WERKSMANS
ATTORNEYS

REGULATORY

Privacy: human right or fallacy in the digital world?

7 February 2024 *6 min read*

> *"The real question is, when will we draft an artificial intelligence bill of rights? What will that consist of? And who will get to decide that?"*
>
> *-Gray Scott*

The increased reliance on online services and the desire for connectivity in the daily lives of people cannot but introduce an evolving notion of privacy. In an environment where individuals shift many of their activities into the "cyberspace" we need to consider to what extent this behaviour impacts on the fundamental rights that the South African Constitution guarantees. Does this it in itself call for the institution of new rights for cyberspace or could existing human rights be applicable within the online sphere?

In other words, time has arrived to consider how critical privacy and data protection is to the wider impact of developing digital technologies on other interdependent human rights.[1]

The United Nations Human Rights Council and General Assembly ("**Human Rights Council**") reiterated that the "*same rights that people have offline must also be protected online*".[2] The Human Rights Council has also repeatedly affirmed the importance of applying a comprehensive human rights-based approach when providing and expanding access to the Internet.[3]

Individuals share thoughts and opinions online and often without restraint. This would suggest that attitudes towards privacy and data protection might have been recalibrated. This behaviour directly links to fundamental human rights such as freedom of expression and the right to privacy, including the right not to be surveilled.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act ("**RICA**") was passed in 2002 and came into effect in 2005. It regulates when government can surveil citizens through the interception of their communications. At the same time, its aim is to protect the privacy of communications, with exceptions, which are limited to serious crimes or threats to national security.

RICA was amended during the latter half of 2023 in line with the Constitutional Court judgement of *amaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services and Others* **[4]** ("**amaBhungane Judgement**"). Considering privacy and concerns as to surveillance, the following changes were incorporated —

- provision for the adequate notification of surveillance subjects as soon as notification can be given, without jeopardising the purpose of the surveillance and after surveillance has been terminated;
- considering *ex parte* applications sought and obtained, provision has been made for safeguards for interception directions;
- procedures have been prescribed to ensure that data obtained pursuant to surveillance or interception is managed and not used unlawfully, including a lack of procedures for the processing of the data obtained.

These are important amendments to RICA. RICA, amongst others, however also requires telecommunication service providers to retain data over a three year period. Sutherland, J stated in the **amaBhungane Judgement** the following —

> *"In short, all of a person's personal telecommunications, up to three years past, lie in wait for the state to pry into, if its officials convince a judicial officer to authorise access"*

The European Court of Human Rights ("**ECtHR**") stated that the European Convention on Human Rights ("**ECHR**") is a living instrument anchored to the reality of the Member States in which it applies,[5] a principle that is immediately relevant to the impact of technological changes on society. The Court has determined that the notion of private life is a broad one, not susceptible to exhaustive definition; that personal data can be defined as any information relating to an identified or identifiable individual and that public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. These same principles have been adopted in the South African legal system.

As early as 1984, the ECtHR provided guidance on the principles governing interception and more general programs of surveillance in relation to evolving monitoring capabilities —

> *In particular, the requirement of foreseeability cannot mean that an individual should, — be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence (emphases added).[6]*

The integration of large-scale data mining and artificial intelligence facilitates mass surveillance.[7] Steven Feldstein[8] states that governments globally "*are deploying advanced artificial intelligence surveillance tools to monitor, track, and surveil citizens to accomplish a range of policy objectives, some lawful, others that violate human rights, and many of which fall into a murky middle ground*".

But what does this all mean? In a nutshell the following —

- Governments must respect, protect and fulfil human rights, and are obliged to ensure that they employ "judicial, administrative, educative and other appropriate measures in order to fulfil their legal obligations".[9]
- Businesses, particularly as regards the technology sector, have specific responsibilities when they develop or use technologies with the potential to interfere with the enjoyment of human rights.[10]

Without addressing ethics, technology and artificial intelligence can be a cause of chaos and suffering for humanity. The evolution of technology and artificial intelligence should always be guided by human values and the protection of human rights.

> *"I'm increasingly inclined to think that there should be some regulatory oversight, maybe at the national and international level, just to make sure that we don't do something very foolish. I mean with artificial intelligence we're summoning the demon."*
>
> *– Elon Musk*

This is Part 1 of our series on *Human Rights in the digital world.*

---

[1] Andrew, J and Bernard F (ed) in Human Rights Responsibilities in the Digital Age (1st ed) 2023 2

[2] Resolution adopted by the General Assembly on 16 December 2020 (UN Doc A/HRC/RES/75/176, 4 and 6).

[3] A/HRC/RES/75/176, 2

[4] 2021 (3) SA 246

[5] *Tyrer v UK,* no 5856/72 (25 April 1978) 31; *Marckx v Belgium,* no 6833/74 (13 June 1979) 41

[6] *Malone v UK,* no 8691/79 (2 August 1984) 67

[7] Andrew, J and Bernard F (ed) 6 [1]

[8] Feldstein, S The Global Expansion of AI Surveillance https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 last accessed 31 January 2024

[9] Human Rights Committee, General Comment No 31, `*The Nature of the General Legal Obligations Imposed on States Parties to the Covenant*' (26 May 2004) UN Doc CCPR/C/21/Rev.1/ Add.13, 7.

[10] UN Doc CCPR/C/GC/34 (12 September 2011) 7; Council of Europe, Committee of Ministers, `*Recommendation CM/Rec(2012)4 on the Protection of Human Rights with Regard to Social Networking Services*' (4 April 2012); European Commission, `*Recommendation (EU) 2018/334 on Measures to Effectively Tackle Illegal Content Online*' (1 March 2018); OECD, *An Introduction to Online Platforms and Their Role in the Digital Transformation* (Paris, OECD Publishing, 2019)



Ahmore Burger-Smidt

Head of Regulatory

View Profile

Keep us close