

Actualité

SURVEILLANCE AND DEMOCRACY

Human rights in the age of artificial intelligence: what is at stake

WHEN we speak about artificial intelligence (AI) and surveillance, it is tempting to think of distant technologies operating somewhere in the background, complex systems that have little to do with our daily lives. But in reality, surveillance today reaches into the most intimate spaces of our existence – our phone calls, our messages, our opinions, even our private moments. What once required targeted investigation can now be done quietly, continuously, and at scale. Recent events in Mauritius have made this impossible to ignore. They have shown, in the starkest terms, that surveillance is no longer a theoretical concern, but an immediate, deeply personal one, capable of shaping not only individual lives, but the very fabric of our democracy.

In October and November 2024, just weeks before the general elections, the country was shaken by what became known as the *Missie Moustass leaks*. Audio recordings of private conversations between politicians, journalists, diplomats, and public figures were leaked online. Some of those involved even confirmed that the conversations were genuine. For many Mauritians, the shock was not only about what was said in those recordings, but about how those conversations had been obtained in the first place. The idea that private calls could be intercepted, recorded, and later broadcast to the entire nation raised a deeply unsettling question: who is listening, and how far does that power go?

The situation escalated when access to social media platforms was briefly suspended just days before the elections, with authorities citing national security concerns linked to the leaks. This moment crystallised something important for the public. It showed how surveillance, technology, and political power can intersect in ways that directly affect democratic life – what people hear, what they can say, and how they participate in elections. This is exactly where AI and modern surveillance technologies come into focus.

Today, surveillance is no longer limited to traditional wiretapping. With AI, systems can analyse massive amounts of data – messages, calls, online activity – quickly



by Melany NAGEN,
Deputy Chairperson of the National
Human Rights Commission

Transparency is equally important. People should not feel that they are living under invisible systems that watch without explanation. The events surrounding the *Missie Moustass leaks* highlighted how damaging secrecy can be. When surveillance operates in the shadows, it erodes trust – not only in institutions, but in the very idea of justice. At the same time, individuals must feel empowered, not helpless, in the face of technology. People have a right to know when decisions affecting them are influenced by automated systems. They should be able to question those decisions and challenge them if they are unfair. Whether it is a decision about investigation or public services, no one should be left at the mercy of an unexplainable machine.

However, beyond laws and institutions, there is something even more powerful: awareness. The Mauritian public's reaction to the leaks and the temporary social media ban showed that citizens care deeply about their freedoms. When people understand what is at stake, they speak up. They question. They resist. And that is essential in any democracy. The reality is that surveillance is already part of modern life, and it will only grow. The real issue is not whether it exists, but how it is controlled. Will it be guided by clear laws, fairness, and respect for human dignity? Or will it quietly expand in ways that reshape our freedoms without us noticing? Mauritius now stands at a defining moment. The *Missie Moustass* episode was more than a political scandal – it was a wake-up call. It revealed the real risks of unchecked surveillance in a digital age. But it also showed the strength of public awareness and the importance of protecting fundamental rights.

As Mauritius continues its digital transformation, it has a unique opportunity to lead by example. By placing human rights at the centre of how technology is used, the country can ensure that AI strengthens democracy rather than weakens it. Surveillance, if it exists, must never become a tool of control or intimidation. It must remain what it is meant to be – a tool of protection, guided by law, accountability, and above all, respect for human dignity.



and often invisibly. They can detect patterns, predict behaviour, and even flag individuals as 'risks.' This makes surveillance more powerful than ever before, but also more dangerous if left unchecked. That is why safeguards matter. If surveillance tools are used, there must be strong and independent oversight. Decisions to monitor individuals – especially their private communications – should never be taken lightly. Courts and independent bodies must be involved to ensure that such actions are lawful, necessary, and proportionate. Without this, surveillance can easily shift from protection to intrusion.

L'IA et les risques potentiels pour les droits : Enjeux, défis et réalités locales

L'INTELLIGENCE artificielle (IA) transforme profondément les sociétés contemporaines en influençant la gouvernance, l'économie et les interactions sociales. À Maurice, État insulaire engagé dans une stratégie de transformation numérique, l'IA est progressivement intégrée dans les services publics et les dispositifs de sécurité.

Des initiatives telles que le programme Safe City ou les plateformes d'e-Government illustrent cette évolution. Toutefois, comme le soulignent les normes internationales de l'Unesco, l'IA doit être encadrée afin de garantir le respect des droits fondamentaux. Cet article, analyse les risques liés à l'IA à Maurice en s'appuyant sur des exemples concrets du contexte local.

► Safe City : surveillance intelligente et vie privée

Le programme Safe City, développé à Maurice, repose sur l'utilisation de caméras de vidéosurveillance avancées, dont certaines intègrent des capacités d'analyse algorithmique. Ce système vise à renforcer la sécurité publique, notamment dans les zones urbaines et sensibles.

Cependant, l'utilisation de technologies de reconnaissance et d'analyse comportementale soulève des questions importantes concernant le droit à la vie privée. Bien que la Constitution mauricienne protège les libertés fondamentales, l'extension de la surveillance numérique peut créer un sentiment de contrôle permanent. L'usage de l'IA dans la vidéosurveillance pose également des défis en matière de transparence et de contrôle démocratique, comme l'ont souligné des organisations de la société civile à plusieurs reprises.

► Digitalisation de l'administration et risques liés à l'e-Government

Maurice a développé plusieurs plateformes d'e-Government visant à simplifier les démarches administratives (impôts, état civil, services sociaux). Ces systèmes reposent de plus en plus sur des outils automatisés et des algorithmes d'aide à la décision.



par Jean Marie RICHARD, membre de la NHRC

Par exemple, certains services en ligne du gouvernement utilisent des systèmes automatisés pour traiter les demandes des citoyens plus rapidement. Toutefois, cette automatisation peut comporter des risques : des erreurs dans le traitement des données, une absence de recours humain rapide et un risque d'exclusion des citoyens moins familiers avec le numérique. La digitalisation des services publics devrait donc garantir l'inclusion et la transparence afin d'éviter une fracture numérique.

► Discrimination algorithmique dans les services publics et privés

Dans notre contexte multiculturel, l'utilisation d'algorithmes dans les secteurs public et privé peut reproduire des biais existants. Notamment, les systèmes de tri de candidatures dans les ressources humaines peuvent favoriser certains profils, tandis que des outils financiers automatisés peuvent influencer l'accès au crédit bancaire. Ces mécanismes risquent d'accentuer les inégalités sociales, en contradiction avec le principe d'égalité inscrit dans la *Constitution of Mauritius* et les normes internationales de l'Organisation des Nations unies.

► Risques de désinformation numérique et réseaux sociaux

Ces dernières années, les réseaux sociaux sont devenus un espace central du débat public. L'IA y joue un rôle croissant à travers les algorithmes de recommandation et la génération de contenus. Des cas de diffusion de fausses informations politiques ou sociales ont été observés lors de périodes électorales ou de tensions sociales. L'émergence des *deepfakes* représente également un risque pour la crédibilité de l'information, pouvant affecter la confiance dans les institutions démocratiques, notamment lors des consultations électorales. Ce phénomène a été constaté par des observateurs, notamment en Roumanie et dans certains États africains lors de scrutins récents.

Par ailleurs, l'IA influence fortement certains secteurs clés de l'économie mauricienne, notamment les centres d'appels, les services financiers et l'administration publique. L'automatisation de certaines tâches répétitives peut entraîner une réduction des emplois traditionnels, en particulier dans les centres de relation client, où des systèmes automatisés remplacent progressivement certaines fonctions humaines. Selon l'Organisation internationale du travail, la transition vers l'économie numérique nécessite des politiques de reconversion professionnelle afin d'éviter une augmentation des inégalités sociales.

► Gouvernance numérique et encadrement juridique

L'IA représente une opportunité majeure pour la modernisation de Maurice, notamment à travers des projets comme Safe City et l'e-Government. Toutefois, ces avancées s'accompagnent de risques importants pour les droits humains : surveillance accrue, inégalités numériques, désinformation et transformations du marché du travail. Une gouvernance équilibrée, fondée sur le droit, l'éthique et l'inclusion, est essentielle pour garantir que l'IA serve le développement humain sans compromettre les libertés fondamentales. Maurice a ainsi l'opportunité de devenir un modèle régional de transformation numérique responsable.

AI and the new power game
When human rights could disappear

Imagine living in a real-world version of *Game of Thrones* – a landscape of shifting alliances, hidden actors, and relentless battles for power. In many ways, we already do. But today, the game is no longer played only by states and institutions. It is increasingly shaped by something far less visible, yet far more powerful: artificial intelligence (AI).

Because AI is no longer just a tool. It is a force multiplier. It allows individuals, groups, even anonymous actors, to wield influence once reserved for governments. Today, a small group of tech leaders, "AI architects" exercise extraordinary control over the most advanced systems.

And with power comes both promise and peril.

On one hand, AI offers extraordinary potential: improving efficiency, expanding access to information, and enhancing decision-making. On the other, it presents profound risks to fundamental human rights.

The right to privacy is under growing strain, as vast amounts of personal data are collected, analysed, and sometimes misused. Surveillance, once the domain of states, is now enabled by sophisticated technologies capable of tracking behaviour at an unprecedented scale.

Freedom of expression is also being reshaped. Digital platforms allow individuals to speak across borders, often anonymously. While this can empower voices, it also enables abuse. Harmful content can be generated, amplified, and disseminated at scale, often shielded behind fake identities or the dark web. In an age where AI can produce near-perfect text, images, and videos, authenticity itself becomes harder to discern. Ironically, imperfection and human error may soon become the only reliable marker of what is real.

Access to justice raises another set of questions. Can AI provide reliable legal advice? Can it assist, or does it risk reinforcing inequalities for those who lack the means or literacy to challenge automated decisions? According to Sir Geoffrey Vos, Master of the Rolls (UK), AI will not make lawyers redundant because the human mind will remain crucial to the interpretation and development of law, but it will mean that lawyers would have to be tech-savvy to guide clients through the "minefield of AI-driven justice."

Perhaps most concerning is the risk of discrimination. Algorithms are not neutral; they reflect the data on which they are trained. When that data carries bias, the outcomes can perpetuate and even deepen existing inequalities, often in ways that are difficult to detect or contest.

Against this backdrop, National Human Rights Institutions from across the world gathered on 1st April 2026 at the Annual Meeting of the Global Alliance of National Human Rights Institutions (GANHRI) to adopt an Outcome Statement on human rights in the digital space. The statement is a welcome and necessary step, reaffirming that human rights apply online just as they do offline, and calling for stronger safeguards, oversight, and accountability.



by Deepti THAKOOR, barrister-at-law

Yet, an uncomfortable truth remains.

In the digital space, it is often extremely difficult, if not impossible, to identify those responsible for harm. Perpetrators can hide behind layers of anonymity, fake profiles, and complex technological infrastructures that transcend borders and jurisdictions. Traditional models of accountability, which depend on identifying and prosecuting individuals, are no longer sufficient.

This calls for a fundamental shift in approach.

If responsibility cannot always be traced to individuals, it must be embedded within the systems themselves. The "AI architects" have the capacity, and therefore the responsibility, to design systems that can detect, prevent, and mitigate harm at its source because AI is developing at "swarp speed" according to *The Economist*.

Let us remember. Recently, Anthropic launched Claude Myths, a model astutely capable of finding software vulnerabilities, sending an alarm across US Treasury. However, this model was released selectively as it was too dangerous to go public. It was this same company that refused to allow Anthropic's model to be used in fully autonomous weapons or for mass domestic surveillance. Mr Amodei has taken a first step to contain the dangers of AI and it is now time that human rights considerations are built into a proactive design.

The current trajectory also reveals another risk: concentration of power. Ethics alone will not suffice. The GANHRI Outcome Statement is a laudable attempt to chart a path forward and state principles which should guide governments and the international community, especially to create accountability for human rights infringements. But like many international commitments, its impact will ultimately depend on the willingness and power interplay between states, and private actors, to translate principles into practice.

There is no doubt that AI holds enormous potential for the future. But a future that does not respect fundamental human rights is not a future we should accept. The real question is: *Do we build systems where power expands unchecked or systems that embed protection of human rights and human dignity in its very design?*

This is a choice we must make today.

CONTACTS UTILES

Pour toute information, accompagnement ou dépôt de plainte, voici les coordonnées essentielles de la NHRC

Adresse : 3^e étage, Ébène Heights, Ébène

● Secrétariat de la Commission — Tel: 460-5148
Email: mhrcdbs@intnet.mu
Fax: 468-6206

● Human Rights Division — Tel: 460-5148
Email: hrd-nhrc@govmu.org
Fax: 468-6241

● National Preventive Mechanism Division — Tel: 460-5151
Email: npmd-nhrc@govmu.org
Fax: 468-6233