se produzir uma avaliação das implicações dessas iniciativas para os direitos civis, discutindo de que maneira a expansão desses sistemas pode comprometer direitos fundamentais como a privacidade, a liberdade de expressão e outras garantias constitucionais. Por fim, o workshop buscou destacar a importância da governança multissetorial nesse contexto, reforçando a necessidade de uma abordagem inclusiva e participativa, tendo a transparência e a não-discriminação como eixos centrais.

O maior resultado deste workshop foi justamente lançar luz sobre o debate da vigilância em massa e do uso de reconhecimento facial na segurança pública - tema muitas vezes secundado nos debates regulatórios. Sendo assim, o workshop contribuiu para que os participantes compreendessem os desafios relacionados à privacidade e proteção de dados na segurança pública a partir de exemplos já implementados e de reflexões que vêm sendo construídas em diferentes territórios do país. Outro resultado é a produção deste relatório final com a sistematização das discussões, o que permite a continuidade do diálogo entre setores e o fortalecimento de redes colaborativas para discutir o acesso à cidade, vigilância e segurança pública centrados na garantia de direitos fundamentais.

- **Justificativa em relação à governança da internet:**

Considerando o fundamento provido pelos Princípios para a Governança e Uso da Internet no Brasil, aprovados pelo Comitê Gestor da Internet no Brasil no ano de 2009, entende-se que a proposta possui ampla relação com a liberdade, a privacidade e a observância de direitos humanos - já que promove um debate em favor dos direitos civis no que é afeto às tecnologias digitais na segurança pública, a fim de ser garantida a livre fruição de espaços públicos. Ainda, entende-se que apenas a governança democrática e participativa, promovida a partir da escuta adequada, do diálogo e da construção coletiva, é que se alcança resultados efetivamente democráticos.

A discriminação não é um tema novo no cenário brasileiro. Contudo, o uso indiscriminado de tecnologias digitais em uma sociedade conectada tem potencializado o alcance e a incidência de tomadas de decisões discriminatórias que podem afetar grupos vulneráveis inteiros. Assim sendo, se as tecnologias digitais aplicadas à segurança pública podem causar tanto dano a uma sociedade utilizando a internet como um mediador de

relações, torna-se mais do que necessário que se discuta o fenômeno através de uma perspectiva da lei e dos princípios para a boa governança da Internet.

- **Metodologia e formas de participação desenvolvidas durante a atividade**

O workshop contou com 1h30 de duração e foi desenvolvido em uma perspectiva dinâmica com enfoque no diálogo e interação entre os setores governamental, empresarial, terceiro setor, comunidade científica e tecnológica e a audiência. O moderador fez uma breve contextualização sobre o tema e incentivou a participação ativa da audiência presencial e remota ao longo de todo o workshop, utilizando enquetes e perguntas em tempo real para engajar os participantes virtuais e presenciais.

O painel foi dividido em blocos temáticos curtos, seguidos por sessões de perguntas e discussão. Estudos de caso práticos, como o Muralha Paulista (SP), Muralha Digital (PR), Câmara Interativa (BA), foram usados para debater governança de dados, segurança da informação e os impactos das tecnologias de vigilância. As contribuições dos participantes e também do público presente resultaram na sistematização deste relatório, que traz alguns pontos consensuais do debate e os desafios impostos aos setores envolvidos.

- **Síntese dos Debates**

O moderador Pedro Diogo Carvalho iniciou saudando o público presente e apresentando o debate que teria início. Fez a leitura de um pequeno trecho de um panfleto publicitário de uma empresa que oferta serviços de tecnologias e segurança no qual há uma expressa defesa do uso das chamadas “muralhas digitais” como estratégia de proteção contra o crime, mas também como estratégia de controle total das cidades. Depois disso, apresentou os exemplos mais emblemáticos de uso destas tecnologias como Muralha Digital (PR), Câmara Interativa (BA) e Muralha Paulista (SP). Em seguida, fez uma apresentação dos currículos dos palestrantes participantes da mesa e abriu o painel apresentando perguntas disparadoras para cada um das/os palestrantes.

O professor Rodrigo Firmino iniciou sua participação apresentando a dissertação de mestrado de Henrique Kramer da Cruz, defendida em 2025, que tem como título “Muralha digital: análise crítica do sistema de videomonitoramento da cidade de Curitiba”. Nela o autor conduz uma análise sobre o uso das tecnologias de vigilância na cidade de Curitiba como uma possível promessa de segurança pública. Além desta dissertação, também fez referência a outro texto, produzido em parceria com diferentes autores como Gabriel Pereira, Julia Abadi, Henrique Kramer, Carolina Israel e o próprio Rodrigo Firmino, em que os autores produzem uma crítica à muralha digital a partir da economia política. Firmino alerta ao fato de que, embora o Muralha Digital tenha sido oficializado em 2021, trata-se de um projeto de concepção mais antiga, o que o coloca como um dos pioneiros nesta esfera de uso de tecnologias de vigilância para uso na segurança pública, chamada de muralhas.

Na sequência Firmino cita a frase do então prefeito de Curitiba, Rafael Greca, quando do lançamento do Muralha Digital, em 2012. “A muralha digital é uma estrutura da prefeitura de Curitiba que não dorme. É a contribuição de Curitiba - cidade inteligente - à segurança da região metropolitana de Curitiba. Com o cerco digital de segurança ao redor da cidade temos agora a possibilidade de segurança em tempo real. A cidade passa a ser

completamente controlada, não mais permanecerá o corpo de uma criança numa mala no salão da rodoviária como no caso da menina Rachel Genofre.” (referindo-se a um crime hediondo de 2008 que chocou o país). Para Firmino, a fala do ex-prefeito é carregada de simbologias que demonstram o entendimento acerca do uso das tecnologias de vigilância.

De acordo com Firmino, há uma indissociabilidade entre os projetos de segurança digital - ou uma promessa de segurança a partir das tecnologias - e o projeto de cidades inteligentes. Não é apenas uma associação. Para ele, a maior parte dos projetos de cidades inteligentes tem como bandeira o projeto de segurança digital. Ele fala de um duplo tecno-solucionismo envolvido: de uma lado prometendo uma cidade controlada e gerida em tempo real e ao mesmo tempo o uso de tecnologias de inteligência que não falham e que são capazes de deixar as cidades mais seguras.

Na sequência ele apresentou como projeto Muralha Digital que é gerido na cidade de Curitiba. Trata-se de um projeto que conta com mais duas mil câmeras e que prevê a expansão a partir da integração de câmeras privadas; especialmente do comércio, e que prevê o uso de reconhecimento facial, leitura de placas, câmeras térmicas, sensores analíticos e integração com outros bancos de dados. Tudo isso sendo tudo controlado por um centro de controle, gerido pela Guarda Municipal de Curitiba e está na sede do ICI – Instituto Cidades Inteligentes (antigo Centro de Processamento de Dados - CPD). É uma OS (organização social) de status privado, o que é importante salientar neste caso. A prefeitura aluga um pacote de segurança, como os radares de segurança. Todos os contratos da Prefeitura são com o ICI, sendo portanto, o maior cliente desta OS. Neste caso, a prefeitura não compra e nem faz manutenção de equipamentos e sim compra um pacote de segurança. Na verdade, aluga um pacote de segurança, tal qual o funcionamento dos radares de segurança nas cidades. Este modelo de negócios coloca dificuldade sobre a transparência dos contratos, que são quase impossíveis de serem analisados. O ICI vende o mesmo serviço/consultoria para outras cidades do Brasil e de Portugal. E é por isso que a gente sentiu a necessidade de entender o modelo de negócios que vem se replicando a partir da economia política destes projetos de cidade segura, vigiada e controlada.

Por fim, Rodrigo Firmino fez uma referência ao brasileiro Milton Santos em textos em que o geógrafo tece críticas ao que denomina de fábula sobre a globalização. Ou uma promessa de vida plena, baseada em um discurso sedutor que, na maior parte das vezes, esconde as perversidades do processo de globalização. Firmino traz esta referência de fábula para a crítica sobre as cidades inteligentes, cujo discurso sedutor também está baseado em uma promessa de eficiência, conectividade e proteção, mas esconde as perversidades como controle social, exclusão e desigualdades. Para ele, trata-se de um “canto de sereia” – desvendar um pouco estas perversidades e desmontar o discurso sedutor das cidades inteligentes.

A segunda participação foi da Júlia Faustino Abad, pela Secretaria Nacional de Direitos da Criança e do Adolescente do MHDC. Ela iniciou fazendo sua audiodescrição e na sequência apontou que o debate sobre reconhecimento facial na segurança pública também precisa ser olhado a partir dos impactos sobre crianças e adolescentes. Apontou ainda que este reconhecimento facial tem sido implementado em escolas e estádios sem o cuidado do ECA e das percepções que sobre proteção de crianças e adolescentes que existem na LGPD. apresentou um estudo realizado pelo grupo de pesquisa Jararaca e

Tecnosfera que faz uma análise do reconhecimento facial nas escolas do Paraná e os impactos que isso tem causado, a partir da escuta de técnicos da implementação e de professores. Alertou que a tecnologia do reconhecimento facial já está sendo implementada em momento delicados como os da aprendizagem, sem que se tenha estudos conclusivos sobre os impactos disso.

O ECA prevê o livre desenvolvimento de personalidade e o uso de reconhecimento facial dentro da sala de aula tem impacto sobre isso. No Paraná isso tem sido utilizado, por exemplo, para fazer chamadas e confirmar a presença, mesmo sendo uma tecnologia falha. Muitos professores tem relatado que alunos negros não são reconhecidos nas fotos. E isso gera um gasto de tempo dos professores, que precisam coletar novamente as fotos, além de impor a coleta de dados biométricos de crianças e adolescentes que estão sendo coletados todos os dias. O livre desenvolvimento de personalidade vem sendo travado, porque os alunos estão com uma câmera em sala de aula captando seus dados e reconhecendo suas emoções o tempo todo. O ambiente de ensino deve ser de liberdade de expressão e aprendizagem e o uso das câmeras acabam se tornando uma muralha. Outra questão apontada por ela é do uso do reconhecimento facial nos estádios. Ela citou pesquisa realizada pelo Centro de Estudos de Segurança e Cidadania (Cesec) sobre a coleta de dados de adolescentes nos estados e apontou que, em Goiás, 30 mil rostos de crianças e adolescentes foram coletados, sendo 14% de menores de 16 anos.

Na sequência ela falou sobre a produção do “Guia sobre Uso de Dispositivos Digitais - Crianças, Adolescentes e Telas” da preocupação do governo federal em refletir sobre os problemas do ambiente digital. Para a produção do Guia foi realizada uma escuta de crianças e adolescentes para entender como eles lidam com as plataformas. A produção foi realizada em parceria com o Instituto Alana e a Embaixada do Reino Unido. Fez uma referência a duas resoluções do Conanda: 245 e 257 publicadas em 2024 e que tratam da necessidade de estabelecer uma Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. A segunda resolução prevê, além da política nacional, a constituição do Comitê Intersectorial, que será responsável por assegurar a coordenação e a articulação para as ações conjuntas e integradas. Citou ainda o acompanhamento dos projetos de lei em tramitação que envolvem o tema, tais como o PL 2628, que trata da proteção de crianças e adolescentes no ambiente digital, e o PL 2338, que é de regulação do uso da Inteligência Artificial (IA). Um dos fundamentos deste PL é, inclusive, o livre desenvolvimento de personalidade e a proteção de crianças e adolescentes.

Na sequência, a advogada Tatiana Coutinho, que iniciou sua fala fazendo uma audiodescrição. Ela comentou sobre os desconfortos produzidos quando se trabalha assessorando as empresas que estão produzindo e comercializando sistemas de reconhecimento facial ou de uso de biometrias no mercado em geral. Mas também alertou sobre a importância deste trabalho e de terem pessoas negras/periféricas fazendo parte desta conversa sobre tecnologias emergentes. apontou a necessidade de se fazer um arranjo político e público da iniciativa privada sobre este tema. Como mulher negra e periférica, decidiu estudar as questões envolvendo as tecnologias emergentes. Impactos das novas tecnologias no dia a dia sobre os corpos pretos e periféricos. Por isso decidiu ser um vetor de fazer um trabalho duplo sobre educação análise de riscos e tentar traduzir para as empresas e seus clientes o real impacto que isso causa.

O uso de dado pessoal para fins de segurança pública que não está sob a égide da LGPD e por conseguinte a ANPED tem o dever - está sob a sua competência - solicitar relatórios e impactos sobre estas parcerias públicos privadas. no entanto, não há notícias de que estes relatórios estejam sendo solicitados. o relatório de impacto é um documento regulatório obrigatório. é por meio dele que se consegue compreender os riscos que este que este tipo de tecnologia traz para a sociedade e olhando para a inovação e o desenvolvimento tecnológico, sugerir ou assumir um compromisso de algumas medidas mitigadoras. segundo ela, a lacuna existente hoje na LGPD é sobre utilizada.

Ela explicou que, ao fazer uso do dado pessoal, as empresas quase sempre, ao invés de pensar em quais outros mecanismos regulatórios basear suas ações, de modo a garantir os direitos fundamentais, acabam optando pelo entendimento de que “já que não tem previsão na LGPD, vamos usar da pior maneira possível”. Para ela, trata-se também de uma questão cultural. Daí porque é preciso apontar quando o uso dos dados é indevido e não está totalmente regulamentado. Endereça-se o risco, mas o outro lado acaba caindo em uma área cinzenta regulatória. E por outro lado, não há muita ajuda do governo, pelo contrário, muitas vezes o próprio Estado é quem vem implementando sistemas tecnológicos de alto risco. Concluiu sua fala afirmando não conseguir enxergar o interesse público que se diz ter em torno desta agenda, visto que o Estado vem também implementando. Ressaltou que parte significativa do fomento para implementação destes sistemas é público, e muitas vezes se dá sem transparência sobre quem é operador e quem é controlador e sem transparência sobre medidas de segurança, etc.

A quarta participação foi de Jéssica Ribeiro Cardoso, da organização C-Partes, que iniciou com sua audiodescrição e na sequência trouxe reflexões a partir de dados sobre segurança pública e tecnologias de vigilância em Rondônia, estado que segundo ela, é novo e territorialmente muito extenso. Por conta disso, é um estado marcado por muitas disputas fundiárias e violências contra ambientalistas e defensores dos direitos humanos, além de desmatamento, crimes ambientais, narcotráfico, e outras questões inerentes a estados que fazem fronteira com outros países. Em seguida informou que o C-Partes lançou em parceria com o Instituto de Referência em Internet e Sociedade (ÍRIS-BH), uma Cartilha para Proteção Digital de Defensores dos Direitos Humanos.

Pensar como sobre os usos das tecnologias de reconhecimento facial afeta juventudes negras, indígenas e periféricas e com isso permanece invisibilidade destes grupos. Segundo ela, o Estado tem focado muito no uso destas tecnologias como força repressiva e não como instrumento de promoção de direitos. Ela citou matéria do *The Intercept* Brasil, que aponta Rondônia como o estado que mais expandiu clubes e tiro dentro da Amazônia Legal. Também no mesmo período houve aumento de políticas de vigilantismo. Em pesquisa produzida pelo Panóptico, o Estado de Rondônia teria informado que não faz uso de tecnologias de reconhecimento facial, mas ao fazerem uma pesquisa rápida nos sites dos órgãos públicos ficou evidente que houve bastante investimento público nos últimos anos em “pacotes de segurança” que fazem o uso deste sistema. Ações desta ordem também foram usadas no carnaval de 2025, com monitoramento em tempo real e existe projeto de lei propondo o uso de videomonitoramento na capital Porto Velho.

Cerca de R\$1,4 milhões foram investidos em infraestrutura tecnológica para virtualização, armazenamento e monitoramento de rede, sem qualquer transparência. Ao

analisar os documentos e atas relacionadas aos investimentos e a estas políticas em desenvolvimento ficou evidenciado que: a) não há transparência sobre onde estes equipamentos estão sendo instalados; b) quais bancos de dados estão sendo alimentados; c) quais os critérios de inclusão de rostos no sistema; e c) não houve consulta pública ou diálogos realizados durante todo este processo. Na sequência apresentou um rol de questões que devem ser defendidas pela comunidade rondoniense: consulta pública, audiências com Ministério Público e Defensoria Pública e relatórios de impactos nos DHs. Além da participação social, destacam: 1) a importância de políticas de fortalecimento da comunicação comunitária (mídias independentes, coletivos de juventude, etc.); 2) levar a inclusão digital crítica, com políticas de educomunicação para periferias e territórios indígenas; e 3) incidência nas políticas públicas, nos conselhos, parlamentos e fóruns.

O mediador Pedro retomou a fala e reforçou que a pauta da vigilância não pode ser secundária na governança da internet e na sequência abriu para as falas ao público.

A primeira contribuição foi feita pela Pietra do Tecnosfera Lab, que fez uma reflexão sobre o uso excessivo de telas por crianças e adolescentes, dialogando com a fala de Júlia Abad, mas também apontou a ausência de espaços públicos nas cidades que possam ser usados e usufruídos por crianças e adolescentes, com parques, quadras esportivas, centros culturais, etc. Outra contribuição veio da vereadora de Natal (RN) Brisa Bracchi que questionou como é possível criar estratégias para combater este discurso sedutor do techno solucionismo, tendo em vista que o uso do reconhecimento facial já está tão presente no dia a dia, citando o uso em condomínios e prédios. Ela informou também sua participação como signatária da campanha “Tire meu rosto da sua mira”. A relatora Ana Mielke, leu alguns comentários feitos pelo chat no Youtube e apresentou a questão posta pelo internauta Thiago Avelino que queria comentários dos palestrantes sobre o projeto de lei 2338, no que diz respeito ao uso de IA na segurança pública. A relatora ainda pontuou a necessidade de mapear os dados das empresas fornecedoras destas tecnologias para o Brasil, uma vez que muitas destas tecnologias são testadas em situações de guerra, como acontece atualmente na ocupação israelense sobre a Faixa de Gaza.

- **Identificação de consensos e dissensos**

O debate apontou para a necessidade de construir uma regulação das tecnologias emergentes que leve em conta a mitigação de riscos no uso de biometria de longa distância, entre elas o reconhecimento facial para fins de segurança pública, especialmente porque já existem estudos e pesquisas que apontam como estas tecnologias de reconhecimento por vez violem direitos das populações mais vulneráveis. Dentre os grupos populacionais que vêm sendo atingidos estão crianças e adolescentes, com reconhecimento facial em escolas e estádios esportivos.

Muitas vezes o debate sobre o uso de reconhecimento facial na segurança pública não ganha relevância no debate mais amplo sobre regulação de plataformas e de IA, porque a ideia de uma solução tecnológica para conter a criminalidade tanto no campo quanto na cidade é muito sedutora. Há grande penetração da ideia de que a vigilância é a única solução possível para a segurança pública. Nesta linha, houve consenso também sobre a necessidade de se debater a própria ideia de segurança pública, visto que hoje ela está associada exclusivamente a aspectos de policiamento, vigilância e punição.

Outro ponto consensual é a educação para o uso destas tecnologias emergentes. antes se falava em educação para a mídia ou educomunicação, hoje este debate se amplia, incluindo também o uso de tecnologias. A educação é essencial para que as populações entendam os riscos e impactos relativos ao uso destas tecnologias e possam se posicionar por maior transparência e políticas de mitigação destes impactos nos usos.

Dentre os desafios apontados está a lacuna legislativa quanto à proteção de dados em sistemas de vigilância e reconhecimento facial para fins de segurança pública. Como a LGPD (Lei 13.709/2018) é omissa quanto a isso, muitas empresas e até mesmo o Estado brasileiro se abstém do uso de outros regulamentos existentes para a garantia dos direitos fundamentais. Neste sentido, é preciso ampliar o debate sobre a necessidade de uma legislação que condense as diretrizes básicas para o uso dos dados para este fim.