Call for input for the HRC62 thematic report on "Impact of digital and AI-assisted surveillance on assembly and association rights, including chilling effects"

Special Rapporteur on freedom of peaceful assembly and of association[1]

Context

The present Call for Input was issued by the *United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association* to inform her upcoming thematic report on the "Impact of digital and AI-assisted surveillance on assembly and association rights, including chilling effects," to be presented at the 62nd session of the Human Rights Council in June 2026. The report seeks to gather contributions from civil society organizations, academic institutions, and other stakeholders to analyze how the rapid expansion of digital surveillance - including AI-powered tools such as facial recognition, predictive analytics, and social media monitoring - is affecting civic space, human rights, and democratic participation around the world. Submissions are expected to provide evidence, examples, and policy recommendations addressing the use, misuse, and governance of such technologies, as well as their direct and indirect impacts on the exercise of public freedoms.

Over the past decade, digital and AI-assisted surveillance has evolved into one of the most pressing threats to civic space and the exercise of the rights to freedom of peaceful assembly and association. The convergence between widespread data collection, predictive analytics, and opaque algorithmic decision-making has expanded the capacity of both State and non-State actors to monitor, categorize, and constrain civic participation. What was once exceptional - targeted digital surveillance of political opponents - has become a normalized infrastructure of control embedded in public security systems, smart cities, and online platforms.

In Latin America, this reality intersects with historical patterns of authoritarianism, racialized policing, and social inequality. The expansion of predictive policing tools, facial recognition technologies, and mobile device monitoring has intensified the exposure of activists, journalists, and human rights defenders to unlawful surveillance. Simultaneously, non-State actors - including private companies, disinformation networks, and even civilian groups - engage in *digital vigilantism*: practices of doxxing, coordinated harassment, and unauthorized data collection targeting vulnerable communities, particularly women, LGBTQIA+ individuals, and racial minorities. These dynamics

[1] These contributions were written by Fernanda Rodrigues and Luiza Correa de Magalhães Dutra, and reviewed by Ana Bárbara Gomes Pereira.

produce a continuous chilling effect, discouraging participation in public demonstrations and online mobilization.

The ongoing securitization of digital policy debates - often under the pretext of combating crime or misinformation - contributes to legitimizing invasive monitoring and undermining encryption and privacy protections. The lack of transparency in the acquisition and deployment of surveillance technologies, combined with insufficient judicial and parliamentary oversight, further undermines trust in institutions and undermines democratic accountability.

Against this backdrop, the **Institute for Research on Internet & Society (IRIS)** contributes to the strengthening of human rights in the digital environment through interdisciplinary research, public policy advocacy, and public engagement.[2] Since its foundation in 2015, IRIS has developed projects that examine the intersection of surveillance, cybersecurity, and civic freedoms in Brazil and across the Global South. The Institute's work has explored the use of spyware and AI technologies by public authorities, analyzed their implications for transparency and due process, and documented gendered and racialized impacts of digital surveillance practices.

Questions

How has digital surveillance affected the rights of association and assembly of people belonging to groups in vulnerable and marginalised situations (such as women, children and youth, indigenous people, afro-descendant communities, LGBTQI+ persons, historically marginalised groups and minorities, etc)

Digital surveillance has profoundly affected the rights of association and peaceful assembly for people in vulnerable and marginalised situations. Extensive academic and policy literature identifies several interrelated mechanisms by which surveillance constrains collective life: (a) information asymmetry and lack of transparency about data collection and processing; (b) "entangled" surveillance ecologies that combine device-level spyware, platform monitoring, facial recognition and administrative databases; (c) inadequate or ill-fitting legal instruments that lag behind technological change and enable disproportionate monitoring; and (d) unequal exposure to surveillance according to existing social markers, which amplifies the vulnerability of racialised, gendered and otherwise marginalised bodies.

In racialised societies, surveillance practices reproduce and deepen structural hierarchies. Predictive analytics, fused administrative datasets and discriminatory policing disproportionately target Black, Indigenous and other racialised groups, raising the threshold of risk for collective mobilization and political organising. Women, girls and gender-diverse people face specific harms from intimate surveillance: commercial spyware and stalkerware - often disguised as legitimate apps - enable abusers and other actors to access private communications and location data, producing direct safety risks and effectively removing safe spaces for organising and mutual support. LGBTQI+ persons risk

[2] This contribution was translated from Portuguese to English with the help of an artificial intelligence system.

being outed through data analysis or platform monitoring and therefore may avoid associations or meetings that are essential for community existence.

The rise of *governmental hacking* - the adoption by state actors of spyware-like investigative tools, covert intrusions and remote exploitation for intelligence or law-enforcement purposes - amplifies these threats in important ways. Recent systematic reviews and policy analyses point to a troubling calculus: even when framed as legitimate investigative techniques, government hacking tools are hard to bound by meaningful necessity and proportionality in practice; they create opportunities for mission creep, abuse and permanent weakening of security infrastructures. The IRIS systematic review documents that the technical complexity and secrecy surrounding these tools, the opacity of procurement and deployment, and weak external oversight generate real risks of state overreach and of a surveillance market that thrives on insecurity - supporting arguments for strict limits or moratoria on the state's adoption of certain intrusive hacking capabilities.

A related flashpoint concerns proposals and laws that would require *rastreabilidade de mensagens instantâneas* (traceability) of instant messages or exceptional-access mechanisms that undermine end-to-end encryption. While traceability is often presented as a tool to investigate crime, the literature shows that these obligations - including backdoors, traceability logs, or forced key escrow mechanisms - conflict with the fundamental security properties of encrypted systems, are technically fraught, and produce broad collateral harms to privacy and to rights-bearing communities. Demands for message traceability risk exposing organisers' metadata and communications to state or private actors, enabling surveillance-based repression, discriminatory targeting, and chilling effects on assembly and association.

Surveillance practices are also increasingly characterised by *data fusion*: video feeds with facial recognition are combined with social-media intelligence, administrative records and commercial data brokers' profiles. This aggregation multiplies the possible revelations about an individual's political associations, sexual orientation, health, or location - transforming ordinary participation in groups or attendance at assemblies into high-risk events for marginalised people. Algorithmic scoring and predictive models may label communities or organisers as "risks," producing selective policing - like the arising of predictive policing - and pre-emptive suppression of assemblies that are led by or beneficial to marginalised groups.

The practical consequences are stark and multi-layered: individuals self-censor or withdraw from civic life; organisers shift to smaller, closed networks that reduce public visibility and political impact; and trust between participants erodes, hampering recruitment and coalition-building. Moreover, when legal frameworks mandate traceability or permit unchecked hacking, the combination of weakened encryption and covert state intrusion removes effective remedies and increases impunity for abuses.

To protect the rights of association and assembly for vulnerable groups, IRIS[3] highlight some urgent measures that are required: prohibitions or moratoria on the state's use of intrusive governmental hacking tools where oversight and technical safeguards are absent; bans or strict regulation of commercial stalkerware; robust protections for end-to-end encryption and rejection of traceability/backdoor schemes that undermine secure communications; mandatory transparency, independent impact assessments (with an intersectional lens) for any surveillance program; enforceable remedies for victims; and sustained investment in community digital-security capacity-building tailored to women, youth, Indigenous, racialised and LGBTQI+ groups. Legislative or policy shifts on traceability and exceptional access must be grounded in public technical reviews, feasibility analyses and broad societal dialogue.

Recommendations: What specific safeguards should be put in place through the lifecycle of deployment of digital surveillance technology to prevent unlawful and arbitrary surveillance, and to mitigate chilling effects on the exercise of the rights to freedom of peaceful assembly and association (online and offline):

If digital surveillance tools, including AI-powered systems, are deployed, what safeguards must be in place to ensure such uses are legitimate and necessary for protection of security or public order; to ensure these are used in a responsible and accountable manner, consistent with human rights and the obligation of facilitating peaceful assembly and association rights, and to prevent chilling effects?

To prevent unlawful and arbitrary surveillance and mitigate chilling effects on the rights to peaceful assembly and association, robust safeguards must govern the entire lifecycle of digital surveillance technologies - including AI-powered systems.
All surveillance activities must be clearly grounded in law, limited to legitimate aims, and subject to the principles of necessity and proportionality, with their use independently supervised and auditable. Prior and periodic human rights impact assessments must be mandatory, transparent, and participatory. Procurement and deployment processes must ensure public accountability, including disclosure of contracts, suppliers, and technical capabilities.

[3] DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo René da Silva; VIEIRA, Victor Barbieri Rodrigues. **Hacking Governamental: uma revisão sistemática.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, fevereiro de 2023. Disponível em: <https://bit.ly/3YdVcIL>. Acesso em: 04.11.2025
ALTO COMISSARIADO DAS NAÇÕES UNIDAS PARA OS DIREITOS HUMANOS. **O direito à privacidade na era digital: relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos (A/HRC/51/17).** Tradução de Luíza Dutra e Paulo René da Silva Santarém. Belo Horizonte: Instituto de Referência em Internet e Sociedade – Projeto Comunicações Privadas, Investigações e Direitos, 2022. Tradução não oficial da ONU.
RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo René da Silva; VIEIRA, Victor Barbieri Rodrigues. **Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2022. Disponível em: <https://bit.ly/3yLlb0P>. Acesso em: 04.11.2025

Technical safeguards must include data minimization, purpose limitation, and the protection of strong end-to-end encryption - with explicit prohibitions on traceability mechanisms, backdoors, client-side scanning, and governmental hacking that compromise communication security.[4]

Specific restrictions are also essential:

- Authorities' access to mobile devices without a judicial warrant must be strictly prohibited, including during stop-and-searches or in cases of alleged in cases of immediate offense;
- When a warrant is issued, access to mobile devices through intrusive surveillance tools must be strictly limited to the authorized scope and period;
- Investigative hacking tools that allow simultaneous access to past and future communications or enable data alteration are unlawful and inadmissible both as evidence and as investigative means.

Regarding AI technologies, the following recommendations are particularly relevant:

- A complete ban on the use of facial recognition technologies for public security;
- Mandatory algorithmic impact assessments throughout the entire lifecycle of the model, particularly before deployment, to evaluate its impact on criminal selectivity, racial inequalities, and fundamental rights such as privacy, personal data protection, and human dignity;
- Adoption of specific measures to mitigate discriminatory biases;
- Ensuring social participation, especially of marginalized groups, in conducting algorithmic impact assessments and in the governance systems surrounding such technologies;
- Classification of AI technologies used for surveillance as *high-risk* at minimum, with the imposition of stricter transparency and governance requirements;
- Continuous obligation for public security officers to review algorithmic inference outcomes;
- Guaranteeing the rights to explanation, adequate justification, review, and contestation for individuals affected by AI-based surveillance technologies;

[4] DUTRA, Luiza Correa de Magalhães; GOMES, Ana Bárbara; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo René da Silva. **Recomendações sobre privacidade das comunicações, investigações e direitos digitais.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, dezembro de 2022. Disponível em: <http://bit.ly/3ViK38I>. Acesso em: 04.11.2025

- Ensuring that the use of AI in public security is accompanied by effective accountability mechanisms - both internal and external - guaranteeing traceability of automated decisions and the possibility of human review;

- Establishment of independent institutions and bodies, with civil society participation, to oversee and audit the use of AI technologies in order to prevent discriminatory biases;

- Definition of clear minimum standards for the collection, storage, sharing, and cross-referencing of data gathered by digital surveillance technologies (such as body cameras, facial recognition, and predictive systems), to prevent secondary uses and strengthen control over information flows.

What type of digital surveillance, spyware, facial recognition and other biometric surveillance tools, and/or AI-assisted mass surveillance have been authorised for use in your country? On what legal grounds and for what purposes were these procured and used?

In Brazil, we have been following a process of expansion in the use of facial recognition systems for public security purposes. Although this type of technology has been in use since at least 2019,[5] the only regulation governing it was published in June 2025. This is Ordinance 961/2025,[6] issued by the Ministry of Justice and Public Security, which establishes guidelines on the use of information technology solutions applied to criminal investigation and public security intelligence activities.

In the case of real-time remote biometric identification systems in publicly accessible spaces, their use is prohibited, but there are five exceptions that basically legalize the practices that have been employed by State Public Security Secretariats. These exceptions are the use of facial recognition for:

> a) criminal investigation or prosecution, subject to prior and reasoned judicial authorization, when there is reasonable evidence of authorship or participation in a criminal offense, the evidence cannot be obtained by other available means, and the fact under investigation does not constitute a criminal offense of lesser offensive potential;
>
> b) searching for victims of crimes, missing persons, or persons in circumstances involving a serious and imminent threat to the life or physical integrity of natural persons;

[5] OLIVEIRA, Caroline. Cerca de 90% das pessoas presas com uso de reconhecimento facial são negras. **Brasil de Fato,** 27 nov. 2019. Disponível em: https://www.brasildefato.com.br/2019/11/27/cerca-de-90-das-pessoas-presas-com-uso-de-reconhecimento-facial-sao-negras/. Acesso em: 3 nov. 2025.

[6] BRASIL. Ministério da Justiça e Segurança Pública. **Portaria MJSP n. 961, de 24 de junho de 2025.** Estabelece diretrizes sobre uso de soluções de tecnologiainformação aplicadas às atividades de investigação crimininteligência de segurança pública. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/portaria-do-mjsp-regulamenta-uso-de-tecnologia-em-investigacoes-criminais-e-inteligencia-de-seguranca-publica/portaria-mjsp-no-961-de-24-de-junho-de-2025-portaria-mjsp-no-961-de-24-de-junho-de-2025-dou-imprensa-nacional.pdf. Acesso em: 5 nov. 2025.

c) flagrant offenses punishable by imprisonment for more than two years, with immediate notification to the judicial authority;

d) recapture of escaped defendants or prisoners; or

e) enforcement of arrest warrants issued by the Judiciary and the measures and penalties provided for in item II of art. 319 of the Code of Criminal Procedure and item IV of art. 47 of the Penal Code.

However, the aforementioned ordinance is significantly lacking in terms of transparency and governance obligations. Specifically in relation to the use of AI technologies, the text only stipulates that it must be used proportionately in criminal investigation and public security intelligence activities, in order to comply with "the duty to prevent risks and the laws applicable to the case." In cases where there is a chance of violating fundamental rights, the agent is only required to review the "result of the algorithmic inference."

Ordinance 961 also establishes that its guidelines must observe values such as the protection of fundamental rights and guarantees, due process, personal data protection, transparency, accountability, and responsibility. Similarly, it provides that one of its objectives is to ensure the "establishment of risk assessment and mitigation mechanisms." However, the rule is vague on this point, limiting itself to defining as obligations for management bodies the "correct, ethical, and responsible use of information technology solutions, promoting training for users and adopting measures to curb the misuse of solutions under their personal responsibility," as well as the "periodic performance of audits and monitoring of the effectiveness of security measures."

In fact, the ordinance does not, at any point, establish more precise and objective rules on how this ethical and responsible use should take place, nor does it provide for the minimum instruments to ensure adequate transparency and supervision. Given the numerous studies that point to the high failure rate of facial recognition systems on black people—who represent more than half of the population and the largest portion of the incarcerated population in Brazil—[7] we believe that its use should not even be allowed in Brazil and should be banned for public security purposes.

If a total ban is not possible, strict safeguards must be adopted to avoid the potential risks of discrimination and violation of other fundamental rights through undue detentions and arrests.[8] In this regard, it is important to note that the National Congress is discussing the development of a regulatory framework for artificial intelligence systems through Bill 2338/2023, based on a risk and rights

[7] LIMA, Thallita. et al. **Vigilância por lentes opacas:** mapeamento da transparência e responsabilização nos projetos de reconhecimento facial no Brasil. Rio de Janeiro: CESeC, 2024; BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. **Proceedings of Machine Learning Research,** Vol. 81, pp. 1–15, 2018.

[8] SILVA, Fernanda dos Santos Rodrigues. A atualização do racismo nas escolhas tecnológicas de segurança pública e preocupações para uma agenda regulatória da IA no Brasil. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara; HOUANG, André (eds.). **Direitos Fundamentais e Processo Penal na Era Digital:** Doutrina e Prática em Debate. Vol. VII. São Paulo. InternetLab, 2024.

approach. However, despite providing that facial recognition systems also constitute excessive risk technologies, the current text points out almost the same exceptions mentioned in Ordinance 961, once again undermining the meaning of the prohibition.

Finally, the most recent initiative in favor of regulating recognition systems is Bill 1828/2023,[9] which was resubmitted this year to the Chamber of Deputies and had its substitute approved on an urgent basis by the Public Security and Organized Crime Combat Commission. In the justification for the opinion, the rapporteur, Deputy Capitão Alden, pointed out that "Crime in Brazil continues to show worrying rates, with direct repercussions on the population's sense of security" and that the new text seeks to "balance security and freedom, efficiency and guarantees, avoiding excesses and ensuring respect for personal data protection legislation and fundamental rights." The substitute bill aims to establish "general rules on the use of facial recognition systems and other automated means of biometric identification in public administration agencies and entities and in essential public services."

Although it includes some safeguards that are not seen in previous documents, such as the prohibition of coercive or restrictive measures based exclusively on automated inference, requiring prior human review, the proposal again lacks specialized reasoning about the benefits of using the technology and is already the target of criticism from civil society organizations.[10] Without the publication of any study supporting the necessity and reasonableness of the tool, without any consultation with society, or even proof that there are no other measures that could be employed in its place, this has been one of the main tools used by the government today. And its damages and risks have been increasing every year, as demonstrated by research[11] and news reports.[12]

[9] BRASIL. Câmara dos Deputados. **Projeto de Lei 1.828, de 2023.** Autoriza a instalação, em todo o território nacional, de câmeras de reconhecimento facial nas estações ferroviárias e rodoviárias, no interior dos vagões das composições, em vias públicas e repartições públicas; e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=3028748&filename=Tramitacao-PL%201828/2023. Acesso em: 5 nov. 2025.

[10] COALIZÃO DIREITOS NA REDE; CAMPANHA TIRE MEU ROSTO DA SUA MIRA. **Nota Pública sobre Projeto de Lei 1828/2023 que autoriza o uso de sistemas de reconhecimento facial em sistemas de transporte público e repartições públicas**. 2 set. 2025. Disponível em: https://direitosnarede.org.br/2025/09/02/nota-publica-sobre-projeto-de-lei-1828-2023-que-autoriza-o-uso-de-sistemas-de-reconhecimento-facial-em-sistemas-de-transporte-publico-e-reparticoes-publicas/.

[11] NUNES, Pablo et al. **Mapeando a vigilância biométrica [livro eletrônico]:** levantamento nacional sobre o uso do reconhecimento facial na segurança pública. Rio de Janeiro: CESeC, 2025

[12] ARAÚJO, Mateus; VESPA, Talyta. Reconhecimento facial de SP confunde idoso com estuprador foragido. **UOL,** 13 abr. 2025. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2025/04/13/reconhecimento-facial-de-sp-confunde-idoso-com-estuprador-foragido.htm; 'MEDO, frustrado e constrangido', diz homem detido por engano em estádio após erro do sistema de reconhecimento facial. **G1 Fantastico,** 21 abr. 2024. Disponível em: https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml; ALENCAR, Itana. Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por 'racismo algorítmico'; inocente ficou preso por 26 dias. **G1 Bahia,** 1 set. 2023. Disponível em: https://g1.globo.com/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoes-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-preso-por-26-dias.ghtml?utm_source=whatsapp&utm_medium=share-bar-mobile&utm_campaign=materias; SANTIAGO, Abinoan. 'Me urinei de medo ao ser

levada no camburão da PM por erro de IA'. **Tilt UOL,** 15 NOV. 2023. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2023/11/15/erro-camera-reconhecimento-facial.htm.