LEGAL RESOURCES CENTRE

AI SURVEILLANCE AND THE IMPACT ON HUMAN RIGHTS AND DEMOCRACY:

THE GAPS IN SOUTH AFRICAN LAW

AUGUST 2024

Authors: Emily Dinan, Yanela Frans, and Kimal Harvey

TABLE OF CONTENTS

1.0 INTRODUCTION

The concept and use of surveillance has been a hotly debated subject for centuries. This is primarily because of how the government and private corporations have used it in the past.

The debate mainly centres on the ethics of surveillance and its impact on human rights, especially as it pertains to the right to privacy and dignity. Naturally, if human rights are deemed to be under threat, a conversation about the threat to democracy will follow.

The oldest type of surveillance is physical surveillance typically used when investigators suspect certain individuals or a group of individuals of criminal activities, and therefore decide to observe their day-to-day behaviours. However, as technology has improved, so have the techniques and methodologies used in surveillance.

Hidden microphones, public camera systems, hidden/camouflaged cameras, wiretaps, cell phone activity tracking, facial recognition technology, and now Artificial Intelligence systems (AI). The introduction of AI in the past few years has added a new dimension to the operation and technological development of surveillance, and it is this added dimension that this paper aims to discuss.

In the context of this report, AI technology refers to an amalgamation of systems that includes acquisition objectives, logical reasoning principles and self-correction capacities.[1]

Therefore, AI surveillance technology is effectively an operational upgrade on existing surveillance tech by using this amalgamation of systems.

This research report will approach this discussion in the following manner:

(1) It will discuss the development of AI surveillance and differentiate it from other forms of surveillance;

(2) Thereafter, it will seek to identify gaps in South African law with respect to the regulation of AI surveillance and

(3) Finally, through international and regional legal research, it will recommend how best to fill those gaps in our law.

---

[1] Steven Feldstein 'Introducing The AI Global Surveillance (Aigs) Index' (2019) *Carnegie Endowment For International Peace* at 5, available at https://www.jstor.org/stable/feldstein, accessed 31 July 2024.

2.0 AI SURVEILLANCE

Surveillance is defined as "the act of observing another in order to gather evidence."[2] This evidence is analysed and used to manage or influence its target; alternatively, the information is simply collected and stored.

There are two types of surveillance: electronic and physical:

1. **Physical surveillance** is the oldest type of surveillance, and it takes place in-person and involves an individual, usually a police officer and/or investigator observing a crime suspect's home or following them in public.

2. **Electronic surveillance** is relatively new compared to physical surveillance and is generally long-term. The target is observed through technological devices, for example to determine a target's location through security video cameras and automatic number plate recognition (ANPR) cameras. The target could be observed through their own technological devices when their cell phone and/or laptop are wiretapped, and their phone calls are monitored. Their cell phone and laptop can also be used to monitor their internet activity. AI technology has been introduced into this form of surveillance to improve its operational capacity.

AI can enhance surveillance technology in two ways:

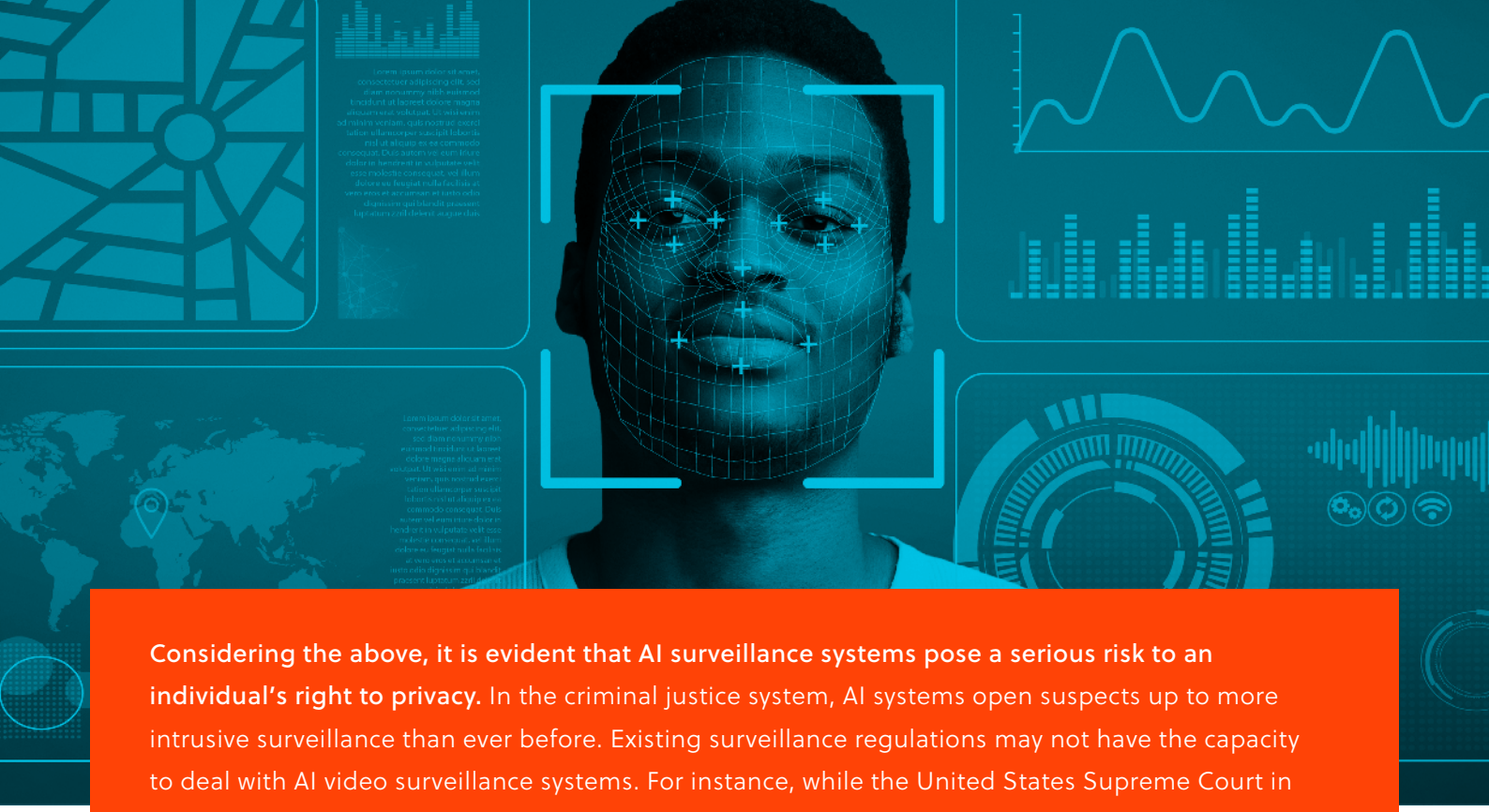
1. AI facial recognition systems make it possible for fixed surveillance to take place remotely. Video surveillance technologies, equipped with AI, can track individuals over a wide geographical area in real time by flagging when those individuals are filmed by different cameras. Traditional systems of facial recognition required manual identification, which would only be possible after the video had been taken, stored, and processed by a human, thus creating a lag time between the time the video was taken and when the individual was identified.

2. AI can be used to help video surveillance systems recognize patterns in activity with the available data and use that to predict the possible patterns in the future. For example, a home security system powered by AI might learn when members of the household come and go and flag activity that deviates from these routines. Law enforcement can use existing data on suspects to analyse their past behaviour and predict future behaviour.[3]

---

[2] Legal Information Institute 'Surveillance' *Cornell Law School* available at https://www.law.cornell.edu/wex/surveillance, accessed on 29 July 2024.

[3] Nicol Turner Lee and Caitlin Chin-Rothmann 'Police surveillance and facial recognition: Why data privacy is imperative for communities of color' *Brookings Institution* 8 April 2022, available at https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/, accessed 31 July 2024.



Considering the above, it is evident that AI surveillance systems pose a serious risk to an individual's right to privacy. In the criminal justice system, AI systems open suspects up to more intrusive surveillance than ever before. Existing surveillance regulations may not have the capacity to deal with AI video surveillance systems. For instance, while the United States Supreme Court in *Carpenter v United States* determined that long-term location tracking via a suspect's cell phone violated the constitutional right to privacy, the Courts have yet to rule on facial recognition systems. Federal Circuit Courts are further divided on whether such systems fall under "public activity", which police officers can access without a warrant.[4] Facial recognition technology is also often inaccurate and is more likely to make a false match when a suspect is dark-skinned, leading to increased false accusations of wrongdoing against people of colour. On the international level, recent reports found that the Israeli Defence Forces have used AI systems to track individual targets and route semi-autonomous weapons in Gaza.[5] Such uses of AI are almost entirely unregulated under Israeli or international law, and there are no mechanisms to determine whether the identification of targets is accurate or in compliance with international human rights law.[6]

Finally, it is important to establish that AI technology is not one single mechanism. It is an integrated system that - acquires specific information, is given its own reasoning principles related to its acquisitive objective and develops self-correcting mechanisms. In effect, this technology gives the user access to a system that can develop its own learnings related to a specific data set, self-improve its own algorithm in order to better collect data, and ultimately advise its user on how to best impact a specific market.[7] This allows users unprecedented access to data sets and related machine learning that can be easily used to create misinformation and disinformation in order to influence the choices of people.[8] Furthermore, States and big corporations in possession of this technology have a surveillance capacity that can easily result in the disruption of elections and other democratic processes.

---

[4] Opinion on *Carpenter v United States* [2018] U.S. available at https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf, accessed 29 July 2024.

[5] Kashmir Hill 'Israel Deploys Exetensive Facial Recognition Program in Gaza' *New York Times* 27 March 2024 available at https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html, accessed 29 July 2024.

[6] 'AI Watch: Global regulatory tracker – *Israel*' *White and Case* 13 May 2024 available at https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-israel, accessed 29 July 2024.

[7] *Feldstein* op cit note 1 at 5.

[8] Ibid, 6.

3.0 SOUTH AFRICA

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".[9]

In the absence of stronger regulation on facial recognition technology, the lack of regulation presents law enforcement with an opportunity to rely on such technology, despite well-founded concerns that facial recognition systems are often inaccurate, especially when it comes to identifying people of colour.[10]

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 Communications and Digital Technologies ('DCDT') put out a draft document outlining a plan for regulating AI in the forthcoming years.[11]

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.

---

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

10 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.

11 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.

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 Act[12] (RICA) unconstitutional.[13]

AmaBhungane submitted to the court that RICA was unconstitutional for the following reasons:

1. 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;
2. 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;
3. 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;
4. 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;
5. It failed to include a "public advocate" to represent the interests of people who have been targeted by the surveillance systems; and
6. 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.

---

[12] 70 of 2002.

[13] *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).

The High Court ruled in favour of amaBhungane, however it suspended the declaration of unconstitutionality for two years to allow Parliament to cure 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 judgment.[14] 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.[15]

The Court then considered whether this invasion was reasonable and justifiable in terms of section 36(1) of the Constitution.[16] It weighed the importance of the right to privacy and dignity[17], 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.

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 Act.[18] However, the Court disagreed, stating that section 2, in fact, does not authorise the practice of bulk surveillance, and is therefore unlawful and invalid.

---

[14] *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).

[15] Constitution of the Republic of South Africa, 1996.

[16] Ibid, Limitation of Rights.

[17] Ibid, Section 10.

[18] 39 of 1994.

In response to the amaBhungane invalidity judgment, the National Assembly introduced the General Intelligence Laws Amendment Bill.

This Bill proposes the legal 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.[19]

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.[20]

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 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)*.[21]

---

[19] 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.

[20] Ibid.

[21] 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).

4.0 INTERNATIONAL AND REGIONAL LEGAL MODELS

International Agreements

As yet, there are no binding international agreements on the regulation of AI, nor are there enforcement mechanisms for the misuse of AI. This presents notable concerns such as job losses of human operators due to the more cost effective and profitable gains that AI technology offers States and corporations. Furthermore, as noted in section 1 above, States and big corporations have the surveillance capacity, with the incorporation of AI, that can be used to disrupt elections and other democratic processes through misinformation and disinformation.[22] As such, they are now able to conduct surveillance on a much broader and intrusive scale. It is therefore more important than ever to have binding international regulatory agreements on AI surveillance technology.

Nevertheless, non-binding agreements have served as models for domestic regulations. Unfortunately, these policies say little about regulating the use of AI in surveillance systems. In 2019, South Africa became a party to the development of OECD guidelines on the use of AI **(OECD Council Recommendation of the Council on Artificial Intelligence OECD/LEGAL/0449(2019))**. The guidelines encourage member states to develop regulations that respect human rights, particularly the right to privacy.

Member States are further encouraged to develop accountability mechanisms and invest in research programmes related to all forms AI technology that operate in their territories. The guidelines suggest that research programs and accountability regulation mechanisms should focus on how AI technology effect individuals' right to privacy particularly with respect to their personal data, which is surveyed by these AI systems.[23]

In March 2024, the United Nations passed a resolution titled **"Seizing the opportunities of safe, secure, and trustworthy artificial intelligence systems for sustainable development."** South Africa is a party to this resolution, which only briefly touches on issues of privacy and surveillance but encourages member states to "[foster] the development, implementation, and disclosure of mechanisms of risk monitoring and management including personal data protection and privacy policies."[24]

---

[22] Feldstein op cit note 1 at 6.

[23] Recommendation of the Council on Artificial Intelligence [2019] OECD available at https://legalinstruments.oecd.org/Recommendations, accessed 29 July 2024.

[24] Draft United Nations Resolution 'Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development' (11 March 2024) RES/78/265 available at https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf, accessed 29 July 2024.

European Union

The European Union's approach to AI regulation appears to be the most comprehensive in the world and could serve as a model for South Africa's approach to regulating AI. In 2024, the EU passed the **AI Act**. The Act divides different uses of artificial intelligence into three categories: unacceptable risk; high risk; and low risk. Each category comes with its own unique regulations.

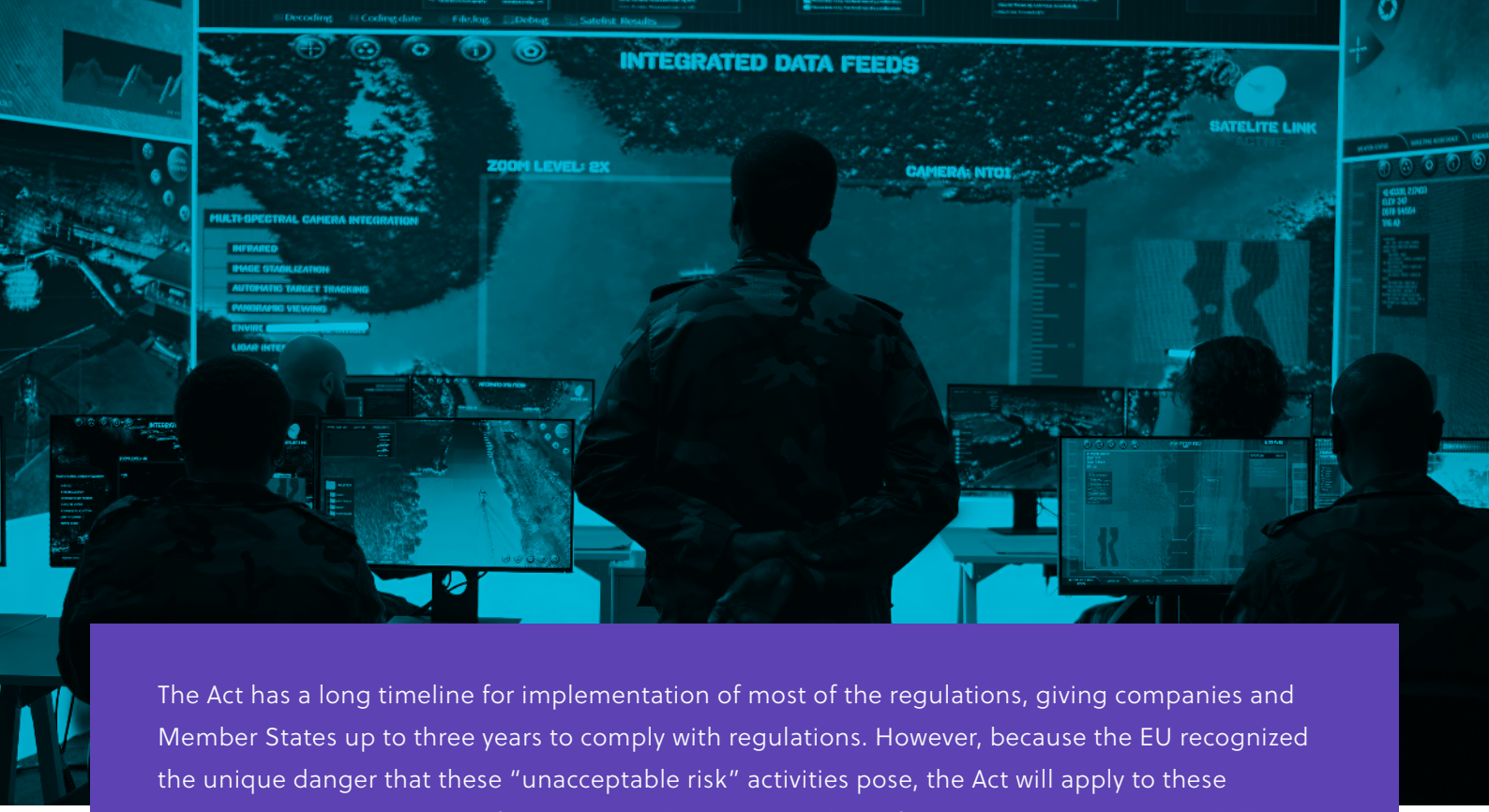
Uses of AI that are considered an 'unacceptable risk' include - behavioural manipulation of people or specific vulnerable groups (i.e. children's toys), social scoring based on an individual's personal data, biometric identification and categorization of people, and real-time identification systems like facial recognition.

Similar to POPIA, the AI Act contains some exceptions, but these exceptions are quite narrow. For instance, law enforcement can use real-time facial recognition, but only with prior authorization by a judicial or administrative authority within a Member State.

Law enforcement can petition to use real-time identification only in certain serious cases, like searching for missing persons, identifying victims of human trafficking, preventing a terrorist attack, or identifying suspects in high-level crimes like murder or rape.

Without such authorization, real-time facial recognition can only be used in high-profile cases if serious harm would result from delayed authorisation. In such cases law enforcement must still request authorisation within 24 hours of using the real-time identification technology.

If the request is subsequently denied, the agency must cease using the surveillance technology and delete all data and results that were collected.



The Act has a long timeline for implementation of most of the regulations, giving companies and Member States up to three years to comply with regulations. However, because the EU recognized the unique danger that these "unacceptable risk" activities pose, the Act will apply to these activities within six months of enactment. The Act entered into force on 2 August 2024, and all prohibitions on unacceptable risk uses of AI will be enforceable on 2 February 2025.

'High risk' uses of AI include any use of AI that has the potential to negatively affect safety or fundamental human rights. This would include AI systems used in especially dangerous products like cars, children's toys; or AI systems used in particularly important sectors like transportation or medicine. Most relevant to surveillance concerns is the requirement that AI systems used in 'high-risk' fields must be registered with the EU and monitored by a regulatory body. This includes uses of AI by law enforcement or border control. In the law enforcement context, this encompasses all technologies not included in the "unacceptable risk" category, which are used to assess - an individual's risk of becoming a crime victim, evaluate the results of polygraph exams, examine evidence, an individual's risk of committing an offence based on past behaviour, or profile criminals. In the migration and border control context, 'high-risk' uses include AI technologies used to - assess polygraphs, examine applications for asylum or residency, or identify individuals beyond verifying travel documents. Companies that provide 'high-risk' AI systems must establish a risk management plan and take several steps to ensure compliance with the AI Act like mitigating bias in the system, being transparent about the potential risks of the system, the data that the system uses, and designing the system to require human oversight. These systems will be monitored for accuracy and to prevent potential bias.

Lastly, all uses of generative AI, like ChatGPT, are considered 'low risk'. However, the AI Act still requires that generative AI systems publish summaries about the data used to train these systems to ensure that they are not trained on biometric data, thereby threatening individuals' privacy. The enforcement mechanism of the Act allows the EU to fine tech companies the equivalent of €35 million or 7% of their global revenue, whichever is higher. However, the EU has much less power to oversee the use of AI by public entities like law enforcement or border control, which leaves the regulations on surveillance somewhat vulnerable.

Case Studies (Australia, Canada, United States, and United Kingdom)

One of the hallmarks of the EU AI Act is the use of risk categorization to prioritize the regulation of AI that poses a direct threat to privacy and human rights. Other countries have also used such categorization to design their AI regulations. For instance, in 2024 Australia released its interim response, which, like the DCDT's draft document, focused primarily on economic harms.

However, the Australian report created a definition of "high-risk" systems based on the EU AI Act, which included AI systems used in law enforcement, border control, biometric identification, and emotion recognition. As the law develops, these AI uses should face the highest level of regulation.[25]

In 2022, Canada first submitted its **Artificial Intelligence and Data Act (AIDA)** to Parliament. The Act is still being developed in Parliament. AIDA classifies certain uses of AI as "high-impact," including uses of AI in law enforcement, immigration, and processing biometric data. Entities responsible for high-impact systems must identify risks of harms and establish measures to mitigate such harms. The entity responsible for the system must also publicize certain information about the system, including its risks and the corresponding mitigation measures.

Ministers have the power to require that entities in charge of "high-impact" systems provide further information about the system and may require the termination of a system that has the potential to create serious harm.[26]

---

[25] Safe and responsible AI in Australia consultation: Australian Government's interim response (2024) Department of Industry, Science and Resources available at https://storage.googleapis.com/converlens-au-industry/industry/p/prj2452c8e24d7a400c72429/public_assets/safe-and-responsible-ai-in-australia-governments-interim-response.pdf, accessed 29 July 2024.

[26] The Digital Charter Implementation Act, Bill C-27 of 2022.

Some countries have developed infrastructure to test AI systems and monitor potential harms before they enter the market. In November 2023, the United Kingdom launched the AI Safety Institute, and the United States announced its own AI Safety Institute in February 2024. These consortia are relatively new; therefore it is unclear how they will function. However, both institutes advertise that one of their aims is to test AI systems to ensure that they don't infringe on individual's human rights.[27]

5.0 CONCLUSION

In *amaBhungane*, the South African judiciary has made it clear that surveillance should not violate human rights. South Africa must move quickly to regulate AI surveillance because evidence suggests that the use of this technology and the misuse of personal data have the potential to cause significant harm.

The South African legislature needs to understand that regulating AI surveillance is important for the purpose of protecting fundamental human rights. The legislature could consider the existing policies of the European Union, Australia and Canada, as they have the most comprehensive policies and regulatory frameworks that could be tailored for the South African context. Accordingly, the regulation of AI surveillance should be prioritized over other regulations pertaining to AI, such as the threat that generative AI poses to copyright law.

As explained, the General Intelligence Amendment Bill is supposed to provide more insight on how surveillance should be regulated but the bill does not explicitly deal with AI. This is a clear oversight and must be rectified as surveillance regulations without the consideration of AI will likely lead to the violation of human rights in the future.

Law enforcement should be barred from using real-time facial recognition without prior judicial approval, subject to limited exceptions. Finally, the private use of AI powered surveillance technology, especially facial recognition technology, should be banned.

[27] Prime Minister's Office, Department for Science, Innovation and Technology, The Rt Hon Michelle Donelan and The Rt Hon Rishi Sunak MP 'Press Release: Prime Minister launches new AI Safety Institute' 2 November 2023, available at https://www.gov.uk/government/news/prime-minister-launches-new-ai-safety-institute, accessed 29 July 2024.

WE LOOK FORWARD TO CONNECTING WITH YOU.

www.lrc.org.za

info@lrc.org.za

LRCSouthAfrica

lrcsouthafrica

LRCSouthAfrica

Legal Resources Centre

LRCSouthAfrica

JOHANNESBURG/NATIONAL OFFICE
Tel: +27 11 038 9709

CAPE TOWN OFFICE
Tel: +27 21 879 2398

DURBAN OFFICE
Tel: +27 31 301 7572

MAKHANDA OFFICE
Tel: +27 46 622 9230

LRC LEGAL RESOURCES CENTRE