



CELS

Dejusticia

AGORA



**Human
Rights
Law
Centre**



**WRITTEN SUBMISSION FOR THEMATIC REPORT BY UNITED NATIONS SPECIAL RAPPORTEUR
ON THE RIGHTS TO FREEDOM OF PEACEFUL ASSEMBLY AND OF ASSOCIATION
TO BE PRESENTED AT THE 62ND SESSION OF THE UN HUMAN RIGHTS COUNCIL BY
THE INTERNATIONAL NETWORK OF CIVIL LIBERTIES ORGANISATIONS (INCLO)**

Submitted to: The Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association
E-mail: hrc-sr-freeassembly@un.org

Submitted by: International Network of Civil Liberties Organizations (INCLO)
C/O Laura Kauer Garcia and Timilehin Ojo, INCLO
E-mail: lkauer@inclo.net and tojo@inclo.net

Re: Submission to 62nd HRC session report

Visit inclo.net

INTRODUCTION	3
ABOUT INCLO AND ITS RELEVANT PUBLICATIONS	3
HUMAN RIGHTS STANDARDS	5
RESPONSES TO THE UNSRS CALL FOR INPUT FOR 62ND HRC SESSION THEMATIC REPORT	9
Current Legislative Landscape and Chilling Effects	10
<i>Argentina</i>	10
<i>Australia</i>	13
<i>Brazil</i>	14
<i>Egypt</i>	15
<i>Ireland</i>	15
<i>Kenya</i>	17
<i>South Africa</i>	19
Digital AI Assisted Surveillance and Technologies Engaged	22
Facial Recognition Technology (FRT)	24
<i>Argentina</i>	25
<i>Brazil</i>	27
<i>Canada</i>	31
<i>Ireland</i>	32
<i>Kenya</i>	34
<i>Russia</i>	35
<i>South Africa</i>	35
Body Worn Cameras (BWCs), Drones and Closed-Circuit Television (CCTV)	39
<i>Australia</i>	40
<i>Brazil</i>	44
<i>Canada</i>	45
<i>Ireland</i>	46
<i>South Africa</i>	49
Cyber Patrolling/Social Media Monitoring	51
<i>Argentina</i>	52
<i>Canada</i>	54
<i>Colombia</i>	57
<i>Ireland</i>	60
<i>Kenya</i>	60
<i>South Africa</i>	61
Spyware	64
<i>Ireland</i>	65
<i>Kenya</i>	67
Encryption	68
<i>Ireland</i>	68
CONCLUSION AND RECOMMENDATIONS	69

INTRODUCTION

1. This written contribution is submitted to the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association (“UNSR”) by the International Network of Civil Liberties Organisations (“INCLO”) in response to the call for inputs for the report to be presented by the UNSR at the 62nd session of the Human Rights Council. The report aims to shed light on, provide analysis and increase the understanding of how the use of digital surveillance impacts the exercise of the rights to freedom of peaceful assembly and association, and especially the associated chilling effects. This written contribution includes inputs by 10 INCLO member organizations and is endorsed by 12 INCLO members.¹

ABOUT INCLO AND ITS RELEVANT PUBLICATIONS

2. INCLO is a network of 16 independent, national human rights organizations from different countries in the North and South that work together to promote fundamental rights and freedoms by supporting and mutually reinforcing the work of member organizations in their respective countries, and collaborating on a bilateral and multilateral basis. INCLO works through four main pillars: (1) civic space; (2) surveillance and digital rights; (3) equality and equity; and (4) climate and environmental justice. The responses included in this written submission are based on efforts led by INCLO members and their unique knowledge in the domestic contexts within which they operate. Given their areas of expertise, the contributions included in this document focus on illustrative cases of the deepening threats to the rights to freedom of peaceful assembly and association, alongside related compound human rights harms and chilling effects, posed by rapidly expanding digital and Artificial Intelligence (AI)-powered surveillance.²
3. Through its programmatic pillars on Civic Space and on Surveillance and Digital Rights, INCLO is a recognised voice in both regional and international forums. Our rigorous, evidence-based research spans a range of topics, including the intersection of protest and surveillance, the use

¹ The INCLO member organizations who endorsed this submission are: Agora International Human Rights Group (Agora, Russia), the Canadian Civil Liberties Association (CCLA, Canada), Centro de Estudios Legales y Sociales (CELS, Argentina), the Commission for the Disappearances and Victims of Violence (KontraS, Indonesia), Conectas Direitos Humanos (Conectas, Brazil), Dejusticia (Colombia), the Egyptian Initiative for Personal Rights (EIPR, Egypt), the Hungarian Civil Liberties Union (HCLU, Hungary), the Human Rights Law Centre (HRLC, Australia), and the Irish Council for Civil Liberties (ICCL, Ireland), the Kenya Human Rights Commission (KHRC, Kenya), the Legal Resources Centre (LRC, South Africa). Other members include: the American Civil Liberties Union (ACLU, United States), the Association for Civil Rights in Israel (ACRI, Israel), the Human Rights Law Network (HRLN, India), and Liberty (United Kingdom).

²For more in-depth analysis of national contexts: INCLO member CELS submitted an individual submission besides contributing to this one. HCLU prepared a submission on the Hungarian context in collaboration with the Hungarian Helsinki Committee and the Hättér Society and can be found here: <https://hatter.hu/sites/default/files/dokumentum/kiadvany/submission-hs-hclu-hhc-un-sr-on-freefom-of-ppeaceful-assembly-impact-of-digital-and-ai-assisted.pdf>. INCLO member Liberty contributed its own submission based on investigations by its journalism unit Liberty Investigates. For more information, see www.libertyinvestigates.org.uk.

- of digital and AI-enabled technologies in the regulation of public assembly, and the disproportionate impacts of these practices on marginalised groups.
4. In 2019, INCLO published *Spying on Dissent: Surveillance Technologies and Protest*³ which looked at new challenges raised by the expansion of online surveillance technologies used by policing institutions which interfered with the rights to online and offline protest. These technologies are designed or used to watch, intercept, record, retain, analyse and disseminate personal data about protesters – often without their knowledge, their consent, without real and effective oversight and control, and without available legal avenues of recourse. This disrupts and precludes their freedom and ability to organise, gather, dissent and assemble. Case studies from 13 countries demonstrated that the way policing institutions select and deploy online surveillance technologies against protesters often occurs without necessary human rights and democratic safeguards. Both the types of technologies and the lack of safeguards remain a source of concern in the years that have passed since the report was published
 5. In 2022, INCLO, the European Center for Not-for-Profit Law (ECNL) and Privacy International (PI) co-published *Under Surveillance: (Mis)use of Technologies in Emergency Responses – Global Lessons from the Covid-19 Pandemic*⁴ to track the negative impacts of surveillance technology and measures deployed during the Covid-19 pandemic on activist movements and organizations. The report identified 5 trends that parallel concerns shared in the case studies further in this submission:
 - The repurposing of existing security measures
 - The silencing of civil society
 - The risk of abuse of personal data
 - The influential role of private companies
 - The normalization of surveillance beyond the pandemic or other crises
 6. In 2025, INCLO published its *Principles on Law Enforcement Use of Facial Recognition Technology*⁵ to provide a foundation for understanding the risks associated with the police use of FRT and to serve as a tool for assessment and advocacy for those seeking to challenge its use in real-time or retrospectively without their knowledge or consent. The Principles clearly illustrate how FRT, a powerful but flawed technology, impacts citizens' rights and daily lives and can have a disproportionate impact on certain communities -especially people of colour - as it has been known to misidentify people for crimes that they did not commit.

³ International Network of Civil Liberties Organizations (INCLO), *Spying on Dissent: Surveillance Technologies and Protest* (Report, 1 June 2019)

<https://inclo.net/publications/spying-on-dissent-surveillance-technologies-and-protest/>

⁴ European Center for Not-for-Profit Law (ECNL), International Network of Civil Liberties Organisations (INCLO) & Privacy International (PI), *Under Surveillance: (Mis)use of Technologies in Emergency Responses – Global Lessons from the Covid-19 Pandemic* (Report, 14 December 2022)

<https://privacyinternational.org/report/5003/under-surveillance-misuse-technologies-emergency-response-s-global-lessons-covid-19>

⁵ INCLO, *Principles on Law Enforcement Use of Facial Recognition Technology* (INCLO, 2025)

<https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/>

7. In August 2025, INCLLO submitted its *Position Paper on the Human Rights Impacts of Using Artificial Intelligence in Countering Terrorism*⁶ to the UN Special Rapporteur on Counter-Terrorism and Human Rights. The submission by 11 INCLLO members addresses the human rights implications of AI in countering terrorism, particularly where biometric surveillance tools like FRT are deployed. The submission outlines key risks, safeguards, and recommendations rooted in INCLLO's commitment to rights-based technology governance.

HUMAN RIGHTS STANDARDS

8. The approach law enforcement institutions take to select and deploy online surveillance technologies against protesters occurs many times without necessary human rights and democratic safeguards. Their purchase, development and deployment is often not accompanied with a defined legal and human rights framework specifying when and how these tools can be used, their limits and the steps governments will take to ensure the protection and full enjoyment of fundamental freedoms and individual rights.⁷ We consider some of the most prominent rights that can be impacted through this approach and that will be further referenced in the illustrative cases included in this submission.

Right to freedom of peaceful assembly and association

9. The right to freedom of peaceful assembly is a fundamental human right protected under international law, allowing individuals and groups to gather publicly or privately to express opinions, protest, celebrate, or advocate for causes without interference from the state, so long as the assembly is peaceful.⁸ The ability to publicly express beliefs and opinions, and to associate is essential to democracy.⁹ Protests¹⁰ are a central tool of public expression and

⁶ *Position Paper on the Human Rights Impacts of Using Artificial Intelligence in Countering Terrorism* to the UN Special Rapporteur on Counter-Terrorism and Human Rights, (2025) https://inclo.net/wp-content/uploads/2025/09/INCLLO_Input-UN_-_Position-Paper-on-the-Human-Rights-Impacts-of-Using-Artificial-Intelligence-in-Countering-Terrorism.pdf;

⁷ International Network of Civil Liberties Organisations (INCLLO), *Spying on Dissent: Surveillance Technologies and Protest* (June 2019) <https://inclo.net/publications/spying-on-dissent-surveillance-technologies-and-protest/> accessed 11 November 2025.

⁸ United Nations Human Rights Committee, General Comment No. 37 on the right of peaceful assembly (Article 21 of the International Covenant on Civil and Political Rights), CCPR/C/GC/37 (17 September 2020), para. 1; and General Comment No. 25 on participation in public affairs and the right of association (Article 25 of the Covenant), CCPR/C/21/Rev.1/Add.7 (12 July 1996), para. 26

⁹ For more information about the rights attached to protest see INCLLO's 2018 report *Defending Dissent*, available at: <https://www.inclo.net/pdf/Defending-Dissent-Report-Complete-WEB-FINAL.pdf>

¹⁰ INCLLO's use of the term 'protest' follows that of the Joint Report of the Special Rapporteur together with the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions on the Proper Management of Assemblies: A protest is 'an intentional and temporary gathering in a private or public space for a specific purpose, and can take the form of demonstrations, meetings, strikes, processions, rallies or sit-ins with the purpose of voicing grievances and aspirations or facilitating celebrations.' See UN Doc. A/HRC/31/66 (4 February 2016), para. 10.

engagement, often serving as the only avenue for advocacy seeking political, social or economic reforms. Despite the importance of protest to a free society, many states have failed to adequately protect protest and public speech. In fact, policing institutions overwhelmingly treat protests as security threats that should be discouraged even before they occur and suppressed.

10. According to the European Court on Human Rights, “the right to freedom of peaceful assembly is a fundamental right in a democratic society and, like the right to freedom of expression, is one of the foundations of such a society. Thus, it should not be interpreted restrictively.”¹¹ This principle underscores that the freedom to assemble peacefully is not merely a peripheral liberty, but the hallmark of a democratic society. Surveillance does not only restrict freedom of assembly but also erodes trust within civil society.
11. Although protest rights are traditionally understood in the context of physical gatherings, human rights protections must equally extend to ‘analogous interactions taking place online’.¹² In the digital age, the rapid expansion of surveillance technologies, such as facial recognition, biometric data collection, location tracking, drones, spyware, bodyworn cameras, phone metadata and online monitoring, poses a growing threat to the exercise of the rights to freedom of peaceful assembly and association under international law.¹³ These tools are increasingly used by policing institutions to watch, intercept, record, retain, analyse, and disseminate personal data about protesters, often without their knowledge, consent, effective oversight, or access to legal recourse. Such practices enable states to identify, track, and intimidate participants in assemblies, thereby discouraging individuals from organizing or taking part in protests and creating a “chilling effect” on civic engagement.¹⁴

Right to Privacy

12. Privacy is recognised in our digital age as essential for the realization of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association.¹⁵ However, despite these protective frameworks, it is increasingly understood that ‘privacy is no longer a social norm’.¹⁶ Technological advancements allow

¹¹ European Court of Human Rights, Guide on Article 11 of the European Convention on Human Rights: Freedom of assembly and association (updated 31 August 2024) https://ks.echr.coe.int/documents/d/echr-ks/guide_art_11_eng accessed 2 November 2025.

¹² Joint Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association and the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions on the Proper Management of Assemblies, UN Doc. A/HRC/31/66 (4 February 2016), para. 10.

¹³ United Nations General Assembly, International Covenant on Civil and Political Rights, adopted 16 December 1966, entered into force 23 March 1976, 999 U.N.T.S. 171, Articles 21–22.

¹⁴ UN Human Rights Council, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, A/HRC/41/41, 17 May 2019, paragraph 28.

¹⁵ United Nations General Assembly (2014) The Right to Privacy in the Digital Age, A/RES/68/167 United Nations, Human Rights Council Resolution 28/16

¹⁶ Bobbie Johnson, ‘Privacy no longer a social norm, says Facebook founder’ Guardian (London, 11 January 2010) accessed 3 October 2018

processing of large amounts of personal data, often without the subject's awareness or consent.¹⁷

13. The use of surveillance tools to monitor or seek to identify people who are freely gathering, attending a protest in a public space or congregating in a place of worship, could potentially reveal the political leanings of individuals and/or their religious beliefs. Even if police were seeking to find a specific individual at a protest whom they have included on a watchlist via a legal mechanism, some surveillance tools could result in every person attending the demonstration – the majority of whom would be of no interest to police – having their biometric data processed, and possibly stored, without their knowledge, active involvement or consent. Such surveillance practice severely affects people's reasonable expectation of being anonymous in a public space, and could result in a chilling effect on citizens' ability or decision to gather, express their opinions, freely exchange information and engage in behaviour that is necessary and vital for a healthy democracy, thereby impairing political participation.¹⁸
14. Protective human rights instruments have been slow to catch up on interrelated privacy and data protection matters. For example, the UN Human Rights Committee General Comment No 16¹⁹ ensures that privacy, under Article 17 of the ICCPR, has taken on enormous new significance since the committee published the comment in 1988.²⁰ INCLLO colleagues previously submitted to the OHCHR input on privacy challenges in the digital age.²¹ Here, we again, reiterate INCLLO members' recommendation²² that the Human Rights Committee issue a new comment on Article 17 as a revision is now, more than ever, urgently needed in our growing digital age.²³
15. We note the General Assembly's resolution 69/166 of December 2014 concerning the right to privacy in the digital age, resolution 70/184 of December 2015 on technology for development, and resolution 70/125 of December 2015 containing the outcome document of the high-level meeting on the overall review of the implementation of the outcomes of the

¹⁷ B. van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in Serge Gutwirth/Ronald Leenes/Paul De Hert (ed), *Data Protection on the Move* (Springer 2016) 411

¹⁸ Murray, D et al., "The Chilling Effect of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe", *Journal of Human Rights Practice*, Volume 16, Issue 1, February 2024, pp. 397–412, <https://doi.org/10.1093/jhuman/huad020>.

¹⁹ UN Human Rights Committee General Comment No 16, 'Article 17 (Right to Privacy)' (8 April 1988) UN Doc HRI/GEN/1/Rev.9 (Vol. I)

²⁰ Jamil Dakwar, Elizabeth Farries, Brenda McPhail, Tsanga Mkumba, The right to privacy in the digital age, Human Rights Council adopted resolution 34/7, 2018, INCLLO, <https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/INCLLO.pdf>

²¹ *ibid*

²² Irish Council for Civil Liberties and International Network of Civil Liberties Organizations, *Right to Privacy in the Digital Age, HRC 48/4* (2022)

https://www.iccl.ie/wp-content/uploads/2024/02/FINAL_-Right-to-privacy-in-the-digital-age-HRC-48_4-1.pdf accessed 3 November 2025.

²³ *ibid*.

World Summit on the Information Society. We further note that the General Assembly reaffirmed the content of these resolutions in resolution 75/176 of December 2020 on the right to privacy in the digital age and resolution 75/202 of December 2020 on technology for development.²⁴

Right to Protection of Personal Data

16. Everyone has the right to the protection of their personal data. Police use of intrusive technologies for surveillance purposes can pose significant risks to data protection rights as it involves processing sensitive personal data, and can lead to discriminatory and biased outcomes for individuals. It also raises questions concerning consent.²⁵ Just because a person is aware they have been photographed or recorded by CCTV or drones in a public space does not mean that they have agreed to make their biometric data public and/or consented to this data being extracted from an image, processed to create a biometric template, and stored or used for identification purposes by law enforcement.
17. Different states have varied, and in some cases no legal safeguards for the retrieval of biometric data and the use, retention and/or destruction of the same. The interference with the right to protection of personal data would be heightened considerably if a person is subjected to any manner of “profiling” or automated processing. Such processing might see a person’s biometric data used to evaluate certain of their personal aspects and/or to analyse or erroneously predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.²⁶

Right to Equality and Non-Discrimination

18. Everyone is equal before the law and entitled without any discrimination to equal protection of the law.²⁷ When surveillance technologies are used to identify, monitor, or profile individuals, systems built on different algorithms, datasets, and operational conditions can exhibit varying levels of accuracy and reliability. However, while performance and error rates may differ across contexts, these inaccuracies do not affect all people equally, some

²⁴ Egyptian Initiative for Personal Rights, *Virtual Freedom: Towards Ending the Cybercrime Law’s Repression of Online Freedom of Expression in Egypt* (EIPR, August 2025) https://eipr.org/sites/default/files/reports/pdf/towards_ending_the_cybercrime_laws_repression_of_online_freedom_of_expression_in_egypt.pdf accessed 14 November 2025.

²⁵ International Network of Civil Liberties Organizations, *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition – Principles to Reduce the Human Rights Harms of Facial Recognition Technology* (March 2024) <https://inco.net/wp-content/uploads/2024/03/INCLLO-FRT-Principles-Final.pdf> accessed 3 November 2025.

²⁶ International Network of Civil Liberties Organizations, *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition – Principles to Reduce the Human Rights Harms of Facial Recognition Technology* (March 2024) <https://inco.net/wp-content/uploads/2024/03/INCLLO-FRT-Principles-Final.pdf> accessed 3 November 2025.

²⁷ Article 7, Universal Declaration of Human Rights, <https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf>

individuals and groups are far more likely to experience adverse or discriminatory outcomes than others.²⁸

19. For marginalized communities, such as informal workers, LGBTQ+ activists, and student organisers, surveillance reinforces existing social vulnerabilities and exposes them to heightened risks of violence and discrimination. Movements that once relied on digital tools for mobilisation now operate under constant threat, undermining the spontaneity and inclusiveness essential to democratic participation.

RESPONSES TO THE UNSR ON THE RIGHTS TO FREEDOM OF PEACEFUL ASSEMBLY AND OF ASSOCIATION'S CALL FOR INPUT FOR THEMATIC REPORT TO BE PRESENTED AT THE 62ND SESSION OF THE HUMAN RIGHTS COUNCIL

20. Concerns about the rapid expanding use of digital technologies and Artificial Intelligence (AI)-powered surveillance are not entirely new. As highlighted in *Under Surveillance: (Mis)use of Technologies in Emergency Responses – Global Lessons from the Covid-19 Pandemic* (ECNL, INCLC, and Privacy International, 2022),²⁹ the Covid-19 pandemic revealed a global trend of repurposing security and law-enforcement technologies, increasingly enhanced by artificial intelligence, for public health surveillance.
21. This is usually the case, where tools originally developed for one purpose, such as facial recognition, mobile phone location tracking, and data-fusion platforms for counter-terrorism and policing are adapted for other purposes such as contact tracing, quarantine enforcement, and population monitoring. In this case, AI-driven analytics, predictive modelling, and automated decision-making systems were employed to identify “high-risk” individuals or areas, often with limited transparency or accountability.
22. The deployment of AI-assisted tools without clear legal frameworks, human-rights impact assessments, or sunset clauses has contributed to the normalisation of intrusive surveillance and created a precedent for the expansion of digital and algorithmic monitoring beyond emergency contexts. These experiences underscore the urgent need for robust safeguards to ensure that AI-enabled surveillance remains lawful, necessary, proportionate, and strictly time-bound.

²⁸ International Network of Civil Liberties Organizations, *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition – Principles to Reduce the Human Rights Harms of Facial Recognition Technology* (March 2024) <https://inco.net/wp-content/uploads/2024/03/INCLC-FRT-Principles-Final.pdf> accessed 3 November 2025.

²⁹ European Centre for Not-for-Profit Law (ECNL), International Network of Civil Liberties Organisations (INCLC) & Privacy International (PI), *Under Surveillance: (Mis)use of Technologies in Emergency Responses – Global Lessons from the COVID-19 Pandemic* (14 December 2022) <https://privacyinternational.org/sites/default/files/2022-12/ECNL%2C%20INCLC%2C%20PI-COVID-19-Report-Final.pdf> accessed 10 November 2025

Current Legislative Landscape and Chilling Effects

23. AI and surveillance technologies are rapidly being deployed without adequate safeguards, disproportionately affecting marginalized groups, activists, and those engaging in contentious issues. Existing legislative frameworks often fail to address risks associated with bulk surveillance, bias, and errors in AI systems. Across these contexts, the expansion of surveillance creates a chilling effect on freedom of expression, assembly, and civic participation, undermining fundamental democratic rights.

Argentina

24. In recent years, Argentina has recorded the enactment of norms of different legal ranks that authorize the use of various technologies that could be used to monitor protesters and social movements. Due to the lack of precision and safeguards in these norms, and based on the declarations of government officials and the priorities of political agendas, these regulations could result in threats to the rights of association, assembly, and freedom of expression. A common point among the different regulations presented below is that none of them were debated in the legislative sphere. In all cases, they refer to unilateral decisions by the Executive Branch and, in some instances, even exceed the powers of this branch of government.

25. In 2024, President Javier Milei issued Decree 614/2024, which introduced significant reforms to the National Intelligence Law (Law 25.520).³⁰ Under the Decree, Argentina's intelligence agencies are allowed to collect a broad set of information from the public. For example, the definition of "national intelligence" in the law was expanded to include not only "National Defense" and "the internal security of the Nation," but also anything that falls under the vague concept of "opportunities for achieving the strategic interests of the Nation" (Decree Art. 6). The Decree also created the Federal Cybersecurity Agency (AFC) within the intelligence system. This body has an extremely broad mandate. According to the Decree, its function is to "[p]rovide intelligence services through technical, computer, signals, radio spectrum telecommunications, and cybersecurity means, through the acquisition, interception, collection, processing, evaluation, and analysis of all information relevant to the National Intelligence System" (Decree Art. 17). No criteria is provided to determine what is relevant. The specific technologies that are being used by the AFC remain unverified.

26. The modifications introduced by the Decree are in tension with important protections set out in the Intelligence Law. Article 18 of Law 25.520 stipulates that "when it is necessary to carry out interceptions or captures of private communications of any kind in the development of intelligence or counterintelligence activities, the Intelligence Secretariat must request the pertinent judicial authorization." The same article also establishes that "such authorization must be made in writing and be well-founded, precisely indicating the telephone number or

³⁰ Argentina, National Executive Branch, Decree of Necessity and Urgency No. 614/2024, "National Intelligence System" (DNU-2024-614-APN-PTE), July 15, 2024, published in the Official Gazette of the Argentine Republic, First Section, July 16, 2024. Available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/310495/20240716>

numbers or electronic or any other means' addresses whose communications are intended to be intercepted or captured." Likewise, the law restricts intelligence agencies from collecting information "solely on the basis of race, religious belief, private actions, or political opinion, or adherence to or membership in party, social, union, community, cooperative, welfare, cultural, or labor organizations..." (Art. 4). With respect to both of these requirements, there are concerns that the lack of detail or criteria with respect to AFC's collection of "all relevant information" may lead to mass intelligence collection without prior judicial approval and facilitate the collection of intelligence information for illicit purposes.

27. Moreover, there are limited safeguards to ensure compliance with these provisions. Judicial proceedings to authorize the interception of communications are secret. And while Argentina has a control body for intelligence in the National Congress, the Bicameral Commission for the Oversight of Intelligence Agencies and Activities, a large part of its work is also confidential. Although the Commission has broad powers to supervise intelligence agencies, the party that holds the majority of seats in Congress usually defines its internal composition, so the effectiveness of oversight often depends on the political will of the legislators.³¹
28. In May 2025, the National Intelligence Plan (PIN), a secret document that establishes the yearly guidelines for the Intelligence System to promote Argentina's strategic interests, was leaked to the press. Only the President, the Intelligence Secretariat, and the Permanent Bicameral Commission for the Oversight of Intelligence Agencies of the National Congress have access to this document. According to information reported in the press, the PIN directed that intelligence be collected on anyone who might: erode public confidence in government officials, generate a loss of confidence in the government's economic policies, "manipulate public opinion during electoral processes," or "spread disinformation."³²
29. Although the Milei administration maintains that it is "the first government in decades to have made the political decision not to use the [intelligence agencies] to persecute opponents, journalists, or political adversaries,"³³ the PIN is clearly oriented toward those types of activities. In fact, the journalist who exposed the document was immediately targeted: they received threats and hacking attempts on their WhatsApp and X accounts.³⁴

³¹ Iván Poczynok, "Política y servicios de inteligencia: Hoja de ruta para un sistema legítimo y efectivo" (Buenos Aires: Fundar, agosto de 2023), available at: https://fundar.ar/wp-content/uploads/2023/07/Fundar_Politica_y_servicios_de_inteligencia.pdf.

³² Hugo Alconada Mon, "La SIDE pone la mira en quienes 'manipulen la opinión pública' o erosionen la confianza en los funcionarios," *La Nación*, 25 de mayo de 2025. Disponible en: <https://www.lanacion.com.ar/politica/la-side-pone-la-mira-en-quienes-manipulen-la-opinion-publica-o-erosionen-la-confianza-en-los-nid25052025/>

³³ Argentina, Presidency of the Nation, Office of the President, "Official Comunicado No. 101," May 25, 2025. Available at: <https://www.argentina.gob.ar/noticias/comunicado-oficial-numero-101>

³⁴ "El periodista Hugo Alconada Mon fue amenazado e intentaron hackearle sus cuentas luego de su revelación sobre la SIDE," *La Nación*, 27 July 2025, available at: <https://www.lanacion.com.ar/politica/el-periodista-hugo-alconada-mon-fue-amenazado-e-intentaron-hackearle-sus-cuentas-luego-de-su-nid26052025/>.

30. The increase in the State's surveillance capabilities should be a cause for concern. While it is difficult to specify exactly how these technologies are being implemented at this early stage, leaks to the press have shown that Argentina's intelligence services have been monitoring political opponents in line with the directives of the aforementioned National Intelligence Plan. In a leaked report titled "Anticipated Events 09JUL25," the Argentine National Security Agency provided details about union protests, street mobilizations, and meetings of opposition leaders ahead of the provincial elections in the province of Buenos Aires in early September.³⁵ The report included sensitive information that would be difficult to obtain from open sources, including details of a meeting of opposition leaders at one of their homes.³⁶
31. With respect to artificial intelligence, the National Ministry of Security also issued Resolution 710/2024, which creates the Applied Artificial Intelligence to Security Unit (UIAAS) and deepens the artificial intelligence capabilities developed in Resolution 428/2024.³⁷ This entity's specific mission is to prevent, detect, investigate, and prosecute law violations through the use of artificial intelligence.
32. The activities assigned to this body suggest few limits on the state's implementation of AI technologies. The resolution mentions the patrolling of publicly accessible internet pages, which is provided for in Resolution 428/2024, but also lists, for example, real-time facial recognition in security cameras, the use of historical crime data to predict and prevent future crimes, the processing of large volumes of data to create profiles of suspicious persons, and the use of drones for aerial surveillance (Art. 4).
33. Upon filing information requests regarding various aspects of the Resolution, the Ministry provided few details. For example, this artificial intelligence unit is tasked with using machine learning algorithms to analyze historical crime data in order to predict future crimes and help prevent them. This is especially dangerous considering that automated systems can have biases that disproportionately impact minorities and other vulnerable populations. The Ministry was asked whether international standards were consulted in forming this Resolution, such as the European Union AI Act. In response, the Ministry simply replied that a thorough analysis of national and comparative legislation was carried out; and that "AI will not make decisions per se, but will be one more tool that agents will have."
34. Likewise, CELS questioned what methods or technologies would be used for the identification and comparison of images on physical and digital media. Questions were also asked about the

³⁵ Hugo Alconada Mon, "La SIDE redacta informes sobre las actividades políticas de la oposición, sindicatos y grupos de jubilados," *La Nación* (Buenos Aires), 28 July 2025, available at: <https://www.lanacion.com.ar/politica/la-side-redacta-informes-sobre-las-actividades-politicas-de-la-oposicion-sindicatos-y-grupos-de-nid28072025/>.

³⁶ Colectivo Editorial Crisis, "Controlar al pueblo para entregar la patria," *Crisis | Informes*, 13 de junio de 2025. Available at: <https://informes.revistacrisis.com.ar/controlar-al-pueblo-para-entregar-la-patria/>.

³⁷ Ministry of Security, Resolution No. 710/2024, "Creating the Applied Artificial Intelligence to Security Unit (UIAAS)," Buenos Aires, July 26, 2024; published in the Official Gazette of the Argentine Republic, First Section, July 29, 2024. Available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/311381/20240729>

images captured, their safeguarding, and how long they will be stored. The Ministry merely indicated that they were working on the construction of the tools and regulations. Further request was made for clarification of various terms used in the resolutions ("open social networks," "Dark Web," among others) the Ministry responded that it "is working on the construction of complementary tools and regulations that account for what is said here" and that "strict adherence to current constitutional norms is ensured."

35. The lack of information about the technologies to be used and the controls for their use reveals a worrying opacity regarding the implementation of various surveillance systems. This situation becomes even riskier in a context where social protest is considered a crime by the government. Network surveillance can be used to discipline political dissent, which negatively affects the right to freedom of expression in the digital environment. Furthermore, there is a certain risk that these network and platform monitoring tasks will be oriented toward producing information and eventually criminalizing expressions of political dissent.

Australia

36. Similar to other countries, peaceful assembly has been essential to advancing justice and fairness in Australia. However, there are growing threats to the ability of people in Melbourne to assemble freely. The Victorian State Government has proposed to ban the use of facial coverings at public protests,³⁸ while the Council of the City of Melbourne is moving to significantly expand its CCTV network across the municipality.³⁹
37. The proposed expansion of surveillance in Melbourne and the Victorian Government's plan to ban facial coverings at protests have not yet taken effect. However, the potential consequences for freedom of assembly are clear. The risks must also be understood in the broader context of Victoria's legislative environment. In the past twenty-one years, seven anti-protest laws have been introduced into the Victorian Parliament, with six passing into law.⁴⁰ These laws have increased penalties, expanded police powers, and created new offences that directly target protest activity. The steady accumulation of restrictions has already narrowed civic space and made people more cautious about participating in assemblies.

³⁸ Jacinta Allan, 'Strong Action to Fight Hate and Help Victoria Heal' (Media Release, 17 December 2024)

<https://www.premier.vic.gov.au/strong-action-fight-hate-and-help-victoria-heal>

³⁹ Nate Woodall, "City of Melbourne set to vote on security camera overhaul, surveillance powers for staff", ABC News (8 October 2025)

<https://www.abc.net.au/news/2025-10-08/melbourne-city-council-cctv-security-network-proposed-expansion/105864992>; City of Melbourne, "Safe City Camera Program" (2025)

<https://participate.melbourne.vic.gov.au/safe-city-cameras>

⁴⁰ David Mejia-Canales, *Protest in Peril: Human Rights and Democracy at Risk* (Report, Human Rights Law Centre, 2 June 2024) <https://www.hrlc.org.au/app/uploads/2025/04/2407-Protest-in-Peril-Report.pdf>; *Safer Protest with a Registration System and a Ban on Face Coverings Bill 2025* (Vic).

38. The combination of these legislative measures with expanded digital surveillance would significantly deepen the chilling effect, weakening Melbourne’s historic role as a focal point for civic engagement and political expression.

Brazil

39. In early December 2024, the Brazilian Federal Senate approved Bill 2338/2023, which regulates the use of artificial intelligence in Brazil. The proposal, which the Chamber of Deputies is now considering, provides remote, real-time biometric identification in public spaces for public safety purposes - it enters as an exception to the systems believed to be of “excessive risk” and, therefore, without even being linked to the governance system established for those classified as “high risk”.⁴¹
40. Conectas consider part of this bill problematic, as this use in Brazil and other parts of the world has raised ethical and human rights concerns, as demonstrated above. In addition to its potential as a significant violation of the right to privacy, varying lighting conditions, angles, and image quality suggest that the accuracy of these systems may decrease. This point raises concerns about reliability and errors when technology is used for public safety policies. Evidence also shows that these systems perpetuate discriminatory biases — leading to racial profiling — reproducing discrimination and deepening social inequalities. Their use, therefore, can promote mass surveillance and put the right to defense at risk.
41. While the legislative debate progresses, the unregulated use of facial recognition continues to negatively impact the lives of Brazilian citizens, especially in public streets, subways, stadiums, schools, and cultural events. There is a clear need to advocate for public policies that prioritize transparency, responsible governance, and the protection of human rights, including the implementation of independent oversight mechanisms and the creation of a solid legal framework to prevent the abusive use of these technologies.
42. Regarding the use of information technology in criminal investigation and intelligence activities, on June 24, 2025, the Ministry of Justice and Public Security (MJSP) published Ordinance No. 961/2025⁴², which establishes guidelines applicable to federal public security agencies and initiatives involving resources from the National Public Security Fund (FNPS) and the National Penitentiary Fund (FUNPEN). The text, however, should be considered only a first step toward regulation, as it replicates the bill’s shortcomings. On the other hand, it advances by establishing governance and transparency parameters for using these systems in the country’s public security sector—by providing for human review of decisions, for example.

⁴¹ Bill 2338/2023 was approved by the Federal Senate in December 2024. The text now moves to the Chamber of Deputies. For approval, it will need to secure the vote of the majority of deputies.

⁴² Available at:

<https://www.gov.br/mj/pt-br/assuntos/noticias/portaria-do-mjsp-regulamenta-uso-de-tecnologia-e-m-investigacoes-criminais-e-inteligencia-de-seguranca-publica>

Egypt

43. In Egypt, legislative, judicial, and security restrictions on digital expression have expanded in Egypt over the past dozen years, giving government tools for surveilling and then prosecuting certain forms of expression shared online, criminalizing a range of acts that were previously legal.⁴³ This is part of a broader pattern where the Egyptian government has developed restrictions to various forms of expression if they find their way online, by both illegally blocking numerous websites and arresting citizens who have published content deemed by the security services to violate the Constitution and law.
44. The Anti-Terrorism Law No. 94 of 2015, the Press and Media Regulation Law of 2018 and the Cybercrime Law of 2018 have all crystallized and made explicit Egypt's ruling elite vision of the internet as a threat and paved the way for using all punitive means and tools for controlling online expression and limiting freedom of expression in general. The law's ambiguity in defining the grounds for restricting freedom of expression has led to similar ambiguity in determining the acts to be criminalized and their intent, therefore creating an environment ripe for self-censorship and chilling of activism, for fear of persecution.
45. One example of this reality in actions is how the Public Prosecution has introduced a new form of social media censorship by establishing an "electronic monitoring unit" to surveil such crimes in real time. It has increased the number of charges it levels using crimes based on old, largely unutilized legislative articles, either from the Penal Code (such as articles 80 (d), 102 (bis), and 188 criminalizing various modes of spreading false news, and article 306 (bis a) criminalizing certain forms of defamation and slander) or the Telecommunications Regulation Law No. 10 of 2003 (especially article 76, which criminalizes "deliberately causing a nuisance using social media").
46. As the scope of criminal acts has widened, the circle of those targeted by the security and judicial authorities has broadened to include members of legally recognized political parties, those accused of terrorism or joining illegally established groups, journalists, media professionals, opinion writers, visual content creators, and users of private social media accounts who are not known for any activity in the public domain.

Ireland

47. The *Garda Síochána (Recording Devices Act) 2023*,⁴⁴ which was signed into law in December 2023, provides for an array of recording devices and measures. Under the Act, a 'recording device' is very broadly defined as any "device or system that is capable of creating a record in any medium from which visual images (including moving visual images) or sounds, or both,

⁴³ EIPR, 'Virtual Freedom: Towards Ending the Cybercrime Law's Repression of Online Freedom of Expression in Egypt' (August 2025) Available at : [towards_ending_the_cybercrime_laws_repression_of_online_freedom_of_expression_in_egypt.pdf](#) accessed 13 November 2025.

⁴⁴ Garda Síochána (Recording Devices) Act 2023, <https://www.irishstatutebook.ie/eli/2023/act/32/enacted/en/html>

may, by any means, be reproduced”.⁴⁵ The broadness of this definition, against the backdrop of rapidly evolving technology, concerns ICCL and it is ICCL’s position that, in the interests of democracy and transparency, the technologies the police use to surveil or monitor us must be known. During the drafting of the legislation, ICCL called for an amendment to ensure that all types of recording devices or systems used by An Garda Síochána are, at the very least, specified in a relevant code of practice; and/or for the insertion of a new section in the legislation requiring the online publication of a rolling list of all devices approved for usage under this legislation, two months prior to their introduction.⁴⁶ However, this amendment was unfortunately not accepted.

48. Despite the broadness of the definition of “recording device”, the Act does explicitly provide for the use of body-worn cameras and drones (both recognised as ‘recording devices’ in the Act); the tracking of vehicles via Automatic Number Plate Recognition (ANPR); searching databases of retained ANPR data; and live-feed access to third-party CCTV, which could entail a private retail outlet, stadium or venue.⁴⁷

49. While primary legislation for these tools and measures, via the 2023 Act, is in place, each measure requires a detailed Code of Practice in respect of their use. At the time of writing, only a Code of Practice for body-worn cameras is in place⁴⁸ while a pilot scheme for Garda use of body-worn cameras is under way.⁴⁹ As such it remains to be seen what specific safeguards and oversight mechanisms will be in place when it comes to Garda use of many of these tools.

50. The legislation provides that Gardaí can use these tools and measures for several purposes, including securing public order and, as such, will have an impact on people’s right to protest. During the legislative passing of the Act, ICCL put forward a proposal that the bill be amended to say that these tools could only be used to secure public order “where there are reasonable grounds to believe there is a significant threat”,⁵⁰ as a means to safeguard against any potential

⁴⁵ Section 2, Garda Síochána (Recording Devices) Act 2023, <https://www.irishstatutebook.ie/eli/2023/act/32/enacted/en/print#sec2>

⁴⁶ ICCL and Digital Rights Submission, [ICCL-DRI-Recording-Devices-bill-amendments-July-2023.pdf](https://www.iccl.ie/wp-content/uploads/2023/07/ICCL-DRI-Recording-Devices-bill-amendments-July-2023.pdf), July 2023.

⁴⁷ Garda Síochána (Recording Devices) Act 2023, <https://www.irishstatutebook.ie/eli/2023/act/32/enacted/en/html>

⁴⁸ Garda Síochána (Recording Devices) Act 2023 (Code of Practice) Order 2024, <https://www.irishstatutebook.ie/eli/2024/si/216/made/en/pdf>

⁴⁹ An Garda Síochána Pilot phase of Body Worn Cameras for frontline members of An Garda Síochána has commenced - Friday, 31st May 2024, <https://www.garda.ie/en/about-us/our-departments/office-of-corporate-communications/press-releases/2024/may/pilot-phase-of-body-worn-cameras-for-frontline-members-of-an-garda-siochana-has-commenced-friday-31st-may-2024.html>

⁵⁰ ICCL and Digital Rights Ireland proposed amendments to the Garda Síochána (Recording Devices) Bill 2022, July 2023, page 2, <https://www.iccl.ie/wp-content/uploads/2023/07/ICCL-DRI-Recording-Devices-bill-amendments-July-2023.pdf>

chilling effect on the right to protest, but this suggested amendment was unfortunately not accepted.

51. Instead, the main safeguards in the primary legislation in relation to the use of ‘recording devices’, notwithstanding any reliance on any as-yet-unwritten codes of practice⁵¹ to protect against unnecessary, arbitrary and unlawful surveillance and the need for any use of a recording device to be in compliance with data protection legislation, are that their use must be “necessary and proportionate”⁵² and that the use should be (as far as practicable) overt.⁵³ ICCL is concerned about the weakness of these safeguards in the phase of such broad provisions and powers to use the devices but it is welcome that the creation of the respective Codes of Practice necessitates prior consultation between An Garda Síochána and a number of policing oversight bodies, the Data Protection Commission and the Irish Human Rights and Equality Commission.⁵⁴

Kenya

52. Kenya’s Constitution guarantees the right to privacy under Article 31, which protects individuals from the unnecessary revelation of private affairs and intrusion into communications. Article 36 safeguards freedom of association, while Article 37 enshrines the right to assemble, demonstrate, and present petitions. These provisions reflect Kenya’s obligations under the International Covenant on Civil and Political Rights (ICCPR), particularly Articles 17, 21, and 22, which protect against arbitrary interference and uphold freedoms of assembly and association.
53. Despite this normative foundation, Kenya’s legislative framework has enabled expansive surveillance powers with limited oversight. The National Intelligence Service Act (2012) empowers intelligence agencies to intercept communications “for national security” without adequate judicial supervision. The National Police Service Act (2011) and Prevention of Terrorism Act (2012) similarly grant broad powers for covert surveillance and data collection. While these statutes contain provisions for judicial authorisation, they lack independent review mechanisms and detailed reporting requirements.
54. The Data Protection Act (2019) was intended to align Kenya’s data governance regime with international standards. It established the Office of the Data Protection Commissioner (ODPC) and introduced principles of lawfulness, fairness, and accountability in data processing. Yet,

⁵¹ ICCL and Digital Rights Ireland proposed amendments to the Garda Síochána (Recording Devices) Bill 2022, July 2023, page 22,

<https://www.iccl.ie/wp-content/uploads/2023/07/ICCL-DRI-Recording-Devices-bill-amendments-July-2023.pdf>

⁵² Section 9(4)(a), Garda Síochána (Recording Devices) Act 2023, <https://www.irishstatutebook.ie/eli/2023/act/32/enacted/en/print#sec8>

⁵³ Section 9(5)(a), Garda Síochána (Recording Devices) Act 2023, <https://www.irishstatutebook.ie/eli/2023/act/32/enacted/en/print#part2>

⁵⁴ Section 47(3), Garda Síochána (Recording Devices) Act 2023, <http://irishstatutebook.ie/eli/2023/act/32/enacted/en/print#sec8>

enforcement has been minimal. The ODPC remains underfunded, and its jurisdiction over national security operations is ambiguous. Civil Society Organizations such as Privacy International and ICNL Africa have noted that state agencies routinely bypass data protection requirements, claiming exemptions for “security purposes”. In practice, surveillance activities have proceeded unchecked, eroding the constitutional guarantees of privacy and association.

55. Parliament has also introduced measures that risk expanding digital monitoring. In 2024, legislators proposed amendments to allow real-time monitoring of internet activity, ostensibly to counter cybercrime. Simultaneously, the Directorate of Criminal Investigations (DCI) secured an increased budget allocation for social media surveillance operations, indicating an institutional shift towards digital policing. These developments, coupled with the absence of robust judicial oversight, have entrenched a culture of impunity in surveillance practices.
56. In summary, Kenya’s legal architecture for regulating surveillance remains fragmented and inadequate. There is no independent oversight body with a mandate to review or audit state surveillance operations. Procurement of surveillance systems occurs through opaque processes that invoke “national security” exemptions to avoid disclosure. The National Intelligence Service Act permits broad interception powers without stringent judicial approval, and the Computer Misuse and Cybercrimes Act continues to be misapplied against digital activists.
57. The Data Protection Act (2019) provides insufficient protection against state overreach, partly because the Office of the Data Protection Commissioner lacks authority to compel compliance by security agencies. Moreover, there is no legislation specifically regulating the deployment of facial recognition or AI-based analytics. This vacuum allows for arbitrary and disproportionate interference with fundamental rights.
58. The absence of remedies compounds the problem. Victims of unlawful surveillance rarely receive redress, as investigative mechanisms are opaque and accountability for human rights violations in policing remains minimal. The result is a surveillance regime that operates beyond democratic scrutiny, undermining Kenya’s constitutional order.
59. The cumulative impact of Kenya’s surveillance ecosystem has been to constrict civic space and normalise fear. The 2024–2025 period witnessed systematic targeting of activists, journalists, and ordinary citizens engaged in peaceful protest. According to Amnesty International Kenya and the Law Society of Kenya, at least 72 people were abducted or disappeared during the protests, many last seen in police custody. More than 600 were arbitrarily arrested, and at least 60 were killed through excessive use of force. The coordination of these operations through digital monitoring demonstrates the fusion of technological and physical repression.
60. The psychological impact has been equally damaging. Many activists now avoid participating in protests, fearing identification through facial recognition cameras or tracing via mobile

metadata. Organisations report self-censorship, reduced collaboration, and withdrawal from high-profile campaigns. This chilling effect extends beyond activists to ordinary citizens, who increasingly perceive civic participation as risky.

61. The CIVICUS Monitor (2025) categorises Kenya’s civic space as “repressed”, citing digital surveillance as a central driver of this decline. The intersectional impact is also notable. Privacy International and FIDA Kenya have documented cases where women human rights defenders experience gendered digital harassment, including doxing and stalking, often linked to surveillance of their online activities.
62. Kenya’s civic space has long been shaped by tensions between security imperatives and democratic aspirations. The state’s growing reliance on technology to monitor and control civic activity has placed these rights under strain. The emergence of a digital surveillance state, manifested through facial recognition technology (FRTs), mass camera networks, spyware, and algorithmic monitoring, has engendered a climate of fear and deterrence, eroding the ability of individuals and organizations to organise, dissent, and even communicate freely.
63. The situation deteriorated dramatically following the #RejectFinanceBill2024 protests, during which thousands of Kenyans, primarily young people, mobilised online and offline to oppose regressive fiscal measures. The government’s response combined traditional repression with sophisticated technological surveillance. Protest organisers were tracked online, internet access was throttled, broadcast signals were suspended, and social media accounts were monitored. These actions illustrate the convergence of digital and physical coercion, transforming Kenya’s public sphere into a heavily monitored landscape.

South Africa

64. AI remains largely unregulated in South Africa. Current regulations stem from existing legislation such as the Protection of Personal Information Act No.4 of 2013 (POPIA), which prevents the unlawful processing of personal data. However, when it comes to AI surveillance, POPIA does not deal extensively with how AI surveillance should be regulated. For instance, under POPIA, biometric data can be processed by law enforcement for the “prosecution of offenders or the execution of sentences of security measures”.⁵⁵ In the absence of stronger regulation on facial recognition technology, law enforcement default to relying on this technology, despite well-founded concerns that facial recognition systems are often inaccurate, especially when it comes to identifying people of colour.⁵⁶
65. While South Africa has recently made efforts to study and develop regulations on AI, these proposed regulations have little to do with surveillance. In October 2023, the Department of

⁵⁵ Section 6(1)(c)(ii) of Protection of Personal Information Act 4 of 2013.

⁵⁶ Rachel Fergus ‘Facial recognition remains largely ungoverned - and dangerous - in Minnesota’ *ACLU Minnesota* 29 February 2024 available at <https://www.aclu-mn.org/en/news/biased-technology-automated-discrimination-facial-recognition>, accessed 29 July 2024.

Communications and Digital Technologies (‘DCDT’) put out a draft document outlining a plan for regulating AI in the forthcoming years.⁵⁷ The document covers multiple risks, particularly the threat of generative AI, misinformation, racial bias in AI systems, and copyright concerns. The plan focuses mostly on economic threats, and the word “surveillance” does not appear anywhere in the document. The plan mentions only that the South African government should bear in mind privacy concerns when developing future regulations.

66. In 2019, the amaBhungane Centre for Investigative Journalism approached the Gauteng High Court for an order declaring the Regulation of Interception of Communications and Provision of Communication Related Information Act⁵⁸ (RICA) unconstitutional.⁵⁹ AmaBhungane submitted to the court that RICA was unconstitutional for the following reasons:

- It authorised surveillance of people without informing them of the warrant to intercept their communications, even when the interception has ended, and the investigation has concluded;
- It required private companies to store personal information related to their users and information on who they communicate with, without providing for any oversight mechanisms;
- There were no provisions on the procedures officials should follow with respect to examining, copying, sharing, and storing intercepted data, and related procedures in terms of destroying intercepted data that may be irrelevant to investigations;
- It failed to provide extra protections for persons with special legal duties to protect the confidentiality of those they speak with, such as lawyers and journalists;
- It failed to include a “public advocate” to represent the interests of people who have been targeted by the surveillance systems; and
- It failed to regulate the use of “bulk interception” programmes wherein mass surveillance practices would be employed to collect and analyse massive flows of data on large groups of people.

67. The High Court ruled in favour of amaBhungane, however it suspended the declaration of unconstitutionality for two years to allow Parliament to amend the legislation of its defects. The cited government departments appealed the High Court ruling to the Constitutional Court. In 2021, the Constitutional Court dismissed the appeal and upheld the High Court’s

⁵⁷ AI National Government Summit: Discussion Document South Africa’s Artificial Intelligence (AI) Planning (2023) *Department of Communications & Digital Technologies* available at https://www.dcdt.gov.za/Discussion_Document.pdf, accessed 29 July 2024.

⁵⁸ 70 of 2002

⁵⁹ *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* (25978/2017) [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP); 2020 (1) SA 90 (GP); 2020 (1) SACR 139 (GP).

judgment.⁶⁰ The Court held that the interception and surveillance of an individual's communications under RICA is a highly invasive violation of privacy, which is protected under section 14 of the Constitution.⁶¹ The Court then considered whether this invasion was reasonable and justifiable in terms of section 36(1) of the Constitution.⁶² It weighed the importance of the right to privacy and dignity,⁶³ against the importance of national security, with respect to the State's obligations to investigate and combat serious crime; maintain public order; and to ensure the safety of the Republic and its people.

68. The Court ultimately found that the surveillance proposed by the Act was "egregiously intrusive" in nature. Furthermore, it held that the proposition of bulk interception/surveillance should be declared unconstitutional. The Minister of Safety and Security argued that bulk surveillance should be allowed as it was consistent with section 2 of the National Strategic Intelligence Act⁶⁴. However, the Court disagreed, stating that section 2, in fact, does not authorise the practice of bulk surveillance, and is therefore unlawful and invalid.
69. In response to the *amaBhungane* invalidity judgment, the National Assembly introduced the General Intelligence Laws Amendment Bill. This Bill proposes the regulation of the National Communication Centre with respect to its functions, including surveillance. In vague terms, the Bill provides for the Centre's functions with respect to the gathering, correlating, evaluating, and analysing of relevant intelligence to identify any threat or potential threat to national security.⁶⁵
70. However, experts in the surveillance sector have pointed out that the Bill does not provide for the criticisms laid down by the Constitutional Court in the *amaBhungane* judgment. Furthermore, there are a variety of other dangers, most important of which is that it still allows for bulk identification, which puts large numbers of people under surveillance regardless of whether they are suspected of threats to national security.⁶⁶
71. Finally, the Bill fails to incorporate international best practices on the regulation of strategic intelligence and bulk interception in a democratic state. These require domestic legal

⁶⁰ *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC).

⁶¹ Constitution of the Republic of South Africa, 1996.

⁶² Limitation of Rights, Constitution of the Republic of South Africa, 1996.

⁶³ Section 10, Constitution of the Republic of South Africa, 1996.

⁶⁴ 39 of 1994

⁶⁵ Jane Duncan 'Surveillance and the state: South Africa's proposed new spying law is open for comment – an expert points out its flaws' *The Conversation* 5 February 2024 available at <https://theconversation.com/proposed-new-spying-law-an-expert-points-out-its-flaws>, accessed on 31 July 2024.

⁶⁶ *Ibid.*

frameworks to provide for what the European Court of Human Rights refers to as “end-to-end” safeguards covering all stages of bulk interception (*see footnote*).⁶⁷

72. Regarding social media surveillance, the Protection of Personal Information Act (POPIA), provides for the protection of personal information as it is processed by public and private bodies and sets out various obligations for organizations, including Big AdTech companies. More of that can be read in the social media surveillance section (paras. 213 and 214).

73. Finally, in 2021, the South African legislature bolstered the protection of personal information by promulgating the Cybercrimes Act.⁶⁸ The Cybercrimes Act established new offences while also developing the existing criminal offences with respect to cybercrimes. As a result, the Cybercrimes Act criminalises the unlawful and intentional access to a person’s computer or computer data storage system (hacking); unlawful interception or acquisition of data; as well as the developed offences such as cyber- fraud, forgery, uttering (passing-off of false data with the intention of fraud), and the theft of a person’s incorporeal property (e.g. their personal online data).⁴⁶

Digital AI Assisted Surveillance and Technologies Engaged

Introduction

74. Digital surveillance powered by AI is no longer a futuristic concept; it is now a global reality.⁶⁹ From citywide facial recognition in Delhi and annual scanning of millions of faces in the UK⁷⁰ to behavioral tracking in Poland,⁷¹ governments are rapidly adopting these tools to monitor public spaces. While they offer powerful possibilities for crime prevention, they are increasingly used to surveil protests and suppress dissent. For instance, in Myanmar, AI

⁶⁷ Ibid; “the European Court has stated that a domestic legal framework should define, (1) the grounds on which bulk interception may be authorized, (2) the circumstances, (3) the procedures to be followed for granting authorization, [and] (4) [the] procedures for selecting, examining and using material obtained from intercepts. The framework should also set out (1) the precautions to be taken when communicating the material to other parties, (2) limits on the duration of interception, (3) procedures for the storage of intercepted material, (4) the circumstances in which such material must be erased and destroyed, (5) supervision procedures by an independent authority, [and] (6) compliance procedures for review of surveillance once it has been completed.” (See *Big Brother Watch and Others v. The United Kingdom*, no. 58170/13, 25 May 2021).

⁶⁸ No. 19 of 2020.

⁶⁹ Steven Feldstein, ‘The Global Expansion of AI Surveillance’ (Carnegie Endowment for International Peace, 17 September 2019) <https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en> accessed 11 November 2025.

⁷⁰ Isabelle Walker, ‘The Evolution of Surveillance Technology’ (International Bar Association, 23 July 2025) <https://www.ibanet.org/The-evolution-of-surveillance-technology> accessed 11 November 2025.

⁷¹ ‘Polish gov’t expands AI surveillance powers’ (Central European Times, 24 May 2025) <https://centraleuropeantimes.com/polish-govt-expands-ai-surveillance-powers-2/> accessed 11 November 2025.

surveillance has been linked to violent crackdowns.⁷² Also, in *Glukhin v Russia*, the Court indeed found that the use of highly intrusive facial recognition technology to identify, locate and arrest a peaceful protester had breached his right to a private life and freedom of expression.⁷³

75. As these technologies gain traction worldwide, laws and proposals have emerged in attempts to reshape the surveillance landscape, raising alarms about their potential impact on civil liberties. For instance, in Ireland, new legislative measures, such as the *Garda Síochána (Recording Devices Act) 2023* have vastly expanded the ability of members of the police force (gardaí) to record, collect and store data about people and their movements by capturing still images, video footage and sounds in public spaces and places where gardaí have lawful access.⁷⁴ One of the purposes for which they can use the tools or measures is to secure ‘public order’. The use of surveillance tools to secure ‘public order’ brings them into the realm of protest and as they could lead to the identification of protestors, could have a significant chilling effect on the exercise of the right to freedom of assembly and of association. However in many other instances, either existing legislative frameworks are unable to address or predict risks associated with constantly evolving surveillance technologies, or there is a vacuum being purposely exploited by manufacturers and actors seeking to weaken and discourage civic participation and activism.
76. These concerns are exacerbated by plans to introduce facial recognition technology (FRT),⁷⁵ proposals to empower Irish police to order someone to remove a face covering in a public space,⁷⁶ and the use of AI tools to analyse vast stores of data.⁷⁷ ICCL is also concerned that as An Garda Síochána expands its use of surveillance technologies to secure public order, it fails to have an overarching policy on the use of technology in policing. As recently stated by an independent statutory body tasked with overseeing the services performed by An Garda

⁷² Isabelle Walker, ‘The Evolution of Surveillance Technology’ (International Bar Association, 23 July 2025) <https://www.ibanet.org/The-evolution-of-surveillance-technology> accessed 11 November 2025.

⁷³ *Glukhin v Russia* (App. No. 11519/20) (ECtHR Third Section, 4 July 2023) <https://hudoc.echr.coe.int/eng?i=001-225655> accessed 11 November 2025.

⁷⁴ ICCL, Briefing for Committee Stage of the An Garda Síochána (Recording Devices) Bill 2022, July 2023, <https://www.iccl.ie/wp-content/uploads/2023/07/ICCL-DRI-Recording-Devices-bill-briefing-July-2023.pdf>

⁷⁵ ICCL, Facial recognition tech could mean innocent people being misidentified as criminal suspects, 31 October 2024, <https://www.iccl.ie/2024/garda-frt-mural-unveiled/>

⁷⁶ ICCL, ICCL Submission on the General Scheme of the Criminal Law and Civil Law (Miscellaneous) Bill 2025, 27 June 2025, <https://www.iccl.ie/news/iccl-submission-on-the-general-scheme-of-the-criminal-law-and-civil-law-miscellaneous-bill-2025/>

⁷⁷ Harry McGee, Facial recognition: Work on law to introduce technology ‘well advanced’, says Minister, The Irish Times, 25 April, 2025, <https://www.irishtimes.com/politics/2025/04/25/work-on-legislation-to-introduce-facial-recognition-technology-well-advanced-says-minister/>

Siochana in Ireland, such a policy is important to ensure that principles such as fairness, proportionality, legality and non-discrimination are appropriately addressed and enforced.⁷⁸

77. These developments raise critical questions about how surveillance affects civil liberties, especially the right to protest. As the technology spreads, the challenge lies in balancing technological advancement with the protection of fundamental rights.
78. The subsequent sections outline various instances of AI-assisted surveillance technologies in practice, organised under different headings that correspond to the specific tools or methods employed. Each section highlights how these technologies are being deployed, the contexts in which they are used, and their implications for civil liberties and the right to protest.

Facial Recognition Technology (FRT)

Summary

79. The development and deployment of artificial intelligence technologies for public security purposes, such as automated facial recognition, can violate several fundamental rights, including privacy, freedom of association and assembly, presumption of innocence, and due process - but also cultural rights, the right to the city, and even to health. The connection with this topic is not always evident.
80. The implementation of a surveillance framework based on FRT raises concerns, both due to the risk of targeting protesters and the recognized discriminatory and racist bias, as system errors,⁷⁹ which disproportionately affect Black people, can lead to the unjust criminalization of individuals, further being used as a pretext for violent police interventions. Transgender people are also at greater risk, as facial biometrics accuracy drops to less than 60% concerning this population.⁸⁰ Thus, the biases embedded in AI-based surveillance and evidence-gathering tools are neither incidental nor easily correctable by technical means alone. They reflect and reinforce existing hierarchies of race, gender, and class, making their unregulated use in public security and judicial systems a direct threat to the principles of fairness, equality, and human dignity.
81. Across all the country case studies included below, a clear global pattern emerges: the use of Facial Recognition Technology (FRT) has expanded rapidly in policing and public surveillance, often justified by security and crime prevention goals but implemented in the absence of strong legal or regulatory frameworks. In nearly every case, FRT deployment has occurred without public consultation, transparency, or effective oversight, enabling unchecked data

⁷⁸ Policing Authority, Policing Authority Assessment of Policing Performance, December 2024, https://www.policingauthority.ie/assets/uploads/documents/Half-year_Assessment_of_Policing_Performance_2024.pdf

⁷⁹ BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: Conference on fairness, accountability and transparency. PMLR, 2018. p. 77-91.

⁸⁰ Teixeira, Pedro. Facial recognition misgenders transgender individuals. Folha de São Paulo, 2024. Available at: <https://www1.folha.uol.com.br/tec/2024/05/reconhecimento-facial-erra-genero-de-pessoa-trans.shtml>

collection and the integration of state and private surveillance networks. High rates of false positives and documented cases of misidentification, especially affecting Black and marginalized individuals, expose the technology's inherent biases and its potential to reinforce structural racism.

82. The widespread and unregulated use of FRT in public spaces, including protests, festivals, transport systems, and cultural events, has produced a chilling effect on freedom of expression, assembly, and participation in civic life. Courts and authorities in several countries have tended to accept public safety arguments to justify surveillance, while civil society organizations across regions have consistently warned that FRT, without strict legal safeguards and oversight, is incompatible with democratic values. Overall, the dominant trend is one of technological expansion outpacing human rights protections, leading to growing risks of discrimination, wrongful arrests, privacy violations, and the erosion of anonymity and democratic freedoms in public life.

Argentina

83. Starting in April 2019, a facial recognition system was established through an executive branch resolution in the City of Buenos Aires.⁸¹ The mechanism was meant to be used "only for tasks required by the Public Prosecutor's Office, the National, Provincial, and Autonomous City of Buenos Aires Judiciary, as well as for the detection of wanted persons exclusively by judicial order, registered in the National Database of Warrants and Captures (CONARC)." (Art. 2 of the Annex to the Resolution). Furthermore, it was established that the CONARC database and the corresponding personal data in the National Registry of Persons (RENAPER) would be provided by federal government representatives. The Resolution expressly stated that the national registry data must correspond to those who have a duly registered judicial order restricting their liberty (Art. 3).
84. Shortly after the program's announcement, it became clear that the system was producing a significant number of false positives. In 2019, it was used to detain 1,648 people, and 141 false positives were registered, according to an official response to an access to information request that year.⁸² This led to a judicial challenge and revelations that the system had been searched extensively: the trial court ruling in September 2022 confirmed nearly 10 million "extractions" of biometric data from the official database of wanted persons, including searches of political figures, journalists, and social leaders.⁸³ It was estimated that these

⁸¹ City of Buenos Aires Government, Ministry of Justice and Security, Resolution No. 398/MJYSGC/2019, "Approving the implementation of the Fugitive Facial Recognition System (SRFP)," sanctioned April 24, 2019. Available at: https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PE-RES-MJYSGC-MJYSGC-398-19-5604.pdf.

⁸² City of Buenos Aires Government, "Respuesta al pedido de información en 'O.D.I.A. c/ G.C.B.A. s/ Amparo', Expte. N° 9480/19 (NO-2019-33610651-GCABA-DGALSE)," 2019, available at: <https://srfp.odia.legal/respuesta-aip.pdf>.

⁸³ Court of First Instance in Administrative and Tax Litigation No. 4 (CABA), *Argentine Observatory of Computer Law (O.D.I.A.) et al. v. Government of the City of Buenos Aires (GCBA), amparo—other*, Case No. 182908/2020-0 (CUIJ EXP J-01-00409611-4/2020-0), judgment, Autonomous City of Buenos Aires,

requests involved 7 to 7.5 million people. Moreover, an expert report indicated that around 15,459 people had been improperly included in the system (they were not in the official CONARC database of wanted persons).⁸⁴ In 2022, the judicial ruling forced the City to suspend the program due to concerns about privacy and the lack of adequate controls.

85. In parallel with the legal battle, the Legislature of the City of Buenos Aires took steps to regulate the technology. On November 19, 2020, Law No. 6339 was passed, modifying Law No. 5688 (the Comprehensive Public Security System of the City of Buenos Aires) to create a specific legal framework for the use of facial recognition technology, given that the program had been implemented through a Ministry of Security resolution and lacked safeguards. The new law defined the aim of the fugitive facial recognition system as “the identification and recognition of fugitives from justice based on the real-time analysis of video images.” The regulation limited the system's use to tasks required by the National, Provincial, or City of Buenos Aires Judiciary, and to the detection of persons exclusively wanted by judicial order, registered in the CONARC National Database of Warrants and Captures (Art. 480 bis of Law 5688).
86. During the legislative debates over this new bill, civil society organizations highlighted various objections to the use of facial recognition systems. CELS warned that the system could lead to arbitrary detentions and threaten the presumption of innocence. CELS also noted that the use of this technology affects the principle of equality and non-discrimination, as facial recognition software has been repeatedly criticized for having higher false positive rates for women and people with darker skin tones, putting vulnerable groups at further risk.⁸⁵ Furthermore, CELS pointed out that facial recognition in video surveillance activities carries potential risks to rights such as privacy, freedom of expression, and protest.⁸⁶
87. For its part, the Ombudsman's Office of the City of Buenos Aires highlighted inaccuracies in the CONARC databases (e.g., incorrect or missing ID numbers), and stated that errors could have been avoided if an impact assessment had been conducted prior to the system's implementation. The Ombudsman requested that the Supreme Court correct these errors, but

September 2022. Available at: <https://www.cels.org.ar/web/wp-content/uploads/2022/09/reconocimientofacialsentencia070922.pdf>

⁸⁴ Karen Naundorf, “Un escándalo en Buenos Aires revela los peligros del reconocimiento facial,” WIRED, 15 de septiembre de 2023, available at:

<https://es.wired.com/articulos/escandalo-en-buenos-aires-revela-los-peligros-del-reconocimiento-facial>

⁸⁵ See P. Grother, M. Ngan y K. Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects [Informe técnico NISTIR 8280], Instituto Nacional de Estándares y Tecnología (NIST), Gaithersburg, MD, 2019, disponible en: <https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf>; Joy Buolamwini y Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification [Artículo de congreso], Proceedings of Machine Learning Research, vol. 81 (Conference on Fairness, Accountability, and Transparency), 2018, pp. 1–15, disponible en: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.

⁸⁶ Center for Legal and Social Studies (CELS), “The Buenos Aires City Legislature must reject the use of facial recognition technology for the surveillance of public space,” October 2020. Available at: <https://www.cels.org.ar/web/2020/10/la-legislatura-portena-debe-rechazar-el-uso-de-la-tecnologia-de-reconocimiento-facial-para-la-vigilancia-del-espacio-publico/>

this has not been done and CONARC remains outdated.⁸⁷ No impact study has yet been carried out either. Currently, the program remains suspended while civil society organizations work to determine how a system of this nature could be implemented in a way that can be audited to ensure respect for human rights.⁸⁸

88. Nevertheless, the issue of facial recognition remains an active concern. In 2025, the Public Prosecutor's Office of the City of Buenos Aires announced a recent purchase of facial recognition technology for nearly \$30,000 from the company Clearview AI.⁸⁹ Unlike the system applied by the City's Executive Branch, this new technology acquired by the Public Prosecutor's Office does not operate in real-time; it is applied to images that function as evidence within a judicial case. Since the earlier judicial ruling only refers to the system enabled by the City Executive Branch's resolution, there is no impediment to the City implementing the new Clearview system. This again raises the same structural problems as were observed with the previous attempt to implement facial recognition technology: an extremely intrusive biometric identification technology is being incorporated without clear safeguards.

Brazil

89. Since 2019, studies have indicated a significant increase in the use of surveillance devices in Brazil, primarily through facial recognition systems, which have been contracted despite the lack of evidence regarding their effectiveness and transparency in operation. São Paulo is the state in the Southeast region of Brazil with the most significant number of active projects—second only to Goiás (73) considering the whole country—and with the most crucial number of potentially surveilled individuals in the country (20,893,147).⁹⁰
90. It is essential to highlight that due to the lack of a federal law regulating personal and sensitive data use in public security, each Brazilian state has implemented surveillance systems with its own rules. According to Conjur, by May 2024, five states had placed over 1,700 people in custody based on facial recognition technology, with Bahia accounting for 90% of these arrests.⁹¹ However, this number is likely much higher now, as in the city of São

⁸⁷ Center for Legal and Social Studies (CELS), *Amicus curiae submission in ODIA et al. v. Government of the City of Buenos Aires (Facial Recognition System case)*, undated (PDF). Available at: <https://srfp.odia.legal/cels.pdf>.

⁸⁸ Juan Brodersen, "Why facial recognition remains suspended in the City of Buenos Aires: keys to understanding the uses and risks of this artificial intelligence," *Clarín*, March 8, 2024. Available at: https://www.clarin.com/tecnologia/reconocimiento-facial-sigue-suspendido-ciudad-buenos-aires-claves-entender-usos-riesgos-inteligencia-artificial_0_eT30Dwx2Gm.html.

⁸⁹ Sasha Pallares, "The City reignites the electronic eye: facial recognition and social control in Buenos Aires City," *El Grito del Sur* (Buenos Aires), October 7, 2025. Available at: <https://elgritodelsur.com.ar/2025/10/ciudad-reconocimiento-facial-ojo-electronico/>

⁹⁰ O PANÓPTICO. Monitoring facial recognition projects in Brazil. Available at: <https://www.opanoptico.com.br/#regioes>.

⁹¹ TAJRA, Alex. Proceedings of Surveillance: See how each Brazilian state uses facial recognition for police purposes. Conjur, 2024. Available at: <https://www.conjur.com.br/2024-mai-17/veja-como-cada-estado-usa-o-reconhecimento-facial-para-fins-policiais/>.

Paulo alone, 2,000 fugitives were arrested and over 3,000 people were arrested in the act, as of October 2025.⁹²

91. Although there is no recent data on the profiles of individuals deprived of their liberty in these situations – which is, in itself, a problem – a 2019 study by CESeC found that 90% of the 151 people arrested in Brazil through facial recognition by that time were Black.⁹³ The press reports that these arrests have been accompanied by a series of serious failures.⁹⁴
92. According to the data monitored by CESeC from 2019 to April 2025, there were 24 cases of errors. Of these, 15 were in Rio de Janeiro, 4 in São Paulo, 3 in Bahia, and 2 in Sergipe. Of the profile of those being wrongly identified, 62.5% are men. In cases where there is information, 75% of the people improperly recognized are black. The majority of approaches took place on public roads (11), followed by approaches at stadiums (10) and health facilities (3). This is only a partial picture of an unknown number of false positives, since there is no official record of when a person is only brought to the police station but not detained or arrested.
93. An emblematic example occurred in April 2024, during the final of the Sergipe Championship, when a Black man was wrongly detained after the system identified him as a criminal. He later reported the embarrassment and humiliation he suffered after being wrongly misidentified in front of thousands of people in a football stadium.⁹⁵
94. Another case involved a Black woman who was approached three times by the police during a popular event in Aracaju/SE due to flaws in facial recognition. In one of these incidents, the woman urinated in her pants out of nervousness and embarrassment and was taken to the police van like a criminal despite her innocence.⁹⁶
95. More recently, in April 2025, an 80-year-old Black man was erroneously identified by cameras at a health facility, where he did volunteer work, and was mistaken for a white man wanted

⁹² DE LUCA, Adriana. Smart Sampa Hits 2,000 Fugitive Arrests; See Real-Time Arrests in São Paulo. CNN, 2025. Available at:

<https://www.cnnbrasil.com.br/nacional/sudeste/sp/smart-sampa-atinge-marca-de-2-mil-foragidos-p-resos-veja-fla-grantes-em-sp/>

⁹³ BARBON, Júlia. 151 people are arrested through facial recognition in the country; 90% are Black. Folha de São Paulo, 2019. Available at:

<https://www1.folha.uol.com.br/cotidiano/2019/11/151-pessoas-sao-presas-por-reconhecimento-facial-no-pais-90-sao-negras.shtml>.

⁹⁴ GRINBERG, Felipe et al. Facial recognition arrests are advancing across the country, but a series of errors challenge the crime-fighting technology. O Globo, 2024. Available at:

<https://oglobo.globo.com/brasil/noticia/2024/01/05/prisoos-por-reconhecimento-facial-avancam-pelo-pais-mas-e-rros-serie-desafiam-tecnologia-de-combate-ao-crime.ghtml>

⁹⁵ GLOBO. “Fearful, frustrated, and embarrassed,” says man wrongfully detained in stadium after facial recognition system error. *Fantástico*, 2024. Available at:

<https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-enga-no-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml>.

⁹⁶ UOL. Facial Recognition: Errors and Lack of Transparency. UOL Notícias, 2024. Available at:

<https://noticias.uol.com.br/cotidiano/ultimas-noticias/2024/04/28/reconhecimento-facial-erros-falta-de-transparencia.htm>.

for the crime of rape. He was taken to the police station, where he remained for over 10 hours.⁹⁷

96. Also at a public health facility, a pregnant woman was identified through FRT. According to press reports, the police's aggressiveness led to her premature delivery.⁹⁸ These are only the most visible incidents — many others remain undocumented due to the lack of systematic data collection, supervision, and public transparency regarding the use of AI technologies in Brazilian public security. This opacity, combined with error-prone systems and structural racism, severely hampers any proper evaluation of the impacts.
97. Another event related to using FRT and the right to assembly and cultural rights was the São Paulo City Hall's announcement that it would monitor individuals during Carnival – Brazil's main popular festival, in 2025. On February 20, at a press conference on security forces' actions during the holiday in São Paulo, the City Hall presented the monitoring of street parties through the "Smart Sampa"⁹⁹ program as a new development in its action plan, highlighting the possibility of arrests through facial recognition.
98. Based on its responsibilities, the Specialized Center for Citizenship and Human Rights of the Public Defender's Office of São Paulo officially notified the mayor and the municipal secretary of Urban Security, stating that "*Street Carnival must be understood as a way to exercise the right to protest and freedom of expression, being fundamental to guaranteeing the realization of civil, political, social, and cultural rights. Security forces must act to FACILITATE the holding of demonstrations, such as Carnival, and must not involve undue interference.*"¹⁰⁰ In the document, it also highlighted the "Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests" from this rapporteur, implying that the use of technology by the Government must facilitate demonstrations and aim to guarantee freedom of assembly, preventing such moments from being seen as opportunities for surveillance.

⁹⁷ UOL. Facial recognition in São Paulo mistakes elderly man for fugitive rapist. Available at: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2025/04/13/reconhecimento-facial-de-sp-convolve-idoso-com-estuprador-foragido.htm>

⁹⁸ APUBLICA. Smart Sampa: grávida é presa em posto de saúde e cabatando parto prematuro. Available at: <https://apublica.org/2025/04/smart-sampa-gravida-e-presa-em-posto-de-saude-e-acaba-tendo-parto-prematuro/>

⁹⁹ In 2022, the City Hall of São Paulo issued a bidding notice for hiring video surveillance and facial recognition services, known as Smart Sampa, planning the installation of 20,000 cameras in the city. Civil society organizations, such as the campaign "Take My Face Off Your Target", which Conectas is a member, have pointed out serious issues in this process, such as the absence of an impact assessment on rights. In addition, a section of the original notice stated that the cameras should allow the tracking of characteristics such as color and point out situations of "vagrancy", terms that are racist and aporophobic. Although the project has been the subject of an investigation by the Public Prosecutor's Office and legal actions its implementation is ongoing.

¹⁰⁰ Disponível em: https://www.conjur.com.br/wp-content/uploads/2025/02/OF_020_2025-Blocos-e-Carnaval-de-Rua_smart-sampa-a-uso-de-tecnologia-para-prisoas.pdf

99. Furthermore, it expressly recommends that FRT and other biometric systems should not be used to identify individuals who peacefully participated in Carnival¹⁰¹; that this technology was not used to remotely categorize, profile, or identify individuals, as they are discriminatory and inconsistent¹⁰²; that the use of digital technologies was made exclusively to enable the right to freedom of assembly¹⁰³; that transparent and auditable recording of all relevant decisions on digital technologies be guaranteed¹⁰⁴; that there was no demand for participants in demonstrations during their routes, except under relevant justification¹⁰⁵; and that, in exceptional cases, the procedure was duly recorded and justified¹⁰⁶.
100. On February 24, in a press release, the City Hall said that it would deny the Center's request and received the request with "strangeness" and "indignation"¹⁰⁷. Days later, a state representative requested the opening of an administrative procedure against the three defenders who signed the questioning and asked to remove one of them, stating that the letter does not serve "the good population"¹⁰⁸. Following this retaliation, on February 28, the Public Defender met with municipal authorities, including the mayor, and the Public Defender's Office published a statement backtracking from its position.¹⁰⁹
101. In addition to this case, and the growing use of this technology in football stadiums - a national passion - it is also possible to see how the FRT has been applied to significant events, such as musical concerts throughout Brazil, such as Lady Gaga's, in Copacabana, in Rio de Janeiro, which brought together 2.5 million people. A serious aggravation accompanies this entire scenario: the cooperation between private companies and different spheres of the public sector without any transparency regarding how data is being collected and processed.
102. Reinforcing these concerns, in 2024, the media reported the integration, through an agreement, of the systems from the "Muralha Paulista" program - from São Paulo state - and "Smart Sampa" - from São Paulo municipality -, allowing data sharing. Attention is also drawn to the provision and possibility of incorporating images from private system cameras into

¹⁰¹ 71 b - "Model Protocol".

¹⁰² 32 - "Model Protocol".

¹⁰³ 39 - "Model Protocol".

¹⁰⁴ 53 - "Model Protocol".

¹⁰⁵ 80 - "Model Protocol".

¹⁰⁶ 81 - "Model Protocol".

¹⁰⁷ G1. Defensoria Pública de SP pede à prefeitura que não utilize reconhecimento facial do Smart Sampa em blocos de carnaval. Disponível em:

<https://g1.globo.com/politica/blog/julia-duailibi/post/2025/02/24/defensoria-publica-de-sp-pede-que-pre-feitura-nao-utilize-reconhecimento-facial-do-smart-sampa-em-blocos-de-carnaval.ghtml>.

¹⁰⁸ Metrópoles. Defensora que questionou Smart Sampa no Carnaval é alvo de deputada. Disponível em:

<https://www.metropoles.com/sao-paulo/defensora-que-questionou-smart-sampa-no-carnaval-e-alvo-de-deputada>

¹⁰⁹ Disponível em:

<https://www1.folha.uol.com.br/colunas/painel/2025/02/apos-reacao-de-aliados-de-nunes-defensoria-de-sp-recua-e-diz-nao-ser-contraria-ao-smart-sampa.shtml>

these tools.¹¹⁰ In January 2025, a deal that will integrate the “Smart Sampa” cameras with the “Córtex” platform of the Ministry of Justice of the federal government was announced.¹¹¹ In 2022, along with partner organizations, Conectas alerted the Federal Public Prosecutor’s Office regarding “Córtex”, capable of gathering personal data from different databases, cross-referencing them, and defining targets for real-time monitoring. In addition, “Córtex” operates without any control or auditing, allowing improper use and misuse by state agencies, as well as serious violations of the right to privacy and intimacy.¹¹²

Canada

103. There are no documented instances where Facial Recognition Technologies were used by Canadian police in relation to political protests. However, Canadian policing agencies are using FRT in other contexts, and there is no explicit prohibition on the use of the technology on protestors.
104. There are no clearcut regulations regarding the use of FRT in Canada. The Office of the Privacy Commissioner of Canada has held, for example, that the legal framework for FRT in Canada can at best be described as a patchwork of existing legislations.¹¹³ A Parliamentary committee studying the technology similarly concluded that Canada’s current legislative framework does not adequately regulate FRT.¹¹⁴
105. There have been a number of documented uses of FRT by policing forces in Canada. The Royal Canadian Mounted Police (“RCMP”) and other Canadian policing agencies were found to have used a commercial provider (ClearviewAI) to perform facial recognition searches against a large database of images scraped from the Internet without consent.¹¹⁵ ClearviewAI no longer offers its services to Canadian policing agencies after the FRT company was found to violate

¹¹⁰ LEITE, Maju Arruda. Facial recognition and video surveillance programs will be unified in São Paulo.

Available at:

<https://www.band.uol.com.br/noticias/programas-de-reconhecimento-facial-e-videomonitoramento-serao-unificados-os-em-sp-16668352>

¹¹¹ PASSARELLI, Vinícius. Agreement will integrate Smart Sampa cameras with the Córtex platform.

Metrópoles, 2025. Available at:

<https://www.metropoles.com/sao-paulo/acordo-vai-integrar-cameras-do-smart-sampa-a-plataforma-cortex>

¹¹² Available at:

<https://www.conectas.org/noticias/entidades-pedem-que-mpf-estude-sistema-de-vigilantismo-do-governo-bolsonaro/>

¹¹³ Office of the Privacy Commissioner of Canada, *Privacy guidance on facial recognition for police agencies* (May 2022) https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/ accessed 24 October 2025.

¹¹⁴

<https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf>

¹¹⁵ Office of the Privacy Commissioner of Canada, *Privacy Commissioner calls for ban on use of facial recognition technology for mass surveillance* (10 June 2021)

https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210610 accessed 24 October 2025.

Canadian privacy laws in its operation.¹¹⁶ Policing agencies have also created facial recognition-enabled mugshot databases.¹¹⁷

106. There have been calls in Canada for a moratorium or a ban on the use of FRT and more specifically for restrictions on its use in political protests.¹¹⁸ The Canadian Civil Liberties Association (CCLA) and other civil society organizations have continuously called for a moratorium on the use of FRT in Canada until appropriate legislation is put in place and an oversight body is established to consider all the possible consequences of its use.¹¹⁹ A Parliamentary committee studying the technology recommended that a moratorium be imposed on the use of FRT by federal policing services in Canada; and a joint statement by Canada's federal, provincial and territorial privacy commissioners have called for a direct and explicit ban on the use of FRTs to monitor individuals participating in protests.¹²⁰
107. As noted above, there are no documented cases in Canada where facial recognition was used to identify participants in political protests. However, awareness that law enforcement have access to these technologies and are not legally prohibited from using them at protests has fuelled concerns among protest participants.¹²¹

Ireland

108. Given the *Recording Devices Act* has vastly expanded An Garda Síochána's ability to collect and store imagery and video material concerning members of the public, through a variety of new technologies, serious concerns about how this vast collection of data will impact people's right to protest are only exacerbated by the fact there are plans afoot to allow Irish police use Facial Recognition Technology (FRT).¹²²

¹¹⁶

<https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>; https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

¹¹⁷ <https://www.oipc.bc.ca/documents/investigation-reports/1178/>;

https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/; *R v Voong*, 2018 ONCJ 352, <https://www.canlii.org/en/on/oncj/doc/2018/2018oncj352/2018oncj352.html>.

¹¹⁸ A number of policing agencies have stated they do not use FRT in the context of protests or at all:

<https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf>, pp 19-20; <https://www.cbc.ca/newsinteractives/features/police-drones/>;

¹¹⁹ Canadian Civil Liberties Association and Privacy International, *Consultation Response: Draft Privacy Guidance on Facial Recognition for Police Agencies* (21 October 2021)

<https://ccla.org/wp-content/uploads/2021/11/2021-10-21-CCLA-PI-FRT-submission.pdf> accessed 24 October 2025.

¹²⁰ Joint Statement by Federal, Provincial and Territorial Privacy Commissioners, *Recommended legal framework for police agencies' use of facial recognition technology* (2 May 2022)

https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/s-d_prov_20220502/ accessed 24 October 2025

¹²¹

<https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf>, p 19;

https://www.pivotallegal.org/vpd_surveillance_of_demonstrators_supporting_palestinian_human_rights.

¹²² European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Adopted 26 April, 2023, p.15,

109. A general scheme of the FRT legislation proposes that An Garda Síochána could use FRT in respect of any imagery or footage that it legally retains, or can legally access, “to locate a person or to follow the movements of a person in order to progress an investigation...” in respect of certain offences, including the public order offence of obstructing a Garda (Police officer).¹²³ ICCL has heard testimonies from peaceful protesters that they have been arrested for this offence, frequently alongside the broad offence of failure to comply with a direction of a Garda.¹²⁴ ICCL has been concerned that public order offences are being used to criminalise protesters and the use of FRT may enable increased charges for public order offences. Coupled with the use of body-worn cameras, it is ICCL’s position that such a measure would undoubtedly have an impact on people’s right to protest and may create a chilling effect.
110. ICCL has outlined its serious concerns with this proposed piece of legislation in full before the Irish parliament.¹²⁵ It has also contributed to INCLO’s recently published *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition: Principles to reduce the human rights harms of FRT* which state that police should never use FRT to identify protesters or collect information on people attending peaceful assemblies.¹²⁶
111. ICCL, along with fellow INCLO members, believes that the mere knowledge that police are using FRT, either in a manner that is live or retrospective, severely affects people’s reasonable expectation of being anonymous in a public space, and could result in a chilling effect on citizens’ ability or decision to gather, express their opinions, freely exchange information and engage in behaviour that is necessary and vital for a healthy democracy, thereby impairing political participation.¹²⁷ ICCL also agrees with experts who have warned that the long-term chilling effects of FRT on democratic societies have not been fully examined by the courts or the police.¹²⁸

https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

¹²³ Section 19, <https://www.irishstatutebook.ie/eli/1994/act/2/section/19/enacted/en/html#sec19>

¹²⁴ Section 8, <https://www.irishstatutebook.ie/eli/1994/act/2/section/8/enacted/en/html>

¹²⁵ Submission to the Joint Oireachtas Committee on Justice Draft General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023 18 January 2024,

<https://www.iccl.ie/wp-content/uploads/2024/02/ICCL-and-DRI-FRT-submission.pdf>

¹²⁶ International Network of Civil Liberties Organizations, *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition – Principles to Reduce the Human Rights Harms of Facial Recognition Technology* (March 2024) <https://inclo.net/wp-content/uploads/2024/03/INCLO-FRT-Principles-Final.pdf> accessed 3 November 2025.

¹²⁷ Murray, D et al., “The Chilling Effect of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe”, *Journal of Human Rights Practice*, Volume 16, Issue 1, February 2024, pp. 397–412, <https://academic.oup.com/jhrp/article/16/1/397/7234270>

¹²⁸ Murray, D, “Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework”, *Modern Law Review*, December 2023, <https://onlinelibrary.wiley.com/doi/10.1111/1468-2230.12862>

112. In tandem with ICCL's opposition to Ireland's policing FRT plans,¹²⁹ ICCL is also concerned about how those plans relate to proposed amendments to Ireland's public order legislation to explicitly grant gardaí the power to ask someone to remove a face covering in a public space when someone is engaging in violence or intimidation. ICCL's position is that gardaí have existing powers under the Public Order Act to address threatening, intimidating or violent behaviour at protests and that the proposed amendments to the Public Order Act are a disproportionate interference with the right to peaceful protest and an unnecessary expansion of Garda powers. The Bar Council of Ireland agrees with our assessment.¹³⁰
113. These concerns sit alongside broader objections to proposals empowering Irish police to compel the removal of face coverings in public spaces,¹³¹ and the use of AI tools to analyse vast stores of data.¹³² ICCL is also concerned that as An Garda Síochána expands its use of surveillance technologies to secure public order, it fails to have an overarching policy on the use of technology in policing. As recently stated by an independent statutory body tasked with overseeing the services performed by An Garda Síochána in Ireland, such a policy is important to ensure that principles such as fairness, proportionality, legality and non-discrimination are appropriately addressed and enforced.¹³³
114. Furthermore, ICCL believes that wearing a face covering is not in itself violent behaviour, nor does it indicate an intention to engage in violence. There are many reasons people may wish to cover their face at a protest or in daily life – including for health reasons, for religious reasons, to protect their privacy or to demonstrate political solidarity.
115. It is ICCL's position that, combined with increased Garda surveillance through body-worn cameras, drones, live access to third-party CCTV and plans to use facial recognition technology, as outlined above, criminalising face coverings risks creating a chilling effect whereby people feel unable to express their opinions in public spaces.¹³⁴ ICCL would greatly

¹²⁹ ICCL, Facial recognition tech could mean innocent people being misidentified as criminal suspects, 31 October 2024, <https://www.iccl.ie/2024/garda-frt-mural-unveiled/>

¹³⁰ Bar Council Submission on the General Scheme of the Criminal Law and Civil Law (Miscellaneous Provisions) Bill 2025, June 2025
https://www.lawlibrary.ie/app/uploads/securepdfs/2025/06/Submission-to-Oireachtas-Joint-Cttee-on-Criminal-Civil-Bill-26.6.25_.pdf

¹³¹ ICCL, ICCL Submission on the General Scheme of the Criminal Law and Civil Law (Miscellaneous) Bill 2025, 27 June 2025,
<https://www.iccl.ie/news/iccl-submission-on-the-general-scheme-of-the-criminal-law-and-civil-law-miscellaneous-bill-2025/>

¹³² Harry McGee, Facial recognition: Work on law to introduce technology 'well advanced', says Minister, The Irish Times, 25 April, 2025,
<https://www.irishtimes.com/politics/2025/04/25/work-on-legislation-to-introduce-facial-recognition-technology-well-advanced-says-minister/>

¹³³ Policing Authority, Policing Authority Assessment of Policing Performance, December 2024,
https://www.policingauthority.ie/assets/uploads/documents/Half-year_Assessment_of_Policing_Performance_2024.pdf

¹³⁴ ICCL Submission on the General Scheme of Criminal Law and Civil Law (Miscellaneous Provisions) Bill 2025 June 2025
<https://www.iccl.ie/wp-content/uploads/2025/06/250625-ICCL-submission-on-Criminal-Civil-Misc-Gener>

welcome any reflections from the Special Rapporteur on legislative proposals to ban face coverings at protests in the era of facial recognition technology, body-worn cameras and other digital surveillance tools.

Kenya

116. Kenya's integration of facial recognition into its urban surveillance infrastructure marks a decisive evolution in state monitoring. The "Safe City" projects launched in Nairobi and Mombasa since 2014 have installed thousands of high-definition cameras equipped with AI analytics and facial recognition capabilities. Operated through collaborations between the National Police Service, Safaricom, and Huawei Technologies, these systems are linked to command-and-control centres capable of real-time monitoring.
117. Government officials have justified these projects as tools to enhance security and deter crime. However, research by African Liberty and the Centre for Human Rights and Policy Studies (CHRIPS) reveals that the systems have also been deployed to track protest movements and identify participants in demonstrations. The cameras are equipped with facial and license-plate recognition software capable of identifying individuals in crowds and cross-referencing them with national databases.
118. This practice fundamentally alters the nature of public participation. The knowledge that one's presence at a protest can be permanently recorded and analysed through AI-enabled recognition deters individuals from exercising their right to assemble. Moreover, the technology's algorithmic bias risks disproportionate targeting of marginalised groups. International Network of Civil Liberties Organisations (INCLO) warns that live facial recognition "renders anonymity impossible in protest environments", making its use inherently disproportionate and incompatible with democratic assembly.
119. In the Kenyan context, the deployment of such systems has proceeded without public consultation or data protection impact assessments. There is no legal requirement for transparency on how data is collected, how long it is stored, or who can access it. The absence of oversight creates opportunities for misuse, including the tracking of political opponents and civic activists. The result is an invisible infrastructure of surveillance that chills democratic participation and undermines public trust.

Russia

120. On 13 July 2023 Andrey M. was on a Moscow metro train; there he wrote "[expletive] no to war!" over a metro map. Four days later, on 17 July, he was arrested at a different location in the Moscow metro, at a station. He was told that his face matched the sample taken by the CCTV cameras on the train on 13 July. This match was explicitly referred to in the administrative offence filed against him. Also on 17 July a district court judge in Moscow found Andrey guilty of the offence of "discrediting the Russian Armed Forces" and sentenced

him to a fine of RUB 30,000 (approx. EUR 323 or USD 374). The judge dismissed any arguments as to the legality of the functioning of the FRT on the Moscow metro.

121. On 23 July 2023 Andrey was briefly arrested on the metro again, his biometrics were taken by the police and he was promptly released. He took judicial review proceedings against the use of FRT and his arrest, but the courts from a district judge in Moscow to the Russian Supreme Court dismissed his claims. Essentially the courts ruled that biometric personal data can be taken and processed without consent, including for FRT purposes for the reason of public safety. Surveillance on the metro was, for the Russian courts, covered by definition under public safety at all times.

South Africa

122. Within South Africa, the use of FRT in recent years has greatly expanded; however, public concern regarding the technology is nearly non-existent.¹³⁵ Despite the public view that FRT and related surveillance technologies will bolster security, there are real concerns about their development and use.
123. In 2022, Karen Hao and Heidi Swart outlined the harms arising from FRT development in South Africa, which is especially prevalent as foreign companies, many of which originating in Switzerland, Sweden, and other European countries, “dump their AI technologies” into South Africa; “[t]he local security industry, forged under the pressures of a high crime environment, embraced the menu of options. The effect has been the rapid creation of a centralized, coordinated, entirely privatized mass surveillance operation.”¹³⁶ Unfortunately, the new technologies are replicating patterns of colonial history, with “predominantly white people having the means to pay for surveillance, and predominantly black people ending up without a say about being surveilled.”¹³⁷
124. While much of the development and deployment of AI and FRT in South Africa are primarily within the private sector, the South African government has been developing its own system for law enforcement use.¹³⁸ The Automated Biometric Identification System is intended to

¹³⁵ Facial recognition on the rise as businesses go touchless, <https://itecgroup.co.za/insights/press/facial-recognition-on-the-rise-as-businesses-go-touchless/>; Digital transformation, facial recognition technologies anticipated to grow despite slowing economic growth, 19 Apr 2023, <https://www.itweb.co.za/article/digital-transformation-facial-recognition-technologies-anticipated-to-grow-despite-slowing-economic-growth/KWEBbvyLKPyqmRjO>

¹³⁶ South Africa’s private surveillance machine is fuelling a digital apartheid, 19 Apr 2022, <https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid/>

¹³⁷ Ibid

¹³⁸ What is ABIS?, <https://www.dha.gov.za/index.php/civic-services/abis>; DHA 2019-2020 Annual Performance Plan https://static.pmg.org.za/DHA_APP_2019_V6.pdf, (“The Automated Biometric Identification System (ABIS), that will enable advance identification and verification through fingerprints and other selected modes of biometrics (palm-prints, iris, facial recognition and DNA), was launched on 16 May 2018. The ABIS will form the backbone of the future national identity system, which will replace the current national population register, using real time data from the civic registers, enhanced movement control system (EMCS) and the national immigration identification system (NIIS). The delivery of this project will happen in a phased approach. The State Information Technology Agency (SITA) and Council for Scientific and Industrial

include the face of every resident and foreign visitor to the country; the Department of Home Affairs states ABIS's expected benefits include faster turnaround time for ID documents, faster client identity verification for banks, improved board control, and suspect identification matching latent prints against records on ABIS.

125. The ABIS project is funded from the Integrated Justice System and, as of 2024, is estimated to cost R30 million.¹³⁹ DHA's current identification system, the Home Affairs National Identification System ("HANIS") has been in operation since 2002 and stores fingerprints and facial photographs. The implementation of ABIS is intended to transfer the functionalities currently under the HANIS to the new platform as well as incorporate additional features and capabilities, including facial recognition, biometrics, iris, palm-print and infant footprint recognition, for enrolment, identification, verification, and latent searches. Additionally, while DHA's plans to advance their IT by moving from HANIS to ABIS, then Minister of Home Affairs, Dr Aaron Motsoaledi, stated HANIS is not obsolete and "when there is a problem [with ABIS], we run back to it."
126. The DHA states that all data migrated to ABIS will be in readily usable form, with no duplication of data and no compromise of data, and the system will be "deployed into production," meaning it will be usable by both Immigration and Civic Services as a backend system with new capabilities. As such, ABIS will interface with all systems to ensure a single view of the data of citizens and non-citizens.
127. IDEMIA, a French multinational technology company, has been tasked with implementing ABIS. However, there have been significant delays since the project was first announced at the end of 2017. The first phase of ABIS was initially intended to be up and running within 12 months.
128. In May 2023, the Portfolio Committee on Home Affairs released a media statement outlining their concerns regarding the persistent delays from HANIS to ABIS.¹⁴⁰ The committee noted

Research (CSIR) have completed comprehensive system conceptual design and specifications. Procurement of a service provider through SITA was completed in the 2017/18 financial year. The development of the new system and data migration were planned for the 2018/19 financial year. This system will enable effective e-Government initiatives, with all departments and government entities that require instant identification and verification during service delivery, having central access to ABIS. The replacement of biographic databases, i.e. national population register and its sub-systems, is a mammoth task and the main component of the modernisation of DHA systems. The replacement of these systems and integration with other systems in especially the immigration environment will speed up and secure both civic and immigration processes. SITA has appointed CSIR to undertake the review of the current system, gather the comprehensive requirements from all stakeholders and to develop system specifications. The new system will enable the full modernisation of the DHA (front and back-end systems)"

¹³⁹ DHA 2023-2024 Annual Performance Plan, 48, https://www.dha.gov.za/images/AnnualReports/DHA-APP-2023-V5_update2.pdf; see also, DHA Strategic Plan 2020-2025, https://www.dha.gov.za/images/FILES2/DHA_Strategic_Plan2020_25_WEB.pdf

¹⁴⁰ Media Statement: Home Affairs Committee Disappointed With Lack of Progress in Migrating to Automated Biometric Identification System, 10 May 2023,

that despite the delays and problems with data migration between the two systems, they still “support the use of an upgraded system with innovative technological functionalities, such as facial recognition and palm biometric modalities, which will create further confidence in the population register.”¹⁴¹ Additionally, with regard to the Biometrics Movement Control System (“BMCS”), the committee similarly raised concerns about teething challenges, such as inadequate bandwidth and the impact of load shedding at some ports of entry, which impact on the system’s functionality. The committee urged the DHA to find workable solutions to these challenges to ensure a fully functional movement control system, “as this has a direct impact on securing [RSA’s] borders.”

129. Regarding current functionalities, in a 2023 committee meeting, Mavuso stated that ABIS’s current functionalities are facial recognition, fingerprints, and latent search.¹⁴² The project consists of three phases. On completion of Phase One, ABIS should be fully functional and the migration of the HANIS biometric data will be 100% complete and in a usable format. Fingerprints, facial recognition, and latent search functionality should be fully operational and in production as well. Phase Two entails the Enhancement of ABIS functionality by implementing Iris, Palmprint, and Infants Footprint biometrics. And finally, Phase Three involves the addition of any other biometric modalities as required by DHA such as DNA, and system maintenance and support.
130. A major concern with ABIS is that every South African, as well as foreign national (upon entering the country legally), will have their biometric information captured in ABIS; South Africa already has a similar database to Interpol – a criminal database with a facial recognition system containing mugshots from 180 countries; South Africa’s Automated Fingerprint Identification System (“AFIS”) is only capable of fingerprint searches. AFIS lets SAPS take fingerprints from crime scenes (latent fingerprints) and do one-to-many identification searches with a database of convicts’ fingerprints. However, AFIS cannot do anything if the suspect has no record. As a result, SAPS advocates desperately for direct access to the biometrics of all citizens and visitors.¹⁴³
131. SAPS started advocating for access to citizen biometrics over a decade ago, resulting in the Criminal Law Amendment Act 6 of 2010. The Act forces all government departments, and

<https://www.parliament.gov.za/press-releases/media-statement/home-affairs-committee-disappointed-lack-progress-migrating-automated-biometric-identification-system>

¹⁴¹ South Africa’s private surveillance machine is fuelling a digital apartheid, 19 Apr 2022,

<https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid/>

¹⁴² Facial recognition on the rise as businesses go touchless, <https://itecgroup.co.za/insights/press/facial-recognition-on-the-rise-as-businesses-go-touchless/>; Digital transformation, facial recognition technologies anticipated to grow despite slowing economic growth, 19 Apr 2023, <https://www.itweb.co.za/article/digital-transformation-facial-recognition-technologies-anticipated-to-grow-despite-slowing-economic-growth/KWEBbvyLKPyqmRj>

¹⁴³ Bill to help SAPS establish collective fingerprints database, 10 Dec 2008,

[https://www.phfirms.co.za/kc/Data/Bill to help SAPS establish collective fingerprint 3205.asp](https://www.phfirms.co.za/kc/Data/Bill%20to%20help%20SAPS%20establish%20collective%20fingerprint%203205.asp);

Government wants to ‘track’ all South Africans from birth – here’s why, 30 Oct 2020,

<https://businesstech.co.za/news/technology/444722/government-wants-to-track-all-south-africans-from-birth-heres-why/>

specifically DHA, to let police do “comparative” searches for investigative purposes against the fingerprints and facial photographs in all their databases. However, DHA’s draft official identity management policy, released on 22 December 2020, confirms that ABIS will support biometric identification searches (to identify unknown people), and will be “expandable to include additional biometrics such as iris scans, palm and footprints and facial recognition.”¹⁴⁴

132. The DHA has stated they will ensure their FRT is in line with ISO 29794-part 5, the international standard for facial images to ensure they’re of sufficient quality for facial recognition algorithms to work properly.¹⁴⁵ The Daily Maverick noted in 2021 that the current photographs in HANIS do not meet these specifications, nor do SAPS’ mugshots.¹⁴⁶
133. While the DHA continues to make plans for facial recognition with AI integration, South Africa has no legislation regulating police use. In a detailed study about biometric surveillance in South Africa and Kenya, ENACT found that regulations to oversee centralized government biometric databases like ABIS are non-existent in South Africa.¹⁴⁷ Daily Maverick asked SAPS how they would regulate facial recognition searches, and SAPS responded only that they were legally allowed to “perform comparative searches against fingerprint or photographic image databases kept by any other government department for purposes of exclusion or inclusion.”¹⁴⁸ The DHA’s draft identity management policy recognizes “there are no documented and transparent guidelines” regulating how the DHA shares people’s identity data. The policy further acknowledges that the DHA’s information systems security policy isn’t aligned with the Protection of Personal Information Act (“POPIA”). The act regulates how government and private entities use citizens’ personal information, including biometrics. The DHA draft policy recognizes that POPIA isn’t fully enforced but recommends there should be independent oversight with legal powers to “ensure compliance” with the legislation.
134. Regarding policing, it states that the “use (of identity data) for enforcement-related activities must be noted in writing” to “promote accountability.” It suggests any processing of identity data for “crime-related purposes” must be legally authorized, and that the DHA only discloses citizens’ information if there’s a court order. However, the policy suggests that sharing biometric data should be excluded from the court order requirement, and that all personal

¹⁴⁴ Draft Official Identity Management Policy, 22 Dec 2020, https://www.gov.za/sites/default/files/gcis_document/202101/44048gon1425.pdf

¹⁴⁵ Information Technology – Biometric Sample Quality, Part 5: Face image Data, 04 Jan 2010, <https://www.sis.se/api/document/preview/912124>

¹⁴⁶ *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC).

¹⁴⁷ Cybercrime / Who’s watching who? Biometric surveillance in Kenya and South Africa, 11 Nov 2020, <https://enactafrica.org/research/research-papers/whos-watching-who-biometric-surveillance-in-kenya-and-south-africa>

¹⁴⁸ *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC).

information – including biometrics – can be disclosed “in the interest of national security on the approval of the director-general or delegated officials.”

Body Worn Cameras (BWCs), Drones and Closed-Circuit Television (CCTV)

Summary

135. Across all the reports below, a clear global trend emerges: body-worn cameras, drones, and CCTV systems are expanding rapidly as core elements of modern policing and urban management, yet their deployment consistently outpaces the development of effective safeguards for privacy, accountability, and human rights. Governments and police justify these technologies as tools for transparency, efficiency, and crime prevention, but in practice they often concentrate control of surveillance data in the hands of law enforcement, with little or no independent oversight, public consultation, or clarity on when and how recording occurs.
136. These technologies share systemic issues of discretion and opacity, officers decide when to record, what to retain, and who can access footage, creating conditions for selective use, manipulation, and lack of redress. The integration of surveillance tools into public and private networks, often with private companies providing hardware, software, and monitoring services, further blurs lines of accountability and expands the reach of surveillance into everyday life.
137. In combination, body-worn cameras, drones, and CCTV can generate new forms of pervasive and mobile surveillance, capable of recording people in intimate or previously private spaces and monitoring peaceful assemblies. Their presence, especially at protests and other civic gatherings, produces a chilling effect on freedom of expression and the right to assemble by undermining the sense of anonymity in public space.
138. For body-worn cameras used by law enforcement, or in some instances even military personnel, there are regional differences in the policy recommendations civil society actors make. While in Brazil the uninterrupted recording — when implemented with strong and well-defined safeguards — has served as an important mechanism to reduce police lethality and strengthen accountability, in Ireland, body-worn cameras are not seen as necessary or proportional. Regardless of the jurisdiction and potential differing results, the use of these and all technologies, must be always governed by the following principles:
 - must be provided by law
 - must not be arbitrary
 - must pursue legitimate aim
 - must be necessary to achieve the aim in question
 - must be proportionate.
139. Overall, the dominant trend is one of technological expansion without proportional legal, ethical, or democratic safeguards, a shift that transforms tools promoted as enhancing safety

and accountability into mechanisms that risk entrenching state power, weakening transparency, and eroding privacy and civic freedoms.

Australia

140. The City of Melbourne is proposing to expand its closed-circuit television (CCTV) network of 328 cameras (18 of which are privately owned) by an additional 100 cameras. The expansion would see an additional 60 privately owned camera feeds integrated into the public system.¹⁴⁹ For the first time, local law enforcement officers would be able to use the footage from an expanded CCTV network to enforce breaches of minor local laws, like littering, smoking, and busking. The City of Melbourne has indicated its intention to add artificial intelligence and potentially facial recognition technology, into the CCTV system in 2026.¹⁵⁰
141. At the state level, the Victorian Government has also announced plans to ban facial coverings at protests,¹⁵¹ however the full details of the proposal are not yet publicly available. These measures are not formally connected, but in combination they pose a grave risk to the right to peaceful assembly by stripping away anonymity protections for individuals while building an expanded surveillance infrastructure capable of identifying and monitoring demonstrators.
142. The inclusion of additional private camera feeds in the network and the extension of video surveillance powers to local law officers raises further risks. Community legal centres in Victoria have already documented serious problems with the use of contracted security guards and Melbourne City Council Officers to enforce local laws. These include harassment, the confiscation of personal belongings, move-on or dispersal orders and threats of arrest, often directed at people experiencing homelessness or psychosocial distress.¹⁵²
143. Legal experts and service providers have raised concerns that authorising security officers to issue move-on directions, perform citizen's arrests or even use handcuffs not only undermines fundamental rights but also risks unlawful conduct.¹⁵³ These concerns are especially pressing in the context of peaceful assemblies.

¹⁴⁹ Cara Waters, 'Councillors Alarmed at Addition of Private Cameras to City of Melbourne's CCTV Network' *The Age* (online, 22 October 2025)

<<https://www.theage.com.au/national/victoria/councillors-alarmed-at-addition-of-private-cameras-to-city-of-melbourne-s-cctv-network-20251016-p5n2za.html>> accessed 11 November 2025.

¹⁵⁰ Nate Woodall, 'Melbourne City Council to Vote on Expanding CBD CCTV Network' *ABC News* (8 October 2025)

<<https://www.abc.net.au/news/2025-10-08/melbourne-city-council-cctv-security-network-proposed-expansion/105864992>> accessed 11 November 2025.

¹⁵¹ Jacinta Allan, 'Strong Action to Fight Hate and Help Victoria Heal' (Media Release, 17 December 2024) <<https://www.premier.vic.gov.au/strong-action-fight-hate-and-help-victoria-heal>> accessed 11 November 2025.

¹⁵² City of Melbourne, *Submissions to the Future Melbourne Committee, 21 October 2025 (Meeting 5:30pm)* (PDF) <https://mvga-prod-files.s3.ap-southeast-4.amazonaws.com/public/2025-10/OCT25%20FMC%20SUBMISSIONS.pdf> ('Submissions') 10, 26, 87 (accessed 23 October 2025).

¹⁵³ City of Melbourne, *Submissions to the Future Melbourne Committee, 21 October 2025 (Meeting 5:30pm)* (PDF) <https://mvga-prod-files.s3.ap-southeast-4.amazonaws.com/public/2025-10/OCT25%20FMC%20SUBMISSIONS.pdf> ('Submissions') 10, 26, 87 (accessed 23 October 2025).

144. If Melbourne City Council officers are empowered to use surveillance footage from public and private CCTV cameras throughout the city to identify protest participants for minor by-law breaches such as littering or loitering, the result will be the misuse of surveillance to criminalise protest and deter participation. The lack of specialised human rights training for Council officers in managing and responding to civic demonstrations also creates a heightened risk of escalation, discriminatory enforcement and rights violations.
145. These developments have been reported by national media, debated in Council meetings and confirmed in public documents.¹⁵⁴ Civil society organisations, including the Human Rights Law Centre, the Victorian Aboriginal Legal Service, the Victorian Council for Civil Liberties (Liberty Victoria) and Melbourne Activist Legal Support, have raised concerns publicly.¹⁵⁵
146. Authorities have presented a range of justifications for the expansion of Melbourne’s CCTV system and the proposed introduction of artificial intelligence and facial recognition technology. The Lord Mayor of Melbourne has explicitly referred to overseas models, including the United Kingdom and the United States, as evidence that facial recognition can be effective.¹⁵⁶ However, no compelling evidence has been provided to demonstrate that such technology would be necessary or proportionate in Melbourne. Noting that at present, the use of facial recognition remains a proposal.
147. For the expansion of CCTV systems, the Council has relied on the *Victoria Police Sentiment Survey 2024*, a public, state-wide survey initiated by Victoria Police, which reported that residents’ top three safety concerns were “safety in public places”, “safety of my property and possessions” and “drugs and alcohol.” When asked how to improve safety, the most common responses to that survey were “increased police presence”, “more patrols” and “improving community environments such as better lighting on streets or more CCTV.”¹⁵⁷ The Council has also cited its *2024 Neighbourhoods Survey*, where “cleaner streets, waste and graffiti removal” was identified as a top priority, and also community engagement feedback around the

¹⁵⁴ City of Melbourne, ‘Draft Safe City Cameras Policy’ (Web Page) <https://participate.melbourne.vic.gov.au/safe-city-cameras/draft-policy> (accessed 22 October 2025); Nate Woodall, ‘Melbourne City Council to Vote on Expanding CBD CCTV Network’ (ABC News, 8 October 2025) <https://www.abc.net.au/news/2025-10-08/melbourne-city-council-cctv-security-network-proposed-expansion/105864992>; City of Melbourne, ‘Future Melbourne Committee – 21 October 2025’ (Web Page, <https://www.melbourne.vic.gov.au/meeting/future-melbourne-committee-21-october-2025>) (accessed 23 October 2025).

¹⁵⁵ City of Melbourne, *Submissions to the Future Melbourne Committee, 21 October 2025 (Meeting 5:30pm)* (PDF) <https://mvg-prod-files.s3.ap-southeast-4.amazonaws.com/public/2025-10/OCT25%20FMC%20SUBMISSIONS.pdf> (‘Submissions’) 10 (accessed 23 October 2025).

¹⁵⁶ Nate Woodall, ‘Melbourne City Council to Vote on Expanding CBD CCTV Network’ *ABC News* (8 October 2025) <<https://www.abc.net.au/news/2025-10-08/melbourne-city-council-cctv-security-network-proposed-expansion/105864992>> accessed 11 November 2025.

¹⁵⁷ City of Melbourne, ‘Draft Safe City Cameras Policy’ (Web Page) <https://participate.melbourne.vic.gov.au/safe-city-cameras/draft-policy> (‘Draft Policy’) FAQ (accessed 23 October 2025).

Council's *Melbourne2050 Vision* and *Council Plan 2025–2029*, which highlighted cleanliness and city presentation as strong themes.¹⁵⁸ These responses are being used to justify expanding the CCTV system from its original purposes of assisting emergency services, including Victoria Police, in crime detection to include monitoring and enforcement of local laws.

148. While these justifications focus on urban amenity and efficiency, they ignore the risks that arise when a system designed for crime prevention is repurposed to monitor everyday behaviour. Expanding surveillance into the realm of by-law enforcement opens the door to its use against assemblies and protests, where gatherings may easily be recast as “nuisance” or “public order” problems that require a legal response. This risks chilling participation in demonstrations in Melbourne’s central civic spaces.
149. Victoria does have a *Charter of Human Rights and Responsibilities* which requires public authorities, including local government, to act compatibly with rights such as privacy, the freedom of expression, the rights to peaceful assembly and association, among others. Yet the Council’s record on transparency and accountability in the operation of its CCTV program undermines confidence that these obligations are being met.¹⁵⁹
150. Despite the CCTV program operating for decades, its governing policy framework has never previously been made publicly available, until now.¹⁶⁰ The explanation offered was that the policies governing the CCTV program contained sensitive operational information that could not be made public.¹⁶¹ This is unconvincing, as the policy and operating procedures could have been separated at any time. The failure to do so has left the public without clarity about how surveillance in the City of Melbourne has been governed in practice.
151. Some private building owners already have their cameras integrated into the Council’s monitoring network. While Council officers may access the footage, ownership of the cameras remains with the private operators. This creates serious accountability gaps, particularly around data retention and secondary use. Under public questioning, Melbourne City Council officers were unable to answer whether footage from private cameras was retained by the camera’s owners and whether or not it was subject to the Melbourne City Council’s policy

¹⁵⁸ City of Melbourne, ‘*Draft Safe City Cameras Policy*’ (Web Page) <https://participate.melbourne.vic.gov.au/safe-city-cameras/draft-policy> (‘Draft Policy’) FAQ (accessed 23 October 2025).

¹⁵⁹ Interview with Cr Olivia Ball, *ABC Radio Melbourne Drive* (23 October 2025, 5–11 min) <<https://www.abc.net.au/listen/programs/melbourne-drive/drive/105910364>> accessed 11 November 2025.

¹⁶⁰ City of Melbourne, *Council Meeting Papers* (2 October 2025) <<https://mvga-prod-files.s3.ap-southeast-4.amazonaws.com/public/2025-09/OCT25%20FMC1%20AGENDA%20ITEM%206.3.pdf>> accessed 11 November 2025.

¹⁶¹ City of Melbourne, ‘*Draft Safe City Cameras Policy*’ (Web Page) <<https://participate.melbourne.vic.gov.au/safe-city-cameras/draft-policy>> (‘Draft Policy’) FAQ (accessed 23 October 2025).

regarding storage, access and retention.¹⁶² The CCTV policy published for the first time in 2025 and subject to public consultation does not mention the private cameras at all.¹⁶³

152. Private contractors are employed by the City of Melbourne to monitor CCTV footage 24 hours a day and they liaise with Victoria Police, emergency services, and other parties requesting footage. This service was formerly provided by Securecorp, however National Protective Services commenced a 7-year contract for this monitoring in May 2024.¹⁶⁴ Technology vendors would also be directly involved in any future rollout of AI analysis.
153. If facial recognition or other AI tools are embedded in the city's CCTV network, and protestors are simultaneously denied the ability to cover their faces, people gathering in public will be easily identifiable, traceable and at risk of reprisal. This prospect alone will deter individuals from exercising their right to peaceful assembly, particularly those from communities that already experience over-policing or harassment.

Brazil

154. In Brazil, Conectas Human Rights has been closely monitoring the implementation of the "Olho Vivo" program,¹⁶⁵ which introduced body-worn cameras for police officers in the state of São Paulo, resulting in a significant reduction in both police lethality and officer fatalities. Despite successfully defending against attempts by the state governor to terminate the program—including actions monitored by the Supreme Court—current proposals still risk undermining the use of body cameras. These proposals threaten to shift from a policy focused on controlling police lethality to one centered on facial recognition technology, which would compromise transparency, privacy, and exacerbate racial bias, particularly since cameras fail to activate in 70% of incidents.
155. A study released in May 2023 by the Brazilian Forum on Public Safety indicates that in São Paulo, deaths resulting from interventions by on-duty military police decreased by 62.7%, with the majority (76.2%) occurring in battalions participating in the body camera program. Police fatalities in São Paulo also dropped by 62.7%, from 697 deaths in 2019 to 260 in 2022,

¹⁶² Melbourne City Council, *Livestream Video Recording of Future Melbourne Committee Meeting* (7 October 2025) at 1:53:00

<<https://www.melbourne.vic.gov.au/meeting/future-melbourne-committee-07-october-2025>> accessed 11 November 2025.

¹⁶³ City of Melbourne, 'Draft Safe City Camera Program Policy' (7 October 2025)

<<https://mvga-prod-files.s3.ap-southeast-4.amazonaws.com/public/2025-09/OCT25%20FMC1%20AGENDA%20ITEM%206.3.pdf>> 8–12 accessed 11 November 2025.

¹⁶⁴ City of Melbourne, *Safe City Cameras Program Audit Committee Annual Report 2024* (May 2025) 7

<<https://mvga-prod-files.s3.ap-southeast-4.amazonaws.com/public/2025-05/sccp-audit-committee-annual-audit-report-2024.pdf>> accessed 11 November 2025.

¹⁶⁵ Conectas, *Body cameras: Conectas denounces dismantling of the "Olho Vivo" program at the UN* (26 June 2024)

conectas.org/en/noticias/body-cameras-conectas-denounces-dismantling-of-the-olho-vivo-program-at-the-un/ accessed 19 November 2025.

according to research conducted by the United Nations Children’s Fund (UNICEF) and the Brazilian Forum on Public Safety.

156. Conectas emphasizes the urgent need for the Brazilian government to ensure the broad implementation of body-worn cameras across police forces. In particular, the state of São Paulo must reinstate policies that guarantee both the control of police lethality and the protection of officers through continuous, automatic recording and independent data storage, coupled with strict accountability for non-compliance. These measures are essential to safeguard lives and build public trust in law enforcement.

Canada

157. Canadian policing agencies have been using drones at political protests since when the Royal Canadian Mounted Police (RCMP) deployed drones as part of Operation GRIZZLY to monitor protestors at the 2002 G8 summit.¹⁶⁶ While it is clear that drones have been used extensively to monitor political protests in Canada,¹⁶⁷ it remains difficult to document specific instances or to fully document the practice.
158. Adoption and use of drones in Canada is plagued by transparency and accountability challenges. Some provinces adopt the surveillance technologies without any public discussion or policy in place, while others have indicated their willingness to depart from policies when convenient.¹⁶⁸
159. In other instances, drones are regularly used to monitor peaceful protests even where law enforcement policies prohibit their use for surveillance purposes or to record peaceful protestors.¹⁶⁹ Attempts to challenge drone use at political protests through police

¹⁶⁶ Information and Privacy Commissioner of Ontario, *The Existing and Emergent State of UAV/RPAS/Drones Surveillance Capacities and Law Enforcement* (9 April 2025)

<https://www.ipc.on.ca/en/resources/research-hub/drones-surveillance-capacities-and-law-enforcement> accessed 28 October 2025

¹⁶⁷ CBC News, ‘Eye in the Sky: Police Drones’ (CBC NewsInteractives, 23 April 2023)

<https://www.cbc.ca/newsinteractives/features/police-drones> accessed 31 October 2025.

¹⁶⁸ Greer D, “Drones helped in big Vancouver arrest. It’s time for policy scrutiny, researchers say”, *The Canadian Press*, 6 September 2024)

https://www.thecanadianpressnews.ca/politics/drones-helped-in-big-vancouver-arrest-its-time-for-policy-scrutiny-researchers-say/article_b30b03ae-faa3-5301-9227-32ab16b0aa09.html accessed 31 October 2025;

Abby O’Brien, “‘Just fly a drone over’: Suggestion on encampment response at U of T Council meeting sparks privacy concerns for protesters, advocates”, *CTV News Toronto* (18 July 2024)

<https://www.ctvnews.ca/toronto/article/just-fly-a-drone-over-suggestion-on-encampment-response-at-u-of-t-council-meeting-sparks-privacy-concerns-for-protesters-advocates/> accessed 18 September 2025.

¹⁶⁹ Pivot Legal Society, ‘VPD Surveillance of Demonstrators Supporting Palestinian Human Rights’ (2025)

<https://www.pivotlegal.org/vpd_surveillance_of_demonstrators_supporting_palestinian_human_rights>

accessed 11 November 2025. BC Civil Liberties Association, ‘Press Release: Vancouver Police Board Handling of Surveillance Complaint Raises Oversight Concerns’ (18 September 2025)

<<https://bccla.org/2025/09/press-release-vancouver-police-board-handling-of-surveillance-complaint-raise-s-oversight-concerns/>> accessed 31 October 2025.

accountability mechanisms have met with resistance and deeply flawed processes.¹⁷⁰ These accountability mechanisms have wholly disregarded any chilling impact that the use of drones may have on protest participants who have experienced marginalization and persecution in the past and are legitimately wary of police surveillance.¹⁷¹

160. A case in point is the Vancouver Police Department's (VPD) use of an array of video and audio surveillance capabilities to monitor Palestine solidarity protests. This surveillance involves use of drones, police body-worn cameras and hand-held recording devices.
161. The use of extensive video surveillance at Palestine solidarity protests is particularly problematic in light of the heightened chilling effect that overt surveillance will have on protest participants and in light of the aggressive approach to Palestine solidarity taken by policing agencies in Canada more generally.
162. Despite this chilling effect, and the fact that unlawful activity is only alleged to occur at less than 5% of Palestine solidarity protests, almost 70% of all VPD drone deployments at public events in 2024 related to Palestine solidarity protests. VPD policies do not consider the implications of surveillance on protest participants with a history of oppression and persecution when assessing whether to deploy surveillance techniques.
163. VPD's use of drones at political protests is additionally problematic as its policy on the use of drones does not anticipate use of the intrusive surveillance mechanisms at demonstrations. Indeed, VPD's policies prohibit the use of drones for surveillance purposes in the absence of judicial authorization or a threat to life. Its policies also prohibit the use of drones for recording or identifying people at peaceful protests. Nonetheless, VPD's use of drones at protests is extensive.
164. A complaint was filed by the British Columbia Civil Liberties Association (BCCLA) and Pivot Legal Society asking VPD to consider the chilling effects of its surveillance practices on participants in Palestine solidarity protests as well as to consider whether its surveillance

¹⁷⁰Pivot Legal Society, 'VPD Surveillance of Demonstrators Supporting Palestinian Human Rights' (2025) <https://www.pivotlegal.org/vpd_surveillance_of_demonstrators_supporting_palestinian_human_rights> accessed 11 November 2025. BC Civil Liberties Association, 'Press Release: Vancouver Police Board Handling of Surveillance Complaint Raises Oversight Concerns' (18 September 2025) <<https://bccla.org/2025/09/press-release-vancouver-police-board-handling-of-surveillance-complaint-raise-s-oversight-concerns/>> accessed 31 October 2025.

¹⁷¹ Pivot Legal Society, 'VPD Surveillance of Demonstrators Supporting Palestinian Human Rights' (2025) <https://www.pivotlegal.org/vpd_surveillance_of_demonstrators_supporting_palestinian_human_rights> accessed 11 November 2025. BC Civil Liberties Association, 'Press Release: Vancouver Police Board Handling of Surveillance Complaint Raises Oversight Concerns' (18 September 2025) <<https://bccla.org/2025/09/press-release-vancouver-police-board-handling-of-surveillance-complaint-raise-s-oversight-concerns/>> accessed 31 October 2025.

practices aligned with its policies. This complaint met with severe procedural and substantive flaws, and reaffirmed VPD's ongoing practices.¹⁷²

Ireland

165. In Ireland, the law explicitly provides for the use of body-worn cameras as a type of 'recording device'. ICCL has been, and is, concerned by the significant gap between the Government¹⁷³ and Garda¹⁷⁴ perceptions of the effectiveness of body-worn cameras as a tool for accountability and transparency and actual evidence of their effectiveness in respect of these goals.¹⁷⁵
166. Eleven years after the fatal shooting of unarmed Black teenager Michael Brown by police officer Darren Wilson in Ferguson, Missouri in the United States largely prompted the mass roll-out of body-worn cameras in the US,¹⁷⁶ followed by a wider uptake in other jurisdictions worldwide including London,¹⁷⁷ It is ICCL's position that the jury is out on whether body-worn

¹⁷² BC Civil Liberties Association, 'Press Release: Vancouver Police Board Handling of Surveillance Complaint Raises Oversight Concerns' (18 September 2025)

<<https://bccla.org/2025/09/press-release-vancouver-police-board-handling-of-surveillance-complaint-raise-s-oversight-concerns/>> accessed 31 October 2025; Pivot Legal Society, 'VPD Surveillance of Demonstrators Supporting Palestinian Human Rights' (2025)

<https://www.pivotlegal.org/vpd_surveillance_of_demonstrators_supporting_palestinian_human_rights> accessed 11 November 2025.

¹⁷³ In June 2019, the then Irish Minister for Justice Charlie Flanagan announced that the Cabinet had approved the drafting of legislation for BWCs. In this press release, the Minister stated that: "The use of BWCs by modern police services around the world has increased dramatically over the last five years or so. The evidence available suggests that they can greatly improve police frontline capability with the accurate recording of incidents. They provide a contemporaneous evidence capture and a clear unambiguous record of particular events and interactions such as at public order protests. Their deployment can lead to an increase in admissions and early guilty pleas. Most importantly, their usage may increase public trust and build confidence in policing generally." Press Release, Department of Justice, Equality and Law Reform, 25 June 2019, <http://www.justice.ie/en/JELR/Pages/PR19000170>

¹⁷⁴ Use of body cameras proposed for gardaí, 26 June 2019,

<https://www.lawsociety.ie/gazette/top-stories/2019/06-june/use-of-body-cameras-by-gardai-is-proposed/>

¹⁷⁵ Research on BWCs, What we know, what we need to know, Cynthia Lum, Megan Stoltz, Christopher S. Koper, J. Amber Scherer, George Mason University, Criminology and Public Policy, March 2019, accessed here:

https://www.researchgate.net/publication/331981847_Research_on_body-worn_cameras; Police Officer

BWCs: Assessing the Evidence, Michael D. White, 2014, Washington, DC: Office of Community Oriented

Policing Services, accessed here: <https://cops.usdoj.gov/RIC/Publications/cosp289-pub.pdf>; "There have

been nearly 40 studies on the use of body cameras, including a dozen randomised controlled trials on the

magnitude of their effect on policing. Despite all this work, it's still not entirely apparent why these cameras

are helpful, under what conditions, or for whom". Do Police Body Cameras Really Work? Barak Ariel, IEEE

Spectrum, 4 May 2016,

<https://spectrum.ieee.org/consumer-electronics/portable-devices/do-police-body-cameras-really-work>;

Yokum, D., et al, A randomized control trial evaluating the effects of police BWCs, PNAS, May, 2019,

<https://www.pnas.org/doi/full/10.1073/pnas.1814773116>

¹⁷⁶ Hermann, P. and Weiner, H., Issues over police shooting in Ferguson lead push for officers and body

cameras, 2 December 2014,

https://www.washingtonpost.com/local/crime/issues-over-police-shooting-in-ferguson-lead-push-for-office-rs-and-b-ody-cameras/2014/12/02/dedcb2d8-7a58-11e4-84d4-7c896b90abdc_story.html

¹⁷⁷ Metropolitan Police, Roll-out of body worn cameras, Oct 2017

<http://news.met.police.uk/news/rollout-of-body-worn-cameras-191380>

cameras have had a positive impact on policing.¹⁷⁸ At the same time, there are some indications, in the US at least, that body-worn cameras may be primarily used to serve the interests of police as opposed to the people they have sworn to serve,¹⁷⁹ mainly due to issues over who controls the material recorded. Specifically, the issues pertaining to the use of body-worn cameras include, but are not limited to:

- Police discretion over their use;
- Police discretion over when a camera is specifically turned on and off;
- Police control over disclosure, or nondisclosure, of the audio and video material recorded to people recorded, victims of force or victims' families, or media;
- Access to redress in instances of misuse or abuse of data;
- Lack of independent oversight or review; and
- Lack of transparency and accountability.

167. ICCL believes these issues will likely arise in Ireland in respect of body-worn cameras (but also in respect of the other aforementioned tools and measures) because the Code of Practice for Garda use of body-worn cameras makes it clear that control of the body-worn camera-recorded footage and audio material will rest solely in the hands of An Garda Síochána, while the gardaí who make the recordings will decide whether or not the footage or audio material is evidential or non-evidential (leading to its deletion). Moreover, gardaí will decide under what circumstances or in which situations to use a body-worn camera, when to turn it on, when to turn it off, when material may be released to media, and to whom it may be released; while if/when a person asks a Garda to stop recording them or, in other circumstances, to record them, discretion is left up to the Garda member.

168. In addition, body-worn cameras are more intrusive than other forms of static surveillance such as CCTV because they can record a person at very close range, and can record in places where there is no CCTV, such as homes or other private spaces. If the Irish public forms an expectation that all interactions with the gardaí will be automatically recorded, by body-worn

¹⁷⁸ Prior to their introduction, the Irish Government said they wanted to introduce BWCs in order to increase frontline policing capability and improve the criminal justice outcomes. At the time, having conducted an assessment of research carried out in other jurisdictions where BWCs had been introduced, ICCL did not find consistent, conclusive or convincing evidence that BWCs had led to better policing or that evidence of crimes gathered by such cameras have generated better outcomes in the criminal justice system. In fact, ICCL found that flagship research carried out in Rialto, California - often cited to prove the benefits of BWCs by governments, police forces and those that stand to profit from the roll out of BWCs - has since been significantly undermined by other, larger research projects and by that study's own authors. See Doireann Ansbro, *Re: BWCs for An Garda Síochána* (Irish Council for Civil Liberties, 2019) <<https://www.iccl.ie/wp-content/uploads/2019/10/ICCL-Body-Worn-Cameras-DoJ-submission.pdf>> accessed 11 November 2025; Cynthia Lum, Christopher S Koper, Michael Stoltz and James A Schere, 'Research on Body-Worn Cameras: What We Know, What We Need to Know' (2019) *Criminology and Public Policy* 99; National Institute of Justice, 'Research on Body-Worn Cameras and Law Enforcement' (January 2022) <<https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement#note3>> accessed 11 November 2025.

<https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement#note3>

¹⁷⁹ Eric Umansky, 'How Police Have Undermined the Promise of Body Cameras' *ProPublica* (December 2023) <<https://www.propublica.org/article/how-police-undermined-promise-body-cameras>> accessed 11 November 2025; Noel Titheradge, 'Police Officers Widely Misusing BWCs' *BBC News* (September 2023) <<https://www.bbc.com/news/uk-66809642>> accessed 11 November 2025.

cameras, or drones or any other ‘recording device’, then in addition to potentially infringing privacy rights, freedom of expression may also suffer as people may choose to modify their behaviour.

169. It is for these reasons that ICCL has been continually calling on the Minister for Justice to reveal how the pilot scheme will empirically measure the impact of body-worn cameras on Garda accountability, criminal justice processes, equality and human rights, and how it is expected to demonstrate the alleged benefits of body-worn cameras in the Irish context before any national roll-out of the same.¹⁸⁰
170. ICCL, believes pilot schemes for every specific ‘recording device’ should similarly be carried out and codes of practice created and/or amended to address the issues that arise during each pilot scheme as a means to safeguard against infringements of rights, including the right to protest, and to address the concerns outlined above.

South Africa

171. In 2022, Gauteng Province Premier Panyaza Lesufi was reported saying he intended to launch a wide-ranging network of surveillance cameras.²⁸ In addition, the surveillance network would include 500 drones, a high-performance police car in every ward, and eight helicopters.¹⁸¹ This project was an extension of Vumacam, a private-business project who, as of 2022, had already installed 1,850 cameras throughout Johannesburg. At the time of its conception, the plan was first to be rolled out in townships as more affluent suburbs already had private security and neighborhood watches.¹⁸²
172. In June 2022, Vumacam invested an additional R60 million to expand their security camera network and rolled-out 350 cameras in Alexandra, Soweto, and Diepsloot.¹⁸³ At the same time, Vumacam also announced its support for the Eyes and Ears Initiative (E2) — a coordinated joint crime-fighting initiative between the South African Police Service, Business Against Crime South Africa, and the private security industry.

¹⁸⁰ Irish Council for Civil Liberties ‘Bodyworn Cameras Pilot Must Ensure Fundamental Rights Are Protected – ICCL’ (ICCL, 30 October 2023) <https://www.iccl.ie/press-release/bodyworn-cameras-pilot-must-ensure-fundamental-rights-are-protected-iccl/> accessed 5 November 2025.

¹⁸¹ ‘Plans for Biometric Surveillance Reach Epic Scales with Off-Putting Implications’ *Biometric Update* (November 2022) <<https://www.biometricupdate.com/202211/plans-for-biometric-surveillance-reach-epic-scales-with-off-putting-implications>> accessed 11 November 20

¹⁸² *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC).

¹⁸³ ‘Vumacam Invests R60 Million to Expand Security Camera Network — Including Alexandra and Soweto’ *MyBroadband* (25 June 2022) <<https://mybroadband.co.za/news/security/450236-vumacam-invests-r60-million-to-expand-security-camera-network-including-alexandra-and-soweto.html>> accessed 11 November 2025.

173. As of February 2024, Gauteng has now launched almost 7,000 surveillance cameras across the province that are equipped with FRT.¹⁸⁴ This network is a partnership with Vumacam and uses the company's network of existing cameras, including over 6,000 Vumacam cameras in Gauteng and access to the company's 5,000 partner cameras across South Africa. The Gauteng Department of e Government is another stakeholder in this partnership and has stated their mandate is to ensure that technology bolsters the immediate fight against crime, corruption, vandalism, and lawlessness.¹⁸⁵ According to Vumacam, the partnership builds on the success of its existing public sector collaborations which employ its advanced technology, including the Integrated Intelligence Operations Centre, which sees the group work with the Johannesburg Metro Police Department.
174. More recently, Vumacam has stated it will require Gauteng public officials who view their CCTV cameras to undergo the same training and testing as their private security officers.¹⁸⁶ An investigation by Daily Maverick in August 2023 showed that the initial deployment of the CPWs was unlawful, as it would have required a formal request and approval from the Minister of Justice.¹⁸⁷ Vumacam also reiterated that those appointed to monitor cameras are not able to access their feeds at any time. Vumacam has stated they use dark screen technology, which only brings up a camera feed when AI-powered systems detect an incident that triggers an alert. Vumacam said in cases where a feed is requested to investigate a particular incident, the Gauteng Provincial Government must go through the same approval and submit the same documentation as private security companies.
175. Vumacam said, "This footage is then stored in a secure vault which may only be accessed by those with relevant need and approval to do so. Where any user to observe feeds on one or

¹⁸⁴ Gauteng Premier Panyaza Lesufi Launches Almost 7000 Facial Recognition Cameras' *Briefly News* (13 February 2024)

<<https://briefly.co.za/south-africa/180039-gauteng-premier-panyaza-lesufi-launches-7000-facial-recognition-cameras/>> accessed 11 November 2025; 'Expansive Facial Recognition Surveillance Coming to Hong Kong, Bahrain, South Africa' *Biometric Update* (12 February 2024)

<<https://www.biometricupdate.com/202402/expansive-facial-recognition-surveillance-coming-to-hong-kong-bahrain-southafrica>> accessed 11 November 2025; 'Big Brother Hits Gauteng Streets as Lesufi, Vumacam Roll-Out 6,000 CCTV Cameras to Fight Crime' *IOL* (14 February 2024)

<<https://www.iol.co.za/news/big-brother-hits-gauteng-streets-as-lesufi-vumacam-roll-out-6000-cctv-cameras-to-fight-crime-b0e30a1e-4ad8-430b-a683-c3a0cb8d42aa>> accessed 11 November 2025.

¹⁸⁵ 'Vumacam Announces Crime-Fighting Partnership with Gauteng Government' *Moneyweb* (13 February 2024)

<<https://www.moneyweb.co.za/news/companies-and-deals/vumacam-announces-crime-fighting-partnership-with-gauteng-government/>> accessed 11 November 2025; 'Gauteng Taps into Vumacam's Tech to Fight Crime' *ITWeb* (14 February 2024)

<<https://www.itweb.co.za/article/gauteng-taps-into-vumacams-tech-to-fight-crime/KWEBb7yLPQLvmRjO>> accessed 11 November 2025.

¹⁸⁶ 'Vumacam Training Controversial Gauteng Crime Wardens' *MyBroadband* (6 March 2024)

<<https://mybroadband.co.za/news/security/527745-vumacam-training-controversial-gauteng-crime-wardens.html>> accessed 11 November 2025.

¹⁸⁷ 'Gauteng's Crime Prevention Wardens Were Set Up Unlawfully, Risk Abuse of Police Powers – Experts' *Daily Maverick* (29 August 2023)

<<https://www.dailymaverick.co.za/article/2023-08-29-gauteng-crime-prevention-wardens-set-up-unlawfully-experts/>> accessed 11 November 2025.

more cameras without valid cause for doing so, this would be flagged by our systems.”¹⁸⁸ In addition, Vumacam said it had rigorous controls and two-factor authentication to ensure that all system usage was regulated, monitored and audited, stating, “[i]f any system abuse was to take place, it would be flagged and immediately investigated. Any necessary legal recourse would follow.” Vumacam added that its systems and technology were compliant with the Protection of Personal Information Act and subjected to regular penetration testing, and “[w]hile nefarious attempts or abuse of a system are plausible on any systems or technology, Vumacam’s systems are the most advanced in terms of CCTV security and privacy in South Africa, if not the world.”¹⁸⁹

176. Vumacam has partnered with the Chinese company Hikvision and the Swedish company Axis Communications to provide the hardware while iSentry and Milestone, a popular Denmark-based video surveillance management tool, provide the software.¹⁹⁰ Vumacam has teamed up with private agencies patrolling wealthier residential areas and erected poles with high-definition cameras where they wanted on top of Johannesburg’s fiber network.
177. A Vumacam representative states that after 48 hours, if a license plate in the shared database still doesn’t have a case number, it’s automatically deleted. However, there’s no transparency or mechanism for public accountability about how thoroughly this cleaning is done; nor is the same process applied to plates stored in each user’s private database, meaning any plate number could be added without any vetting. As a result, cars could be monitored and pulled over for erroneous or illegitimate reasons.
178. The integration of social services biometrics, policing and facial recognition technologies poses a significant risk for activists, journalists and the like. This push for AI driven surveillance gives the power to the State to stamp down on political unrest and continue to dissuade the people from challenging their authority.

Cyber Patrolling/Social Media Monitoring

Summary

179. Social media networks are a widely available and well-used resource for organising or responding to calls to participate in protest actions. At the same time, they are also used by

¹⁸⁸ ‘Vumacam Training Controversial Gauteng Crime Wardens’ *MyBroadband* (6 March 2024) <<https://mybroadband.co.za/news/security/527745-vumacam-training-controversial-gauteng-crime-wardens.html>> accessed 11 November 2025.

¹⁸⁹ ‘Vumacam Training Controversial Gauteng Crime Wardens’ *MyBroadband* (6 March 2024) <<https://mybroadband.co.za/news/security/527745-vumacam-training-controversial-gauteng-crime-wardens.html>> accessed 11 November 2025.

¹⁹⁰ ‘Vumacam Invests R60 Million to Expand Security Camera Network — Including Alexandra and Soweto’ *MyBroadband* (25 June 2022) <<https://mybroadband.co.za/news/security/450236-vumacam-invests-r60-million-to-expand-security-camera-network-including-alexandra-and-soweto.html>> accessed 11 November 2025.

policing institutions as a form of 'open-source intelligence', which involves extracting and analysing publicly available data.¹⁹¹ Advances in computing have enabled this practice to expand rapidly, allowing for the automated collection and analysis of vast amounts of information.¹⁹² In INCLO member countries, the use of social media monitoring in this way has, in some cases, interfered with individuals' ability to actively protest or has led to significant legal consequences.¹⁹³

180. Across the reports below, a consistent global trend emerges: cyber-patrolling and social media monitoring are increasingly being institutionalized as state surveillance tools, justified under the guise of national security, public order, or combating disinformation, but frequently used to monitor, profile, and suppress dissent, activism, and journalism. These practices are expanding without adequate legal safeguards, transparency, or oversight, often relying on vague or outdated regulations and advanced technologies such as AI and machine learning. Governments and security forces routinely collect, analyze, and share personal data from online platforms, blurring the line between legitimate intelligence and political control. This unchecked expansion has led to systematic violations of privacy, discrimination against marginalized or dissenting voices, and a chilling effect on freedom of expression and protest, while private technology companies amplify these risks through opaque data practices and political microtargeting.

Argentina

181. In 2024, the National Ministry of Security issued Resolution 428/2024¹⁹⁴ to strengthen the capacities of the federal security forces in the fight against cybercrime. The Resolution directs the federal police and security forces to carry out preventative police work by conducting searches of information publicly accessible on the Internet (Art. 1). The Resolution lists a series of areas that such investigations would focus on, including human trafficking, asset laundering, and terrorism, as well as other broad categories, such as "threats and other forms of intimidation or coercion" and "any other crime that may be reported through cyberspace" (Art. 2).

¹⁹¹ Ashok Yadav, Atul Kumar and Vrijendra Singh, 'Open-Source Intelligence: A Comprehensive Review of the Current State, Applications and Future Perspectives in Cyber Security' (2023) 56(11) *Artificial Intelligence Review* 12407 <<https://dl.acm.org/doi/abs/10.1007/s10462-023-10454-y>> accessed 11 November 2025.

¹⁹² Riccardo Ghioni, Mariarosaria Taddeo and Luciano Floridi, 'Open Source Intelligence and AI: A Systematic Review of the GELSI Literature' (January 2023) *AI & Society* <https://www.researchgate.net/publication/367510276_Open_source_intelligence_and_AI_a_systematic_review_of_the_GELSI_literature> accessed 11 November 2025.

¹⁹³ International Network of Civil Liberties Organisations (INCLO), *Spying on Dissent: Surveillance Technologies and Protest* (June 2019) <https://inclo.net/publications/spying-on-dissent-surveillance-technologies-and-protest/> accessed 11 November 2025.

¹⁹⁴ Argentina, *Resolution 428/2024 – Cybercrime Prevention Protocol Boletín Oficial de la República Argentina* (28 May 2024) <<https://www.boletinoficial.gob.ar/detalleAviso/primera/308291/20240528>> accessed 11 November 2025.

182. The Resolution expressly provides for the use of artificial intelligence (AI) and states that its use "will be strictly adjusted to the needs of the activity regulated in this protocol," and supervised by the Ministry of Security. It does not clearly indicate what limits will be imposed on the use of artificial intelligence in the federal police's open-source intelligence (OSINT) gathering tasks. Based on responses to public information requests, there is no evidence the State will be conducting any impact or risk assessments before implementing this technology across the country. By failing to conduct such an analysis, Argentina is not complying with its obligations under Convention 108+ on data protection, to which it is a State Party.¹⁹⁵
183. CELS has scant information on the specific kinds of technology that will be used pursuant to this Resolution. Through an information request made months after the Resolution's publication, CELS asked the Ministry to report on the technologies that will be used and what mechanisms exist for their control. CELS also asked how the technologies will be acquired and requested that records and work meetings, technical reports on purchasing units, and details of the officials dedicated to designing the technical requirements be shared. The Ministry of Security did not provide any answers to these specific questions; the Ministry only stated that it had not yet acquired these tools.
184. There are also questions as to how this Resolution will comply with the Personal Data Protection Law (No. 25.326). Through cyber-patrolling tasks, the State will necessarily collect substantial amount of personal data, which affects the right to privacy. Under the current law, the state is prohibited from processing sensitive data and publications made by children and adolescents without judicial authorization. In the information request, CELS inquired on how the Ministry of Security would ensure compliance. In its response, the State only indicated that the tools to "adapt to the regulations" were still being built.
185. More recently, in June and July 2025, the National Government modified the organic laws of all federal police and security forces and the Federal Penitentiary System by decree.¹⁹⁶ These reforms similarly authorized the different forces to carry out cyber-patrolling tasks. Under the new rules, without a prior judicial order, the forces may carry out "crime prevention tasks in digital public spaces, such as open social networks, public websites, and other open sources..." Together with Resolution 428/2024, these reforms provide the police with sweeping surveillance powers without any significant controls. This new police spying apparatus has not been considered by Congress and represents a serious threat to civil society groups throughout Argentina.

¹⁹⁵ Argentina, *Approval of the Amending Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+)*, Rule No. 375738 (30 November 2022) <<https://servicios.infoleg.gob.ar/infolegInternet/anexos/375000-379999/375738/norma.htm>> accessed 11 November 2025.

¹⁹⁶ Centro de Estudios Legales y Sociales (CELS), *Fuerzas federales: reformas que ponen derechos en riesgo* (17 July 2025) <<https://www.cels.org.ar/web/2025/07/fuerzas-federales-reformas-que-ponen-derechos-en-riesgo/>> accessed 11 November 2025.

186. There were also suspected surveillance of social organizations through cyber-patrolling. In August 2025, reports were received of various situations where Buenos Aires city police appeared at closed meetings held at the headquarters of various unions and political organizations. The officers would not seek to break up the meetings, but would instead ask questions such as the number of people attending the meeting and the organizations that were present. The obvious intent of these actions was to make it known that the groups were being watched by the police.
187. Specifically, these intimidation tactics have been used at an assembly of the feminist collective Ni Una Menos, at the University of Buenos Aires Teachers' Union Assembly, at a meeting concerning Palestinian rights that took place at one of the offices of the Socialist Workers' Party, and at a meeting of workers from the Garrahan Hospital. In one of these meetings, CELS received information that one of the police officers who showed up stated that they had become aware of the meeting through the Cyber-Patrolling Division. CELS cannot confirm this, but in all of the cases, the information about these meetings had circulated on social networks.
188. After these incidents, CELS sent a request for information to the City's Ministry of Security. In its response, the authorities acknowledged that the police interventions in all cases were ordered based on information produced by the Cyber-patrolling Division and forwarded to the Superintendent of Operations, resulting from the "collection of information from open and publicly accessible sources." According to the Ministry itself, the purpose of these surveys was to identify "gatherings" that could affect "vehicular traffic or public transportation."
189. At the same time, the official response admitted that there was no criminal hypothesis or ongoing judicial investigation, and that the City Police do not have any protocol or specific regulation governing cyber-patrolling activities.
190. The government's response thus confirms that the police presence at the assemblies was triggered as a result of preventive cyber-patrolling activities based on vague criteria, such as "public order," "general security," and "traffic", and carried out without a judicial order, protocol, or specific regulatory framework. This kind of preventive surveillance, lacking a legitimate defined purpose or prior judicial oversight, constitutes an unlawful interference with the exercise of the rights to privacy, freedom of expression, and freedom of assembly.
191. When CELS previously inquired about cyber-patrolling activities by the City Police in September 2024, the force stated that they did not have any specific regulation on cyber-patrolling and therefore, where applicable, adopted the recommendations established by Resolution No. 2024-428-APN-MSG (the resolution discussed above concerning federal forces). The City Police Superintendent for the Fight Against Cybercrime indicated, however, that their cyber-patrolling was not conducted using automated tools. The Superintendent further noted that cyber-patrolling activities were carried out as investigative actions, based

on a specific criminal hypothesis, within the framework of a judicial investigation and in coordination with the agency leading the case investigation.

192. To this day, the suspicion persists that the City Police, through cyber-patrolling investigations, continue to monitor meetings of social, union, and political organizations.

Canada

193. Cyber-patrolling or Open Source Intelligence (OSI) gathering is intended to include monitoring of publicly available sources. In practice, OSI will frequently include access to personal data that is not public or that has been made publicly available through unlawful means. Even when limited to publicly available personal data, OSI can be intrusive, and will frequently rely on various algorithmic systems to surveil public interactions *en masse*.
194. Canadian policing agencies have used a variety of tools that they characterize as OSI in nature including for monitoring of political protests. A municipal police agency, Calgary Police Services, historically used a commercial social media monitoring tool called Media Sonar for a number of purposes including to monitor for “upcoming protests”, but no longer uses the service.¹⁹⁷ The Royal Canadian Mounted Police have employed a number of social media monitoring programs directed at protestors. One historic program (Project Sitka) used social media monitoring as well as a risk assessment tool to create a “watchlist” of prominent indigenous protestors.¹⁹⁸ The RCMP also historically used a commercial tool that bypassed social media site’s privacy settings in order to extract targeted accounts’ hidden social media contacts.¹⁹⁹
195. Project Sitka was the RCMP’s watchlist of key indigenous protest participants which it created in the wake of a growing political movement of indigenous rights activists that included protests regarding resource extraction, unchecked violence targeting indigenous women, and unresolved land claims. The RCMP presented the program as a response to emerging changes in political protest through more diffuse organization techniques inherent in social media dynamics.

¹⁹⁷ Kate Robertson, Cynthia Khoo and Yolanda Song, *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* (Citizen Lab and International Human Rights Program, September 2020) 58 <<https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf>> accessed 11 November 2025.

¹⁹⁸ Jeffrey Monaghan and Brendan Howe, ‘Strategic Incapacitation of Indigenous Dissent’ (2018) <<https://www.sfu.ca/~palys/Howe&Monaghan-2018-StrategicIncapacitationOfIndigenousDissent.pdf>> accessed 11 November 2025.

¹⁹⁹ Office of the Privacy Commissioner of Canada, *Special Report to Parliament: Investigation of the RCMP’s collection of open-source information under Project Wide Awake* (15 February 2024) paras 6–7 <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/sr_pa_20240215_rcmp-pwa/> accessed 11 November 2025; Bryan Carney, ‘RCMP Confirms Tool Unlocks Hidden Facebook Friends’ *The Tyee* (23 November 2020) <<https://thetyee.ca/News/2020/11/23/RCMP-Confirms-Tool-Unlocks-Hidden-Facebook-Friends/>> accessed 11 November 2025.

196. At its core, this program involved the extensive monitoring of social media to profile indigenous activists and applied a risk-assessment tool to the resulting profiles.²⁰⁰ While presented as a tool for assessing risk of potential unlawful activity at political protests, the assessment tool was criticized for focusing less on actual or potential criminal conduct and more on identifying indigenous activists on the basis of their ability to rally public support to their cause (including support from other groups) and influence public debates through social media.
197. The list of people included in the RCMP's watch list was never made public, but members of the political movements being monitored expressed concern at the potential of being included on the list and their view that the exercise was a tactic to deter ongoing participation in the movement. Notably, the RCMP's own assessment concluded that none of the individuals profiled for this watch list had actually committed a crime or posed a direct threat to critical infrastructure.
198. An ongoing social media monitoring program (Project Wide Awake) uses a third party commercial tool called Babel X to monitor social media and other commercial providers for a range of objectives including to monitor and to attempt to predict behaviour at political protests.²⁰¹ The RCMP characterizes Project Wide Awake as non-intrusive and ignores that the program has any privacy implications. The RCMP consistently minimizes the intrusiveness of its OSI capabilities in its internal assessments and in its interactions with regulators and the public.
199. In practice, the commercial provider uses algorithmic tools to monitor public and private data on a mass scale.²⁰² The commercial provider allows law enforcement to analyze account level activity such as public posts on a mass, indiscriminate scale. The commercial provider is also able to access private sources in ways that violate Canadian law. It can, for example, provide access to closed messaging groups that are not available to the general public and to sensitive geolocation data it obtains without user consent.²⁰³ The commercial service also provides

²⁰⁰ Mack Lamoureux, 'The RCMP Used Police Databases and Social Media to Track Aboriginal Protestors' *Vice* (date unknown)
<<https://www.vice.com/en/article/the-rcmp-used-police-databases-and-social-media-to-track-aboriginal-protestors/>> accessed 10 November 2025; Oscar Baker III, 'Mi'kmaq Woman Concerned About Project SITKA' *CBC News* (20 November 2016)
<<https://www.cbc.ca/news/canada/new-brunswick/rcmp-project-sitka-mi-kmaq-1.3858261>> accessed 10 November 2025; Jeffrey Monaghan and Howe, 'Strategic Incapacitation of Indigenous Dissent' (2018)
<<https://www.sfu.ca/~palys/Howe&Monaghan-2018-StrategicIncapacitationOfIndigenousDissent.pdf>> accessed 10 November 2025.

²⁰¹ Bryan Carney, 'Project Wide Awake: How the RCMP Watches Us Online' *The Tyee* (25 March 2019)
<<https://thetyee.ca/News/2019/03/25/Project-Wide-Awake/>> accessed 11 November 2025.

²⁰² Office of the Privacy Commissioner of Canada, *Special Report to Parliament: Investigation of the RCMP's collection of open-source information under Project Wide Awake* (15 February 2024)
<https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/sr_pa_20240215_rcmp-pwa/> accessed 10 November 2025.

²⁰³ *ibid.*

access to sensitive private data obtained by malicious third parties in violation of Canadian laws and sold online.²⁰⁴

200. One of Project Wide Awake's intended uses is to monitor activity at public protests.²⁰⁵ However, the programs' actual operation remains shrouded in secrecy, making actual scrutiny of its protest related operation challenging. The program was found to violate Canada's federal *Privacy Act*, but as the federal law is unenforceable, the RCMP continues to operate the program unabated.²⁰⁶

Colombia

201. In 2020, *Semana*,²⁰⁷ a Colombian media outlet, revealed that the Colombian National Army and its intelligence agencies had used social media posts and publicly available information on the internet with the intention of monitoring and profiling individuals.²⁰⁸ They profiled more than 130 citizens, including journalists, political opponents of the government, human rights defenders, union members, and congressmen.
202. This case showed how data profiling made by intelligence agencies leads to risks to privacy and freedom of expression.²⁰⁹ Moreover, it brings up the issue with the misinterpretation of intelligence agencies that any information publicly available on the internet may be used, even when they are not legitimately fulfilling national security and public defense purposes, but rather profiling people who think differently. It also highlights the risk of discrimination, considering that the people profiled were dissenters from the government.
203. A few years ago, CAJAR, a civil society organization brought a case²¹⁰ to the InterAmerican Court of Human Rights alleging its members had been victims of surveillance which included

²⁰⁴ *ibid.*

²⁰⁵ *ibid*; Bryan Carney, 'You Have Zero Privacy Says an Internal RCMP Presentation' *The Tyee* (16 November 2020) <<https://thetyee.ca/News/2020/11/16/You-Have-Zero-Privacy-RCMP-Web-Spying/>> accessed 10 November 2025.

²⁰⁶ Office of the Privacy Commissioner of Canada, *Special Report to Parliament: Investigation of the RCMP's collection of open-source information under Project Wide Awake* (15 February 2024) <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/sr_pa_20240215_rcmp-pwa/> accessed 10 November 2025; Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, *Submission to the Public Consultation on the Privacy Act* (14 February 2021) <<https://www.justice.gc.ca/fra/sjc-csj/lprp-pa/sou-sub/placing.html>> accessed 10 November 2025.

²⁰⁷ Publicaciones Semana S.A., *Semana.com* <https://www.semana.com/> accessed 9 November 2025.

²⁰⁸ Redacción Semana, 'Espionaje del Ejército Nacional: Las carpetas secretas' Publicaciones Semana S.A. (1 May 2020)

<https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/> accessed 9 November 2025.

²⁰⁹ Lucía Camacho Gutiérrez, Daniel Ospina Celis & Juan Carlos Upegui Mejía, *Inteligencia estatal en internet y redes sociales: el caso colombiano* (Editorial De Justicia 2022) <https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf> accessed 9 November 2025.

²¹⁰ *Members of the Corporation Lawyers Collective "José Alvear Restrepo" (CAJAR) v Colombia* (Inter-American Court of Human Rights, Judgment of 18 October 2023) Series C No 506 https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf accessed 9 November 2025.

illegal espionage, illegal interception of communications, compilation of biographical data on them and their families.²¹¹ They also alleged some of their members were included in the 130 people who were profiled based on their social media posts or information available on the internet.

204. Recently, in May, 2025, the Inspector General's Office (Procuraduría General de la Nación) issued a decision²¹² confirming the responsibility and sanctioning nine members of the Army belonging to intelligence units. It based its decision on the fact that the condemned agents "committed a serious disciplinary offense by ordering, coordinating, and executing, without justification, open source intelligence (OSINT) activities targeting journalists, in violation of constitutional guarantees and fundamental rights". Consequently, it sanctioned them with suspension from office and disqualification from holding public office for between 3 and 6 months. The Fundación para la Libertad de Prensa, FLIP, denounces that these sanctions are not proportional to the seriousness of the offenses, and that no criminal sanction has been adopted yet. Therefore, it urges the Attorney General's Office (Fiscalía General de la Nación) to act timely.
205. On the other hand, in the context of the 2021 national strike, among various tools of repression and persecution of social protest, actions such as cyber patrols were implemented.²¹³ Under the pretext of detecting fake news and promoting the truth, the Ministry of Defense, specifically through the National Police, monitored and persecuted²¹⁴ information circulating on social media, particularly that aimed at calling for and supporting demonstrations during the months of the national strike, as well as that related to reports of repressive and violent actions by the security forces during the protests. This information was discredited by the "official" narrative, which considered it false or erroneous, arguing that the circulation of this information (or disinformation) promoted digital terrorism—understood as a crime that does not actually exist in the legal system—delegitimized institutions, and encouraged hate toward the police.²¹⁵ Although Resolution 5839 of 2015 of the National

²¹¹ CAJAR Press, 'Illegal Intelligence: A State Policy? Who Gave the Order?' (José Alvear Restrepo Lawyers' Collective, 7 May 2020) <https://www.colectivodeabogados.org/la-inteligencia-ilegal-una-politica-de-estado-quien-dio-la-orden/> accessed 9 November 2025.

²¹² Fundación para la Libertad de Prensa (FLIP), 'Procuraduría sanctions nine members of the Army for responsibility in illegal surveillance of journalists' (FLIP, 14 May 2025) <https://flip.org.co/pronunciamientos/procuraduria-sanciona-a-nueve-miembros-del-ejercito-por-su-responsabilidad-en-la-vigilancia-ilegal-a-periodistas> accessed 9 November 2025.

²¹³ Fundación Karisma, *Cuando el estado vigila. Ciberpatrullaje y OSINT en Colombia* (27 February 2023) <<https://web.karisma.org.co/cuando-el-estado-vigila-ciberpatrullaje-y-osint-en-colombia/>> accessed 10 November 2025.

²¹⁴ Fundación para la Libertad de Prensa (FLIP), *Los jueces de la verdad: el mar de mentiras detrás del ciberpatrullaje del Estado* (29 October 2021). <<https://flip.org.co/pronunciamientos/los-jueces-de-la-verdad-el-mar-de-mentiras-detras-del-ciberpatrullaje-del-estado>> accessed 10 November 2025.

²¹⁵ Cuestión Pública, *Disinformation and Terminator: The weapons of the Ministry of Defense to pursue protesters with artificial intelligence* (29 October 2024) <<https://cuestionpublica.com/desinformacion-y-terminator-las-armas-del-mindefensa-para-perseguir-manifestantes-con-inteligencia-artificial-2/>> accessed 10 November 2025.

Police authorized the Police Cyber Center (CPP) to carry out cyber patrols, it is not clear what this consists of, the procedures to be followed, or what its limits or controls are.²¹⁶

206. Karisma, a Colombian NGO, alleges that this Resolution has two structural problems. First, it regulates an activity that affects human rights and, therefore, should be established through a statutory law rather than an *infralegal* provision, as it currently is. Second, it is vague and not precise enough to regulate such a complex matter.²¹⁷
207. This monitoring of social media and review of information to subsequently be classified as true was carried out through a Unified Cybersecurity Command Center (PMU-Ciber), which was set up in the midst of the strike. The PMU-Ciber included the Office of the President (Csirt Presidencia), the Ministry of Defense (ColCERT), the Ministry of Information and Communications Technology (min TIC), the Attorney General's Office, the Armed Forces (CCOCI), the National Police, and the National Intelligence Directorate (DNI). However, there is no clarity regarding the functions and scope of each institution that makes up the PMU.²¹⁸ In addition, cyber patrols were used to gather information on individuals who posted or shared information on social media. This information was then used to profile and start legal proceedings against protesters. Victims of this strategy included young people, students, alternative media journalists, and community leaders, among others.²¹⁹ The information gathered was also used to issue preventive alerts regarding so-called acts of vandalism. All of this results in the stigmatization of people who exercised their right to social protest and even their right to freedom of expression by creating or sharing content, without necessarily having participated in a demonstration.
208. According to the Defense Sector Report dated June 9, 2021, "Through 21,675 hours of cyber patrols, disinformation campaigns were identified with the aim of generating chaos and hatred toward state institutions. A total of 154 pieces of fake news have been identified and validated, 91 of which are aimed at blurring the truth with facts that do not correspond to reality and have affected the image of the National Police. [...] Likewise, 3,420 preventive alerts have been generated to anticipate acts of vandalism. More than 3,723 videos have been

²¹⁶ La Silla Vacía, *With cyber-patrolling, the Ministry of Defense walks the thin line of censorship* (6 March 2023) <<https://www.lasillavacia.com/silla-nacional/con-el-ciberpatrullaje-mindefensa-camina-por-la-delgada-linea-de-la-censura/>> accessed 10 November 2025.

²¹⁷ Fundación Karisma, *Cuando el estado vigila. Ciberpatrullaje y OSINT en Colombia* (27 February 2023) <<https://web.karisma.org.co/cuando-el-estado-vigila-ciberpatrullaje-y-osint-en-colombia/>> accessed 10 November 2025.

²¹⁸ Fundación para la Libertad de Prensa (FLIP), *Los jueces de la verdad: el mar de mentiras detrás del ciberpatrullaje del Estado* (29 October 2021) <<https://flip.org.co/pronunciamientos/los-jueces-de-la-verdad-el-mar-de-mentiras-detras-del-ciberpatrullaje-del-estado>> accessed 10 November 2025.

²¹⁹ Cuestión Pública, *Disinformation and Terminator: The weapons of the Ministry of Defense to pursue protesters with artificial intelligence* (29 October 2024) <<https://cuestionpublica.com/desinformacion-y-terminator-las-armas-del-mindefensa-para-perseguir-manifestantes-con-inteligencia-artificial-2/>> accessed 10 November 2025.

analyzed to identify and individualize those responsible, and 09 investigations have been opened." (p. 87).²²⁰

209. The risks associated with cyberpatrolling were already recognized by the IACHR in the Report on their working visit,²²¹ as follows: "The Commission notes with concern that security forces appear to be assuming powers to check information, classifying such content as true or false. This is especially worrying when the information being categorized mostly concerns the actions of the security forces" (para. 177). In addition, "the Inter-American Commission is concerned about repeated reports of profiling of social media users, whether or not they participated in the protests. Generic characterization through terms such as 'terrorism,' 'vandalism,' or 'criminals' stigmatizes protesters and creates a hostile environment for the exercise of protest and freedom of expression on the Internet" (para. 180). So, it is clear that cyberpatrolling can also lead to self-censorship or generate a chilling effect.²²²

Ireland

210. In Ireland, An Garda Síochána are reported to monitor and analyse social-media platforms for potential public-order threats.²²³ The Guards use reactive or proactive monitoring of social media activity for planned or spontaneous assembly events and for other public order matters.²²⁴
211. Any details around Garda policy, including its legislative basis, are not currently disclosed and so this practice is not transparent. Garda reportedly intend to expand their practice and are apparently guided by a non-public facing policy document requiring this practice be law and rights respecting.²²⁵ Social media posts have recently formed a key part of investigations into the Dublin riots in November 2023.²²⁶

²²⁰ Colombian National Police, *Report from the Defense Sector: Guarantees for Peaceful Protest and Control of Violent Actions (April 28 to June 4, 2021)* (9 June 2021)

<https://www.policia.gov.co/sites/default/files/informe_sector_defensa_-garantias_a_la_manifestacion_pacifica_y_control_de_acciones_violentas-28_de_abril_a_4_de_junio_de_2021_20210609_vf.pdf> accessed 10 November 2025.

²²¹ Organization of American States (OAS), *Observations and Recommendations from the IACHR's Working Visit to Colombia (June 8–10, 2021)* (June 2021)

<https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_cidh_Colombia_spA.pdf> accessed 10 November 2025.

²²² Carolina Botero Cabrera, '21,647 hours watching the internet: Cyber-patrolling during 36 days of the strike' *El Espectador* (25 June 2021)

<<https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/21647-horas-vigilando-internet-el-ciberpatrullaje-en-36-dias-del-paro/?outputType=amp>> accessed 10 November 2025.

²²³ Conor Gallagher, 'Gardaí Expand Social-Media Monitoring to Combat Far-Right Extremism and Serious Offending' *The Irish Times* (11 November 2024)

<<https://www.irishtimes.com/crime-law/2024/11/11/gardai-expand-social-media-monitoring-to-combat-far-right-extremism-and-serious-offending>> accessed 11 November 2025.

²²⁴ Ibid.

²²⁵ Ibid.

²²⁶ Ibid.

Kenya

212. The Kenyan government has increasingly turned to cyber-patrolling to control digital expression and online organising. The DCI's Optimus 3.0 system, acquired in 2025, uses machine learning to monitor social media posts, identify "risk actors," and trace their locations. Funded through a KSh 150 million budget, the system reflects a growing institutionalisation of digital surveillance.
213. During the 2024 protests, this infrastructure was deployed to identify organisers and track communications between protest leaders. The government throttled internet speeds, blocked the Telegram app, and disrupted live broadcasts from media houses. These tactics aimed to sever communication lines among protesters and prevent coordination. In 2025, the arrest of Rose Njeri, a software developer who created a civic participation platform enabling citizens to contact their legislators, epitomises this trend. Detained for 90 hours under the Computer Misuse and Cybercrimes Act (2018), Njeri's case demonstrates how digital activism is being criminalised under the pretext of cybersecurity.
214. Further compounding the issue, the Digital Forensic Research Lab (DFRLab) reported in December 2024 that Kenyan authorities and affiliated accounts had used AI-generated images and disinformation to portray protesters as violent or foreign-funded. These campaigns sought to delegitimise civic mobilisation and justify state crackdowns. The use of AI to manipulate public perception represents a new frontier of repression that blends surveillance with propaganda.

South Africa

215. Regarding social media surveillance in South Africa, the Protection of Personal Information Act (POPIA), provides for the protection of personal information as it is processed by public and private bodies. To ensure the achievement of this, Section 2 of this Act gives effect to Section 14 of the Constitution, which guarantees the right to privacy, by ensuring that personal information, when processed by a responsible party is duly safeguarded. Section 2 of POPIA also regulates the way in which personal information may be processed and used. In achieving this, section 2 of POPIA provides that the purpose of the Act is to:
- give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party;
 - regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;
 - provide persons with rights and remedies to protect their personal information from processing that is not in accordance with POPIA ; and
 - require all individuals, entities and particularly businesses, to establish new methods of operating with regard to the collection and/or dissemination of any personal information stored in any manner.

216. However, in general, POPIA applies to all organisations, including Big AdTech companies, that process personal information in South Africa. It sets out various obligations for these companies, such as obtaining consent for data processing, implementing appropriate security measures, and providing individuals with access to and control over their personal data. Despite POPIA, there are several examples of private actors facilitating or getting involved in State surveillance activities.
217. Part A of Chapter 5 of the Act establishes the authority, powers, duties and functions of the Information Regulator ('IR'). The IR is the body primarily responsible for the monitoring and enforcement of compliance with the Act, handling of complaints, issuing of code of conducts and other functions with respect to the purposes of the Act.²²⁷ The IR regularly sends out announcements that remind public/private bodies of their obligations. Additionally, when evidence was found that implicated certain SAPS officials of leaking rape victims' personal information over WhatsApp, the IR issued summons²²⁸. When matters/events relevant to the processing of personal information occur, the IR has regularly released statements noting how the public's rights will be affected, for example the publishing of Matric results and WhatsApp's new privacy policy.
218. In 2021, WhatsApp introduced certain revisions to its Privacy Policy ("Revise Privacy Policy"), differentiating significantly between European and non-European users. The changes included:
- Mandatory data sharing with Meta companies;
 - Removal of an opt-out option of sharing account information with Meta for some users;
 - A deadline of May 2021 for accepting the new terms, failing which users would lose functionality; and
 - Imposition on gradually increasing limitations on WhatsApp functions for non-accepting users.
219. WhatsApp claimed that the updates to their Revised Privacy Policy were, at least partly, aimed at increasing transparency regarding how WhatsApp collects and uses data. However, these amendments are not compliant with South Africa's current regulatory framework for the collecting and processing of personal information.²²⁹ First, the revisions themselves do not comply with Chapter Three of the Protection of Personal Information Act 4 of 2013. Second, users were not informed that a failure to consent to the revisions would limit the functionality

²²⁷ POPIA supra note 8, section 39 and 40.

²²⁸ Information Regulator Nomzamo Zondi *Information Regulator Issues A Summons Against South African Police Service* (29 August 2022) Available: <https://inforegulator.org.za/wp-content/uploads/2020/07/MEDIA STATEMENT -REGULATOR-ISSUES-A-SUMMONS-AGAINST-SOUTH-AFRICAN-POLICE-SERVICE-.pdf> (accessed 2 May 2023).

²²⁹ Information Regulator Nomzamo Zondi *Information Regulator SA Provides Legal Analysis on WhatsApp Privacy Policy* (3 March 2021) Available: <https://inforegulator.org.za/wp-content/uploads/2020/07/ms 20210303-Whatsapp.pdf> (accessed 24 April 2023).

of the platform, impugning the validity of their consent to the revisions and the validity and enforceability of their contract with WhatsApp.

220. On 10 September 2024, the Information Regulator issued an Enforcement Notice against WhatsApp LLC noting that WhatsApp was in breach of the conditions set under POPIA for the processing of personal information. In its Enforcement Notice, the Information Regulator noted that WhatsApp Revised Privacy Policy was in breach of²³⁰;

- Section 9 of POPIA insofar as it failed to provide both users and the Information Regulator with sufficient information to ascertain when and under which circumstances WhatsApp would process users' personal information;
- Section 11 of POPIA insofar as WhatsApp obtained coerced consent for its Revised Privacy Policy by imposing significant restrictions on the functionality of its platform for users who did not consent to the revised policy;
- Section 17 of POPIA insofar as WhatsApp has failed to maintain documentation of its processing activities in accordance with section 51 of the Promotion of Access to Information Act; and
- Section 19 of POPIA insofar as WhatsApp has failed to demonstrate its maintenance of appropriate safeguards and security practices and procedures.

221. The Information Regulator ordered WhatsApp to take all necessary steps to remedy the identified breaches and ensure the lawfulness of its Revised Privacy Policy. Additionally, WhatsApp was ordered to:

- Undertake a detailed Personal Information Impact Assessment and submit the assessment to the Information Regulator;
- Communicate with its users and data subjects in a manner that is easy to understand and promotes transparency; and
- Provides users with various "Frequency Asked Questions" on key topics.

222. To date, WhatsApp has not taken the necessary steps to comply with the Information Regulator's Enforcement Notice and remedy the shortcomings in its Revised Privacy Policy. WhatsApp thus continues to collect and process users' data unlawfully and without the necessary safeguards in place to prevent the abusive collection, processing and sharing of users' personal information. This allows WhatsApp the ability to surveil users and share data unlawfully.

223. With respect to Facebook, in a study on political microtargeting during the 2024 South African elections, conducted by the LRC and African Internet Rights Alliance, it was found that:

²³⁰ Information Regulator *Enforcement Notice In Terms Of Section 95 Of The Protection Of Personal Information Act 4 of 2013 (10 September 2024)* Available: <https://info regulator.org.za/wp-content/uploads/2025/04/WHATS-APP-ENFORCEMENT-NOTICE.pdf>

- a significant portion (18%) of ads on Facebook were classified as suspected micro-targeted outliers;²³¹
- four dominant themes in ad content, ranged from party-specific campaign messaging to issue-based discussions on governance, independence movements, and environmental concerns;²³²
- micro-targeted ads showed a balanced gender distribution;²³³
- Urban hubs like Gauteng and Western Cape dominated impressions across most topics, indicating a strategic focus on populous areas. Age-wise, the 25-34 and 35-44 groups were consistently the most targeted demographics, particularly in micro-targeted campaigns²³⁴; and
- Micro-targeted ads exhibited longer average durations (11.88 days) compared to normal ads (6.29 days), suggesting a strategy of prolonged engagement with specific audience segments.²³⁵

224. Political microtargeting, the practice of tailoring campaign messages to specific voter segments based on personal data, raises critical concerns regarding privacy, electoral fairness, and social cohesion. In the South African context, where sociopolitical discontent is already at an all time high, a political campaign technique that seeks to manipulate voter behaviour by exploiting biases, fears and vulnerabilities in order to influence an election is of serious concern. Furthermore, it is a form of data surveillance and control that goes against the spirit of the Constitution and international best practices with respect to the use of data and online platforms.

225. Although political campaigns can leverage data-driven microtargeting techniques to reach diverse voter segments, balance gender representation in political messaging and address underrepresented demographics, legislative developments and amendments are crucial to ensure adherence to privacy standards and ethical considerations such as data protection, transparency, and user consent. The underlying goal should be to create more inclusive political discourse without compromising individual privacy or manipulating voters through overly invasive targeting practices.²³⁶

226. Legislative developments are also crucial for ensuring that social media platforms are accountable for and transparent about their role in political advertising. For example, social

²³¹ C Kreuser, J Gitonga Theuri, J Kitili, K Govender, M Tyhulu *Contextualising Political Advertising Policy To Political Micro-Targeting In The South Africa 2024 Elections* ed by A Odunlami (29 November 2024) AIRA, 37. Available: <https://lrc.org.za/docs/political-ad-policy-micro-targeting-in-south-africas-elections/> (accessed 3 November 2025).

²³² Ibid

²³³ Ibid

²³⁴ Ibid

²³⁵ C Kreuser, J Gitonga Theuri, J Kitili, K Govender, M Tyhulu op cit note 230.

²³⁶ Ibid, Pg. 38

media platforms should expand ad libraries and provide more comprehensive targeting information. These measures would enable researchers, regulators, and the public to gain deeper insights into digital political campaigning practices, thereby facilitating more effective monitoring of the evolving landscape of online political communication.²³⁷

227. As highlighted above, the people of South Africa are increasingly campaigning against the State and the largest opposition parties for their failure to govern and implement meaningful change within society. Unrest is at an all-time high and South Africans use social media more now than ever to express discontent, organise as well as discuss the way forward with respect to governance and elections. However, as a consequence, with the implementation of the above technologies and the lack of regulation thereof, the major political parties are able to manipulate and sow further division within and amongst differing demographic groups. This poses significant risk to South African activists and political groups.

Spyware

Summary

228. Across the reports below on Spyware, a clear global trend emerges: states are increasingly using or refusing to clarify their use of spyware, relying on secrecy and outdated legal frameworks that do not explicitly authorize such tools. This lack of transparency and accountability undermines the rule of law and fuels fears of unlawful digital surveillance, especially against journalists, activists, and protestors. Spyware, often justified in the name of national security or crime prevention, is being repurposed for domestic monitoring and political control, eroding privacy, chilling dissent, and weakening trust in democratic institutions.

Ireland

229. ICCL is deeply concerned about the Department of Justice's continued refusal to clarify whether the State uses spyware. This silence persists despite European investigations into spyware use and, most recently, *Irish Times* newspaper revelations that An Garda Síochána's Security and Intelligence Section paid €276,433 to Israeli spyware firm Cognyte Technologies last year.²³⁸
230. Following the 2021 Pegasus Project which revealed that hacking software sold by the Israeli surveillance company NSO Group was used to spy on journalists, politicians, activists, and others around the world,²³⁹ the European Commission launched a mapping exercise in

²³⁷ Ibid

²³⁸ Conor Gallagher, 'Garda Síochána Paid Substantial Sums to Israeli Spyware Firm' *The Irish Times* (4 September 2025)

<<https://www.irishtimes.com/crime-law/2025/09/04/garda-siochana-paid-substantial-sums-to-israeli-spy-ware-firm/>> accessed 11 November 2025.

²³⁹ Forbidden Stories, *The Pegasus Project: Global Democracy Under Cyber Attack* (2021)

<<https://forbiddenstories.org/about-the-pegasus-project/>> accessed 11 November 2025.

December 2022 to query member states' use of spyware and the legal frameworks for any such use.²⁴⁰

231. Responding in February 2023, the Irish Government refused to clarify whether the State used spyware. Instead, it referenced the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993* and the *Criminal Justice (Surveillance) Act 2009*.²⁴¹ However, neither of these laws authorise the use of spyware in Ireland. The 1993 act provides for the interception of postal packets and telecommunication messages, the definitions for which rely on the *Postal and Telecommunications Services Act, 1983*.²⁴² The 2009 act provides for covert audio or video surveillance and/or the use of tracking devices, such as GPS trackers on cars or other vehicles.²⁴³
232. When asked about the payment to Cognyte, both the Department of Justice and An Garda Síochána declined to give any information.²⁴⁴ This silence follows the Irish Department of Justice's continued refusal over recent years to clarify whether the State uses spyware,²⁴⁵ while, at the same time, repeatedly insisting: "These technologies can play a legitimate and important role in supporting the work of law enforcement agencies and security services when they are used in a manner that is consistent with respect for human rights, the rule of law and democratic principles."²⁴⁶
233. In May 2023, the report from the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware also failed to explicitly clarify whether Ireland uses spyware or not. However, it did find: "There is no publicly known evidence of abuse of spyware in Ireland" [*emphasis added*].²⁴⁷

²⁴⁰European Commission, *Spyware Mapping Exercise Letter* (21 December 2022) <<https://cdn.netzpolitik.org/wp-upload/2023/04/Spyware-mapping-exercise-EU-Commission-letter.pdf>>

"1. For what purpose is the use of spyware permitted under national law: a. criminal law enforcement? b. national security? c. any other purpose (please specify)? 2. Please list all authorities which are permitted by national law to use or authorise the use of spyware." accessed 11 November 2025.

²⁴¹TJ McIntyre, 'Irish State Spyware and the Law' *IT Law in Ireland* (3 May 2024)

<<https://www.tjmcintyre.com/2024/05/irish-state-spyware-and-law.html>> accessed 11 November 2025.

²⁴²As per Section 1 of the 1993 Act, "postal packet" and "telecommunications message" have the meanings that they have respectively in the Postal and Telecommunications Services Act, 1983,

<<https://www.irishstatutebook.ie/eli/1993/act/10/enacted/en/print#sec1>> accessed 11 November 2025.

²⁴³*Criminal Justice (Surveillance) Act 2009*

<<https://www.irishstatutebook.ie/eli/2009/act/19/enacted/en/print#sec1>> accessed 11 November 2025.

²⁴⁴Conor Gallagher, 'Why Did An Garda Síochána Give Money to Cognyte, an Israeli Surveillance Company?' *The Irish Times* (4 September 2025)

<<https://www.irishtimes.com/crime-law/2025/09/04/why-is-an-garda-siochana-giving-money-to-cognyte-an-israeli-surveillance-company/>> accessed 11 November 2025.

²⁴⁵TJ McIntyre, 'Irish State Spyware and the Law' *IT Law in Ireland* (3 May 2024)

<<https://www.tjmcintyre.com/2024/05/irish-state-spyware-and-law.html>> accessed 11 November 2025.

²⁴⁶Dáil Éireann Debate, *An Garda Síochána* (9 May 2024)

<https://www.oireachtas.ie/en/debates/question/2024-05-09/245/#pq_245> accessed 11 November 2025; Dáil Éireann Debate, *An Garda Síochána* (1 April 2025)

<https://www.oireachtas.ie/en/debates/question/2025-04-01/548/#pq_548> accessed 11 November 2025.

²⁴⁷European Parliament, 'Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware'

234. In March 2024, the Government signed the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware.²⁴⁸ That statement reaffirmed its commitment to the following principle:

“Governments should ensure transparency on the applicable general legal framework supporting the use of surveillance technologies. Governments should clearly define the legal basis for using surveillance technology with transparency on the safeguards in place to prevent abuse or discriminatory uses.”²⁴⁹

235. But it is ICCL’s position that there is no such transparency. In 2022, 2024, and 2025, respectively, Ministers for Justice were repeatedly asked to clarify whether the State uses spyware. In each instance, the Ministers did not provide a direct answer. Instead, they referenced the 1993 and 2009 Act - legislation which does not authorise the use of spyware, as previously mentioned. Given spyware is used for digital device access, the 2023 decision of the Supreme Court in *The People (DPP) v Patrick Quirke* is of particular significance. It distinguished the search of digital spaces from physical spaces and held that judicial authorisation is required for the search of a computer or ‘digital space’.²⁵⁰

236. Against this backdrop, the *Irish Times* report of Garda payments to Cognyte in 2024 is deeply concerning. Cognyte develops spyware and interception tools that provide covert access to devices. If such technology is being deployed in Ireland and, in particular, against protestors, the State would appear to be (i) relying on legislation that does not authorise its use and/or (ii) failing to take account of *Quirke*. This situation demands urgent clarification.²⁵¹ Again, even a lack of clarity over whether the Irish police use spyware or not could serve to have a chilling effect on the right to protest.

Kenya

237. Parallel to the visible expansion of camera networks, Kenya has engaged in covert digital surveillance through the use of commercial spyware. Reports from Citizen Lab (University of Toronto) and Privacy International have confirmed the presence of Pegasus and Circles

(A9-0189/2023, 22 May 2023) https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html accessed 5 November 2025.

²⁴⁸ US Department of State, *Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware* (22 September 2024) <<https://2021-2025.state.gov/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/>> accessed 11 November 2025.

²⁴⁹ Freedom Online Coalition, *Guiding Principles on Government Use of Surveillance Technologies* (March 2023) <https://freedomonlinecoalition.com/wp-content/uploads/2023/03/FOC_Guiding_Principles_on_Government_Use_of_Surveillance_Technologies.pdf> accessed 11 November 2025.

²⁵⁰ [2023] IESC 20 (Supreme Court of Ireland, 2023) <https://www.courts.ie/acc/alfresco/64404309-c09b-4ced-9099-714890aeb38f/2023_IESC_20.pdf/pdf#view=fitH> accessed 11 November 2025.

²⁵¹ Share Foundation, *A Privacy Nightmare: Understanding Spyware* (September 2025) ch 5 <<https://sharefoundation.info/wp-content/uploads/2025/09/Spyware.pdf>> accessed 11 November 2025.

spyware in Kenya. These tools enable remote access to a target's phone, extracting calls, messages, and location data without the user's knowledge.

238. The KHRC and the Defenders Coalition have documented multiple instances where human rights defenders, journalists, and lawyers were subjected to hacking attempts or unexplained surveillance. Activists involved in protests against police brutality and corruption have reported receiving suspicious links or malware-laced messages preceding arrests or intimidation. In a 2024 Privacy International survey, 68% of defenders interviewed indicated that they had altered their communication patterns due to fear of interception.
239. Such surveillance violates both the right to privacy and the right to freedom of association. The ability of activists to organise depends on the confidentiality of communications. When digital spaces are infiltrated, networks of trust disintegrate, and movements fragment. The use of spyware in Kenya reflects a global trend in which surveillance technology, marketed as a counter-terrorism tool, is repurposed for domestic political control. This repurposing has profound consequences for civic life, as it criminalises dissent and weakens social movements.

Encryption

Summary

240. End-to-end encryption is a process of scrambling data that prevents any third party, including the service provider, from reading messages sent between a sender and a recipient. Users, including journalists and protestors, are increasingly demanding end-to-end encryption, using it to control the privacy and confidentiality of the information that they share.²⁵²
241. In today's digital world, where encryption is the foundation of digital trust, it is not just an essential tool that is used to safeguard private texts, emails, voice calls and social media. It also protects and secures the processing of data when it comes to sensitive activities such as personal banking, online shopping, accessing health data and carrying out employment activities. In essence, it is essential for everyone's collective cybersecurity.
242. Forcing companies to create access pathways within the technical standards upon which encryption relies would put all online activities at risk, as those pathways amount to security vulnerabilities that could be exploited by others.

Ireland

243. ICCL also has serious concerns regarding a recent announcement by Ireland's Minister for Justice to introduce domestic legislation that would give Irish police access to encrypted

²⁵² Olga Cronin, 'Letting Gardaí Access Our WhatsApps and Chats to Investigate Crime Could Backfire' *The Irish Times* (13 August 2025)

<<https://www.irishtimes.com/opinion/2025/08/13/letting-gardai-access-our-whatsapps-and-chats-to-investigate-crime-could-backfire/>> accessed 11 November 2025.

deepened structural discrimination, and eroded the spaces for privacy, protest, and democratic participation.

248. The evidence shows a consistent pattern that technologies introduced in the name of accountability and protection are increasingly being repurposed for control and political surveillance, while secrecy, weak oversight, and blurred boundaries between public and private actors undermine transparency and redress. The resulting environment normalizes constant monitoring, both physical and digital, and produces a chilling effect on free expression, assembly, and civic engagement, particularly among marginalized and dissenting groups.
249. Digital and AI-assisted surveillance does not impact all individuals equally. Marginalized groups, including racialized communities, women, LGBTQ+ activists, persons with disabilities, and others, face heightened risks of profiling, harassment, and discriminatory targeting. Surveillance technologies can expose individuals mobilizing around contentious issues such as gender-based violence, reproductive rights, and queer equality, placing them at greater risk of reprisals and restricting their participation in public life. For already disadvantaged communities, this exclusion from public space compounds existing inequalities and undermines the protections essential for civic engagement.
250. States should require that any deployment of AI-enabled digital surveillance technologies by law enforcement or other authorities be subject to comprehensive, non-delegable human rights impact assessments prior to use. These assessments must evaluate the effects on fundamental rights, including privacy, protection of personal data, freedom of expression, freedom of peaceful assembly, and non-discrimination, and must explicitly define the purpose, scope, operational parameters, and targeted populations for the technology.
251. States should identify the nature and magnitude of potential risks, explain how those risks will be mitigated, and provide evidence-based justification demonstrating that the deployment is strictly necessary, proportionate, and effective in achieving a legitimate objective, while showing why less intrusive alternatives would be insufficient.
252. AI systems and their datasets must be carefully assessed to ensure they do not produce biased or discriminatory outcomes against protected characteristics such as race, gender, age, disability, or other vulnerable attributes.
253. Clear remedies must be available for individuals adversely affected, including those misidentified or whose data has been improperly processed. Post-deployment, AI-enabled systems should undergo regular, periodic reviews to ensure ongoing compliance with human rights standards, with mandatory decommissioning of systems that fail to meet these standards or demonstrate disproportionate, biased, or unlawful outcomes. These measures are essential to safeguard democratic freedoms, prevent abuse, and ensure accountability in the use of increasingly powerful digital and AI-assisted surveillance technologies.

254. In sum, the dominant global trajectory is one of technological expansion outpacing democratic regulation, where surveillance systems are embedding themselves into the fabric of public life without the consent or knowledge of those being watched. Reversing this trend requires urgent, coordinated action: clear legal frameworks, accountability, independent oversight, transparency, limiting intrusive technologies, strong data protection standards and protecting vulnerable groups are critical steps to uphold the right to peaceful assembly and to guarantee that all individuals can participate safely and equally in democratic life.
255. INCLO is thankful to the UN Special Rapporteur on the Freedom of Peaceful Assembly and Association for their consideration of this contribution and remains at its disposal for any further consultation that would benefit the preparation and drafting of the report.
256. ENDS.