ARTIFICIAL INTELLIGENCE, HUMAN INTERVENTION AND TRUST

Legal Safeguards for Accountability and Governance

By Navina Parsuramen
Assistant Parliamentary Counsel
Attorney-General's Office

Presentation

The launch of the **Mauritius National Data Strategy** invites us to reflect on trust, not as an aspiration, but as a legal construct.

In law, trust is sustained where power is exercised within defined boundaries, where responsibility is identifiable, and where individuals are not subjected to decisions they cannot understand or meaningfully challenge.

It is in that legal sense that Artificial Intelligence must now be considered.

Artificial Intelligence and the Shift in Decision-Making

Artificial Intelligence systems are increasingly deployed in contexts where data is no longer merely collected or analysed, but translated into recommendations, prioritisation, and outcomes.

From a legal perspective, this represents a decisive shift.

When data begins to shape decisions, the issue is no longer confined to privacy alone. It becomes a question of governance, accountability, and oversight.

That question becomes unavoidable whenever automated systems influence access to services, the prioritisation of cases, or the assessment of risk.

Speed, Accuracy, and the Need for Governance

At the same time, it must be recognised that Artificial Intelligence is fundamentally about speed and accuracy.

Its capacity to process information at scale and at pace is unmatched. For that reason, its adoption is not something to resist.

It is something that should be responsibly embraced.

But speed without governance does not generate trust.

The ethical use of Artificial Intelligence depends on clear data governance ensuring that data is lawfully sourced, appropriately used, and subject to accountability throughout its lifecycle.

Existing Legal Foundations

Our existing data protection framework already addresses part of this reality.

It regulates automated processing and profiling.

It recognises the risks associated with decisions taken without human involvement. It requires additional safeguards where processing is likely to affect individuals.

These principles remain sound and relevant.

What Artificial Intelligence introduces, however, is scale, complexity, and opacity that traditional legal assumptions did not fully anticipate.

AI systems may evolve after deployment.

They may influence outcomes in ways that are not immediately visible. They may support decisions without replacing them, yet still materially affect individuals.

For this reason, data protection remains foundational, but it must now operate within a broader ecosystem of governance safeguards, where AI systems shape outcomes.

International Approaches and Convergence

Internationally, this evolution has been clearly recognised.

The European Union’s approach to Artificial Intelligence, for example, is not centred on prohibiting technology, but on differentiating uses according to risk and calibrating safeguards to the level of potential impact.

What we see emerging internationally is a governance choice familiar to data protection law:

the higher the potential impact of automated systems on individuals, the stronger the legal safeguards and the clearer the human oversight must be.

At the centre of this approach lies a simple legal proposition:

Where AI systems affect rights, opportunities, or obligations, human oversight must remain central.

This is not a technical requirement.

It is a legal one.

Regulation as an Iterative Process

There is no single or definitive regulatory model for Artificial Intelligence.

The technology is evolving too rapidly for static legal solutions.

What is therefore required is a simple, proportionate data governance framework, capable of evolving over time.

An iterative regulatory approach must be favoured.

The law should set initial guardrails, allow deployment, observe impact, and adjust safeguards as risks and uses become clearer.

In the context of Artificial Intelligence, regulation is not a one-time act. It is a continuous legal process.

Many jurisdictions are already confronting this reality.

In that sense, the question is no longer whether to regulate Artificial Intelligence, but how to do so in a manner that keeps pace with its development.

Human Intervention and Legal Accountability

Human intervention is the point at which the law reasserts itself.

It ensures that decisions remain attributable to a human authority, that automated outcomes can be reviewed and questioned, and that responsibility does not dissolve into technical complexity.

In legal terms, human intervention is not an expression of distrust in technology. It is the means by which accountability is preserved.

Without it, the law is unable to secure the fundamental requirement that individuals have a clearly identifiable authority against whom responsibility and effective redress can be pursued.

This logic is not confined to a single jurisdiction or regulatory model.

Across different approaches - whether prescriptive, principles-based, or sector-specific - there is a clear convergence around one constant:

Artificial Intelligence may assist decision-making, but it must not displace human judgment in high-impact contexts.

That convergence reflects a shared international understanding that trust cannot be automated.

From a legal standpoint, trust is not built by the performance of systems, but by the availability of responsibility and effective redress.

Mauritius

For Mauritius, the relevance is clear.

We are not approaching AI governance from a blank slate.

We already have a solid regulatory foundation, encompassing data protection, cybersecurity and cybercrime frameworks, ICT regulation, and sector-specific oversight including tailored rules for AI-enabled advisory services in regulated domains.

The National Data Strategy provides the framework within which these elements can be aligned coherently.

The objective is not to multiply legal instruments, but to ensure clarity, proportionality, and consistency, particularly in identifying where automation may operate and where the law must insist on human involvement.

That is how trust is translated into enforceable governance.

Conclusion

I will conclude with this.

Artificial Intelligence will continue to evolve rapidly.

Legal frameworks will, by necessity, evolve with greater deliberation.

But one boundary must remain stable.

Where decisions affect people, the law must ensure that a human remains responsible.

Human intervention is not an obstacle to innovation.

It is the legal condition that allows innovation to endure.

That is how trust is protected.

And that is the responsibility the law must continue to carry.

Thank you.

This 28 January 2026