INTERNATIONAL CIVIL LIBERTIES
MONITORING GROUP

People’s Consultation on Artificial Intelligence

Submission by the International Civil Liberties Monitoring Group

March 23, 2026

About the International Civil Liberties Monitoring Group

The International Civil Liberties Monitoring Group (ICLMG) is a national coalition of 45 Canadian civil society organizations that was established after the adoption of the Anti-Terrorism Act of 2001 in order to protect and promote human rights and civil liberties in the context of the so-called “war on terror.” The coalition brings together 45 NGOs, unions, professional associations, faith groups, environmental organizations, human rights and civil liberties advocates, as well as groups representing immigrant and refugee communities in Canada.

Our mandate is to defend the civil liberties and human rights set out in the Canadian Charter of Rights and Freedoms, federal and provincial laws (such as the Canadian Bill of Rights, the Canadian Human Rights Act, provincial charters of human rights or privacy legislation), and international human rights instruments (such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment).

Overarching concerns

Through our work, we have documented how a lack of regulation of artificial intelligence tools and how they are used can have significantly negative impacts on the rights and livelihoods of people in Canada and internationally. This includes its use to power surveillance tools, to profile individuals, to attempt to predict unlawful activity or to make potentially life-altering decisions in a wide-range of sensitive areas, including employment, immigration, border security, law enforcement, and intelligence gathering. We are particularly aware of the interest among government, law enforcement and intelligence agencies to harness AI tools, and to work with private contractors developing those tools, for counter-terrorism and national security purposes. We've seen how AI models are inaccurate, biased, and misleading. A study from September 2025 shows that every AI model of every major AI company deliberately lies to users: OpenAI Google's Gemini, Anthropic's Claude, xAI's Grok, and Meta's Llama all showed the same deceptive behavior. The paper seems to suggest that it's unclear if safety training actually stops deception, or just teaches AI to hide it better."[1] We have also seen how such tools can be used to violate fundamental rights and can either be shared with, sold to, leaked, or stolen by a wide range of actors who can use the tools for their own nefarious purposes. Given all this, we are acutely aware of the need to regulate the development and use of AI tools in the private and public sectors.

We believe that the government should bear in mind the following concerns and principles in developing any further legislation or regulations to govern the use of AI overall, and specifically in the areas of national security and law enforcement.

A. Regulation of AI must be grounded in human rights, Charter rights and international human rights law

As the Canadian government moves forward with regulating AI, it must take a rights-based approach. Currently, it doesn't appear to be the case. While the need to abide by Charter rights is mentioned, the government has not made this central to recent consultations, and there has been no mention of Canada's broader human right obligations, both domestically and internationally.

A 2026 report from the UBC AI & Criminal Justice Initiative summarizes the key components of a human rights-centred approach to AI regulation, based on the early and seminal research in "*To Surveil and Protect: A Human Rights Analysis of*

[1] arXiv:2509.15541v1 **[cs.AI]** and see: https://x.com/heynavtoor/status/2029300381554249922

Algorithmic Policing in Canada", published in 2020 by University of Toronto's Citizen Lab and International Human Rights Program in 2020:

- Right to privacy: ensuring that data collection, processing, and sharing complies with privacy rights; and ensuring data and algorithm accuracy.
- Rights to freedom of expression, peaceful assembly, and association: protecting anonymity in public assemblies, and preventing surveillance of social movements and marginalized communities.
- Right to equality, and freedom from discrimination: adopting an intersectional approach to ensuring equality, addressing algorithmic bias and discriminatory feedback loops, and over-policing of marginalized groups.
- Right to liberty and freedom from arbitrary detention: confronting generalized suspicion, addressing unconscious bias and racial profiling. Right to due process: issues related to algorithmic transparency, private sector influence, and disclosure.
- Right to remedy: notice requirements, ability to challenge algorithmic outcomes, and effective remedies.[2]

Recommendations 1 & 2

1. AI regulation must be grounded in a human rights-first approach, should include human rights-based assessments, and ensure that rights protections are built into the legislation, especially protection of privacy rights.

2. AI legislation should take an approach that addresses the roots of AI companies' algorithms and business models and their significant human rights implications.

B. Definitions

I. AI legislation should clearly define terms and categories (such as high impact systems)

Important definitions, such as what are considered high impact systems that carry the greatest risk of harm to people and human rights, should not be left to regulation nor to the developers of AI systems.

[2] Copied from Benjamin Perrin, Geoffrey Liew and Isabelle Sweeney, AI & Policing: Research Report on the Governance & Use of Artificial Intelligence by Police in Canada, UBC AI & Criminal Justice Initiative, 2026 CanLIIDocs 293, https://canlii.ca/t/7nrqc. See also: Cynthia Khoo, Kate Robertson, and Yolanda Song. "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada," The Citizen Lab and International Human Rights Program (Faculty of Law, University of Toronto), Research Report No. 131, September 2020, https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf

For example, the EU *AI Act* defines four clear categories of AI systems, each with a progressing degree of regulation: Unacceptable Risk, High Risk, Generative AI, Limited Risk.

"Unacceptable risk" would be AI systems that present such an unmitigable risk to rights that it must be banned; "high risk" would require substantial analysis and assessment before use; and "limited risk" would still be required to meet requirements around transparency and user consent.[3]

We would recommend that any future AI legislation include escalating categories of AI systems requiring regulation, modeled after the definitions included in the EU *AI Act*. We would further recommend that new categories be allowed to be added by regulation, as necessary, in order to preserve the ability to adapt the regulatory framework when needed, but to still maintain a minimum level of regulation.

We support the recommendation by the Women's Legal Education and Action Fund (LEAF) in their submission on Bill C-27, the *Digital Charter Implementation Act, 2022*, that an assessment "must include performing an equity and privacy audit as prescribed by regulation."[4]

II. *Definition of harms must include group-based harms*

There is a documented reality of artificial intelligence causing group-based harms by infringing on collective rights. As further explained by LEAF in their brief: "Collective rights are those held by a group as a whole, in contrast to individual rights which are held individually by members of the group. Collective rights protect the interests of a group, such as cultural and language rights, collective privacy, environmental rights, and labour and union rights, all of which are significantly threatened by the introduction of AI systems."[5] There are numerous ways in which collective and group rights are or can be impacted by artificial intelligence tools.

In regards to national security, this includes the selection and categorization of individuals based on assessed risk for the purposes of immigration, employment, travel

[3] European Parliament, "Briefing - EU Legislation in Progress - Artificial Intelligence Act." April 2021. Online at: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[4] Kim, Rosel and Thomasen, Kristen, Submission to The Standing Committee on Industry and Technology on Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (September 11, 2023). At pp. 11, 13. Available at SSRN: https://ssrn.com/abstract=4571389 [LEAF 2023]

[5] [LEAF 2023]

or even surveillance. It also includes the use of artificial intelligence systems to surveil and investigate entire groups based on criteria programmed into the AI tool, as well as the harms visited upon entire groups who face the repercussion of biased systems that have difficulty identifying people of certain races, ages or genders. It can also be used to determine (and exclude) categories of individuals for financial services and immigration or refugee applications. Outside of national security, collective harms can also come in the form of other human rights violations, employment violations, IP right violations, etc.[6]

Recommendations 3 & 4

3. AI legislation should clearly define terms and categories (such as high impact systems). Those definitions should not be left to regulation nor to "people responsible for AI systems."

4. Definition of harms must include group-based harms.

C. The government must develop AI legislation that includes regulations for the national security-related use of AI in both the public and private sectors

Internationally, we have seen the exponential growth in interest in using artificial intelligence tools for counterterrorism and national security purposes. This includes: monitoring for terrorism content online; engaging in surveillance; analysing retained data to identify trends and predict terrorist activities; facilitating and guiding remote and autonomous weapons; and rendering decisions and/or categorizing individuals and groups according to risk in regards to immigration, employment and travel. Each of these engenders the possibility of some of the most serious risks to individuals' rights, including freedom of expression, freedom of association, freedom of movement, security of the person, equality rights, privacy rights and more.

For many years, Canadian national security agencies like the RCMP, CBSA, CSIS and CSE either outright denied, or downplayed, their use of AI tools. However, in recent years they have been more open regarding their interest in increasing their use of artificial intelligence tools for a wide range of purposes, including facial recognition, surveillance, border security, data analytics and cybersecurity. However, they have not revealed the specific ways in which they use artificial intelligence systems, nor what

[6] See Blair Attard-Frost, "Generative AI Systems: Impacts on Artists & Creators and Related Gaps in the Artificial Intelligence and Data Act - Submission to the Standing Committee on Industry and Technology" (5 June 2023) at 13, https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12541028/brexternal/AttardFrostBlair-e.pdf; LEAF 2023; Bailey, J., Burkell, J., and McPhail, B. "Submissions on Bill C-27: The Digital Charter Implementation Act," September 2023.

steps they are taking to mitigate harm. Moreover, no clear legislative framework has been established to regulate their use of these tools in order to prevent serious harm to individuals or to groups.

One example of this issue is the 2020 leaked revelation that RCMP had been using Clearview AI's facial recognition technology (after first affirming it hadn't) without consultation, authorization or disclosure. The Privacy Commissioner of Canada has since declared that Clearview AI, with its non-consensual syphoning of billions of online images, was violating Canadian privacy laws.[7] This raises important questions about what other technologies agencies have been using without our knowledge.[8]

The one attempt by the (previous) federal government to regulate AI in the private sector - the *Artificial Intelligence and Data Act* (AIDA) in former Bill C-27 - explicitly excluded the application of the Act to: …a product, service or activity that is under the direction or control of

> (a) the Minister of National Defence;
> (b) the Director of the Canadian Security Intelligence Service;
> (c) the Chief of the Communications Security Establishment; or
> (d) any other person who is responsible for a federal or provincial department or agency and who is prescribed by regulation.

This would have meant that any AI system developed by a private sector actor which falls under the direction or control of the government would face absolutely no independent regulation or oversight. Such an exclusion is completely unacceptable.

It is crucial that the government develop legislation to regulate the development and use of AI in both the public and private sectors, and that these pieces of legislation explicitly include the regulation of the use of this technology for national security and counter-terrorism purposes.

As the UN Special Rapporteur on Counterterrorism and Human Rights reported to the UN Human Rights Committee in March 2023, "The Special Rapporteur is deeply concerned with the entrenched practice of States adopting legislation that exempts the use of AI for military and national security purposes from ordinary oversight regimes." The report goes on to note: "[The Special Rapporteur] draws attention to the ways in

[7] Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, PIPEDA Findings #2021-001, February 2, 2021, online at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

[8] Benjamin Perrin, Geoffrey Liew and Isabelle Sweeney, AI & Policing: Research Report on the Governance & Use of Artificial Intelligence by Police in Canada, UBC AI & Criminal Justice Initiative, 2026 CanLIIDocs 293, https://canlii.ca/t/7nrqc, p 13.

which security imperatives and counter-terrorism rationales are used to validate the development, use and transfer of new technologies, including, but not limited to, biometric technologies, AI, unmanned aerial vehicles (drones) and surveillance tools. She decries the ways in which, under the guise of preventing terrorism, new technologies have been used that, in practice, function to profoundly undermine the rights of individuals and communities. High-risk technologies have been brought in through the proverbial “back door”, validated by appeals to security that in actuality weaken broader collective security and undermine the promotion and protection of human rights.”[9] In providing the example of the EU *AI Act*, she further stressed, “that AI systems developed for military or dual-use purposes should be regulated by the AI act. She maintains the position that the Council of Europe convention must include the design, development and use of AI systems for national defence within its ambit. To exclude them would effectively make the proposed convention irrelevant to the human rights concerns that are of greatest relevance in the region.”[10]

Similar concerns directly apply to regulatory exclusion of AI systems developed for use by Canadian national security agencies. All AI systems developed by the private sector must face regulation, regardless of its use by national security agencies. While the government may argue that should this technology be sold on the private market, it would then be regulated, it ignores the severe impact that unregulated technology used by these agencies could, and certainly will, have. It also ignores that such technology could be leaked or hacked, or potentially developed for a Canadian agency and then sold in markets without stringent AI regulations. Moreover, we would be concerned that allowing for unregulated development for government use would lead to pressure to weaken regulations around the eventual re-packaging of such technology for the private sector.

Recommendation 5

AI legislation should apply to both the public and private sectors, including government national security, intelligence and law enforcement agencies; and there should be no exemption in AI regulations for national security related technology.

[9] “Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism,” Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin. Human Rights Council, Fifty-second session, A/HRC/52/39, 1 March 2023. Online at https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/reports/A-HRC-52-39-AdvanceEditedVersion.docx. [SR 2023]

[10] [SR 2023]

D. Need for consultation

The federal government has a woeful track record on public consultations regarding artificial intelligence policy and regulations. This dates back to at least the introduction of Bill C-27, and the inclusion of the *Artificial Intelligence and Data Act* (AIDA). While the government had lauded holding more than 300 consultation meetings regarding AIDA, closer inspection reveals that 216 of those were with businesses, and only nine were with civil society stakeholders. Moreover, all of these meetings were held *after* AIDA was introduced in Parliament, and all were held in private. True consultations must begin before legislation is introduced, and be held in an open, accountable manner.[11]

This lack of consultation led 45 leading civil society organisations, experts and academics to write in an open letter that:

> The lack of structured, deliberative, and wide-ranging consultations before and since tabling AIDA is anti-democratic, and it has deprived people in Canada of the rights-protecting, stress-tested AI legislation they need. Innovation, Science and Economic Development Canada's more active consultation on a generative AI Code of Practice—a document that is akin to a statement of principles, yet fails to mention privacy or questionable data practices as a factor in the fairness and equity assessment—is effectively a distraction from getting AIDA right.[12]

Despite these concerns, and the efforts made to lay out what an open and democratic consultation on AI would look like, the government instead proceeded to create a hastily assembled task force that once again skewed heavily toward industry and excluded voices that could speak to the broader implications of AI.[13] This was exacerbated by the launch of an accompanying 30 day public consultation "sprint". This short time period once again limited those most impacted from fully participating.[14] Moreover, the consultation questions prioritized economic benefits of AI, rather than addressing the broader social or human rights concerns.

[11] Andrew Clement, *AIDA Amended - Far From Enough: A response to Minister Champagne's proposed amendments, Addendum to No AIDA is better than this AIDA*. Submitted to the Commons Standing Committee on Industry and Technology on Bill C-27, the Digital Charter Implementation Act, 2022. Online at: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12949365/br-external/ClementAndrew-AIDAAmended2024-03-01-e.pdf

[12] Joint letter of concern regarding the *Artificial Intelligence and Data Act* (AIDA) to the Honourable François-Philippe Champagne, P.C., M.P., Minister of Innovation, Science and Industry, September 25, 2023. Online at: https://iclmg.ca/wp-content/uploads/2023/09/AIDA-JOINT-LETTER-FOR-SIGN-ON.pdf

[13] Teresa Scassa, "Consultation on Canada's New AI Strategy: Don't blink or you'll miss it," October 2, 2025. Online at: https://teresascassa.substack.com/p/consultation-on-canadas-new-ai-strategy

[14] CUPE criticizes federal AI consultation process, December 12, 2025. Online at: https://cupe.ca/cupe-criticizes-federal-ai-consultation-process

In response to these concerns, the ICLMG has joined over 160 other civil society organizations in launching the People's Consultation on AI. Together, we sent an open letter to the Minister of Artificial Intelligence protesting the government's 'national sprint' on AI and documenting the many negative impacts that are already occurring as AI technologies become embedded in every aspect of Canadian society."[15]

While the People's Consultation will serve as an important counter-weight to the government's inadequate rushed process, it cannot - and should not - replace meaningful government consultation. Beyond industry and even academics, communities that are most impacted by AI need to be actively reached out to and engaged in this process. Not only does the federal government have the resources to do so, it has the responsibility as well. This would need to take place both before and after the introduction of future legislation, in order to adequately integrate feedback and concerns.

Finally, these consultations, as well as the drafting and enforcement of AI legislation or the development of regulations post-adoption, cannot and should not be led by the AI ministry or Industry Canada. Their clear mandates of promoting the AI industry and making Canada competitive in the development and use of AI technology is in direct conflict to ethical considerations and a rights-based approach to AI regulation.

Recommendations 6 & 7

6. The government must hold open, inclusive and meaningful consultations, before and after tabling legislation, with a broad range of stakeholders and the public.

7. The consultations should not be led by the Minister of AI or the Ministry of Industry.

E. Need for independent oversight and review

The enforcement of AI regulations should fall to an independent regulator appointed by the Governor in Council after consultation with the Senate and House of Commons opposition leaders. Their appointment should be approved by resolution of the Senate and House of Commons, and they should be granted the power to appoint or lay off employees, require appropriate security clearance, etc.

[15] Press release: Civil Society Launches People's Consultation on AI: Government Regulation of AI Needed, January 21, 2026. Online at: https://iclmg.ca/ai-peoples-consultation-launch/

It will also be essential that, over time, AI regulations be evaluated for effectiveness and impact. They will also need to be re-evaluated given the certainty of new developments within the AI field that, despite attempts at "future-proofing," will require amendments to the law. To accomplish this, future legislation should include provisions for both annual reporting and periodic reviewing.

The federal government's new AI Register provides initial details on the use of AI tools by federal departments and agencies. While still in the early testing phases, and based primarily on already existing information, it provides an interesting example of what further government transparency and accountability initiatives could look like. However, for it to be successful, it must include requirements that all agencies proactively report on their uses of AI tools, and not rely on public data holdings. For example, while the current AI Register relies on Privacy Impact Assessments (PIAs) as a source of information, we know that both the RCMP and CSIS have used new technology without first filing a PIA, that PIAs may not include all relevant information, and that some PIAs are kept secret. The Register, understandably, also only includes government uses of AI technology; while important, it raises questions of transparency and accountability of use of AI technology in the private sector. A register is an important tool, but even at its best cannot replace clear legislation and independent review.

Recommendation 8

The enforcement of AI regulations should fall to an independent regulator, and AI regulations should be periodically reviewed for effectiveness and impact, especially given that AI technology, and its usage, will continue to evolve.

F. Banned uses of AI

Some uses or forms of AI can cause such egregious rights violations and harms that they should be outlawed in any future AI legislation. These are situations where the risk presented to human rights or civil liberties are so high, that their use simply cannot be justified. While completely banning certain uses of AI may seem extreme, it has already been done in leading AI legislation, including the EU *AI Act*. Chapter 2, Article 5 lists prohibited AI systems, including:

- deploying subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making;
- exploiting vulnerabilities related to age, disability, or socio-economic circumstances to distort behaviour;

- biometric categorisation systems inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation)
- social scoring, i.e., evaluating or classifying individuals or groups based on social; behaviour or personal traits, causing detrimental or unfavourable treatment of those people;
- assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits;
- compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage;
- inferring emotions in workplaces or educational institutions;
- 'real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement.[16]

In the EU *AI Act*, many of these outlawed uses of AI include broad exceptions, leading to loopholes that human rights and civil liberties activists have decried for weakening the regime. We have therefore adapted the list in order to remove much of the language allowing for exceptions in order to ensure these restrictions truly protect people and their rights.

Moreover, while this list covers a broad array of harmful uses of AI technology, we would also recommend adding the use of AI for sensitive decision-making around people's lives as well as the deployment of autonomous weapons to the list of banned uses.

In a world where war and weapons still unfortunately exist, decisions regarding military tactics and targets should never be left to AI. This is especially true given that the technology demonstrates biases, has tendencies to lie and, in one recent study, showed a propensity to use nuclear weapons in simulated war games 95 per cent of the time.[17]

It is also crucial that the adoption of any such prohibited measures not include national security loopholes. Unfortunately, EU member states have successfully integrated exceptions into the EU *AI Act* that create significant gaps in regulating law enforcement and intelligence agency use of otherwise prohibited tools. Member states have also used domestic legislation to attempt to circumvent and weaken these protections.[18]

[16] EU Artificial Intelligence Act, High-level summary of the AI Act, May 30, 2024. Online at: https://artificialintelligenceact.eu/high-level-summary/

[17] Chris Stokel-Walker, AIs can't stop recommending nuclear strikes in war game simulations, 25 February 2026: https://www.newscientist.com/article/2516885-ais-cant-stop-recommending-nuclear-strikes-in-war-game-simulations

[18] Ashwin Prabu and Marlena Wisniak, "When National Security Becomes a Shield for Evading AI Accountability," February 16, 2026: https://www.techpolicy.press/when-national-security-becomes-a-shield-for-evading-ai-accountability

European civil society organizations have opposed these exceptions; they should not make their way into Canadian legislation.

Finally, any such legislation should also allow for future additions to the list of banned uses of AI via regulation, to keep up to date with the development of new and unpredictable uses of AI tools and technology.

Recommendation 9

The government should, via legislation, establish a list of banned uses of AI, with the possibility of adding more banned uses by regulation. We would recommend that the initial list include:

- deploying subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making;
- exploiting vulnerabilities related to age, disability, or socio-economic circumstances to distort behaviour;
- biometric categorisation systems inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation)
- social scoring, i.e., evaluating or classifying individuals or groups based on social; behaviour or personal traits, causing detrimental or unfavourable treatment of those people;
- assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits;
- compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage;
- inferring emotions in workplaces or educational institutions;
- ‘real-time’ remote biometric identification (RBI) in publicly accessible spaces for law enforcement.
- decision-making regarding people’s lives (immigration status/removal orders, social benefits, health-related decisions, etc.).
- decision-making regarding the deployment and/or the control of autonomous weapons.

G. Full List of Recommendations:

1. AI regulation must be grounded in a human rights-first approach, should include human rights-based assessments, and ensure that rights protections are built into the legislation, especially protection of privacy rights.

2. AI legislation should take an approach that addresses the roots of AI companies' algorithms and business models and their significant human rights implications.

3. AI legislation should clearly define terms and categories (such as high impact systems). Those definitions should not be left to regulation nor to "people responsible for AI systems."

4. Definition of harms must include group-based harms.

5. AI legislation should apply to both the public and private sectors, including government national security, intelligence and law enforcement agencies; and there should be no exemption in AI regulations for national security related technology.

6. The government must hold open, inclusive and meaningful consultations, before and after tabling legislation, with a broad range of stakeholders and the public.

7. The consultations should not be led by the Minister of AI or the Ministry of Industry.

8. The enforcement of AI regulations should fall to an independent regulator, and AI regulations should be periodically reviewed for effectiveness and impact, especially given that AI technology, and its usage, will continue to evolve.

9. The government should, via legislation, establish a list of banned uses of AI, with the possibility of adding more banned uses by regulation. We would recommend that the initial list include:
   - deploying subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making;
   - exploiting vulnerabilities related to age, disability, or socio-economic circumstances to distort behaviour;

- biometric categorisation systems inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation)
- social scoring, i.e., evaluating or classifying individuals or groups based on social; behaviour or personal traits, causing detrimental or unfavourable treatment of those people;
- assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits;
- compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage;
- inferring emotions in workplaces or educational institutions;
- ‘real-time’ remote biometric identification (RBI) in publicly accessible spaces for law enforcement.
- decision-making regarding people’s lives (immigration status/removal orders, social benefits, health-related decisions, etc.).
- decision-making regarding the deployment and/or the control of autonomous weapons.