International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 20s, 2025
https://theaspd.com/index.php

AI In Corporations: Legal And Environmental Risks And Their Impact On Leadership, Governance, And Sustainability In Australia

Professor Bernard Wong[1]
[1]Enterprise Strategy Consulting, Charles Sturt University, Sydney, Australia bernardw@enterprise-strategy.org
*Corresponding Author: bernardw@enterprise-strategy.org

***Abstract*—** *Artificial Intelligence (AI) is rapidly transforming corporate governance and strategic decision-making in Australia. While AI enhances operational efficiency and data-driven innovation, its deployment raises critical legal, ethical, and environmental governance concerns. This paper examines the intersection of corporate AI use with Australia's regulatory landscape, focusing on legal risks such as data privacy breaches, algorithmic discrimination, surveillance, and cybersecurity vulnerabilities. It argues that responsible AI governance is essential not only for legal compliance but also for sustainable and ethical business conduct. By synthesizing statutory duties, case law, and international frameworks, this paper provides a governance roadmap for corporate leaders seeking to deploy AI responsibly within environmental, social, and legal boundaries. The findings have broader implications for environmental and technological stewardship, digital ethics, and corporate accountability. In addition, the paper examines how AI can both support and undermine environmental, social, and governance (ESG) obligations, urging corporations to adopt sustainability-aware governance practices.*

***Keywords*–** *Artificial Intelligence, Corporate Governance, Legal Risks, AI Regulation, Environmental Governance, Ethics, Australia*

I. INTRODUCTION

Artificial Intelligence's integration into corporate settings presents a dual-edged sword, offering operational and strategic benefits while generating complex legal and ethical risks. Businesses adopting AI must navigate a regulatory landscape, for example in the UK they need to comply with the UK GDPR, Equality Act 2010, Consumer Protection laws, and sector-specific guidance. For corporate leadership and management, this creates new imperatives around compliance, accountability, transparency, and ethical governance [1].

Australia's corporate sector is increasingly reliant on AI to enhance competitiveness. However, AI applications, particularly in employment, customer analytics, and decision-making, have prompted serious legal scrutiny. Although Australia has not enacted a unified AI Act, businesses are bound by laws such as the Privacy Act 1988 (Cth), Fair Work Act 2009 (Cth), and anti-discrimination statutes. Corporate leaders must now navigate a complex regulatory environment, develop governance frameworks, and embed ethical AI principles into their strategic operations [2].

This paper critically examines the principal legal risks associated with corporate AI use in Australia, including issues related to data privacy, discrimination, workplace surveillance, employment law, consumer protection, cybersecurity, and regulatory ambiguity. It explores how these legal risks impact leadership and management.

II. WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial Intelligence (AI) refers to a suite of technologies designed to perform tasks that typically require human intelligence. These systems can interact with their environments, process large amounts of data, interpret patterns, and adapt behavior based on continuous feedback. Glikson & Woolley define AI as "a new generation of technologies capable of interacting with the environment, gathering information, interpreting it, generating outputs, and improving decision systems to achieve specific objectives" [3]. This distinguishes AI from traditional automation, which is limited to pre-defined instructions without the capacity for learning or adaptation.

AI encompasses a variety of methods, including machine learning, neural networks, robotics, and natural language processing. According to Birkstedt et al, AI is not only a research field but also a "moving frontier

of computing" and a core enabler of the fourth industrial revolution [4].

Currently, most real-world applications involve what is termed "narrow AI". These are systems designed to perform specific tasks such as facial recognition or predictive text. This contrasts with "general AI" or "strong AI", which would demonstrate human-level reasoning across diverse tasks. The OECD further emphasizes that trustworthy AI systems must be fair, robust, explainable, and respect human rights [5].

III. Benefits of Artificial Intelligence

As Artificial Intelligence (AI) technologies mature, their transformative impact across sectors is increasingly evident. No longer confined to theoretical or experimental applications, AI is now driving measurable advancements in economic performance, decision-making accuracy, service personalization, public administration, and scientific research. Its capacity to automate tasks, derive insights from complex datasets, and adapt to evolving environments positions AI as a cornerstone of modern innovation. The following subsections explore five key domains where AI delivers significant benefits, illustrating how its strategic implementation enhances productivity, improves public and private sector operations, and accelerates discovery in ways previously unattainable through traditional means.

A. Economic Growth and Industrial Innovation

AI is widely regarded as a catalyst for economic growth and productivity. It automates complex workflows, optimizes supply chains, and reduces human error. Studies have shown that firms adopting AI outperform competitors in process efficiency and cost management. In R. (on the application of the Open Rights Group) v The Secretary of State for the Home Department [2021], the court highlighted the increasing role of algorithmic systems in decision-making processes and reinforced the need for transparency when such systems are deployed in public administration [6].

B. Enhanced Decision-Making

AI can process datasets at speeds and volumes beyond human capability. This has revolutionized sectors such as finance (e.g. in fraud detection), healthcare (e.g. AI-assisted diagnostics), and cybersecurity. For example, in R (Bridges) v Chief Constable of South Wales Police [2020], the Court of Appeal found that the police use of facial recognition technology required appropriate legal safeguards to protect individual rights under the Human Rights Act 1998 and GDPR [7][8][9].

C. Personalized User Experience

Through algorithms, AI systems personalize user experiences across platforms, from Netflix recommendations to dynamic pricing in e-commerce. These services rely on profiling and behavioral tracking, which has raised questions about fairness and data protection. The UK Information Commissioner's Office has provided guidance emphasizing the need for lawful basis and data minimization when using AI for personalization [10].

D. Public Sector Efficiency

AI is increasingly used by governments to automate administrative processes, monitor infrastructure, and support public health initiatives. For example, AI was used to model COVID-19 transmission trends and manage emergency responses. Aaronson, observes that although 814 AI policy initiatives have been reported to the OECD, only 0.49% have been formally evaluated, highlighting the urgent need for accountability mechanisms [5][11].

E. Scientific and Technological Discovery

AI accelerates research and development by enabling predictive modelling in domains like climate science, drug development, and materials engineering. In AI-enabled drug discovery, for instance, DeepMind's AlphaFold project predicted protein structures with unprecedented accuracy, which is expected to revolutionize biomedical science [12].

F. AI for Environmental Monitoring and Compliance

AI plays a growing role in environmental science and sustainability. AI-powered systems are used to monitor air and water quality, track carbon emissions, optimize energy usage, and forecast environmental risks such as floods, bushfires, and extreme weather. For example, organizations like CSIRO and the Bureau of Meteorology in Australia have adopted AI for predictive climate modelling. Such tools are essential for achieving national and corporate environmental targets, and ensuring compliance with frameworks like ISO 14001 and the GRI Standards.

IV. What are the Risks of Artificial Intelligence?

Despite the substantial benefits of Artificial Intelligence (AI), its deployment introduces a spectrum of legal, ethical, and operational risks. These risks arise from AI's opacity, autonomy, data dependency, and capacity to replicate human bias at scale. As Glikson & Woolley note, the very features that make AI powerful, its ability to learn, adapt, and act autonomously, also render it unpredictable and difficult to regulate, especially when embedded in socio-technical systems that affect people's rights and opportunities [3].

A. Data Privacy and Surveillance

AI systems frequently depend on vast datasets containing personal or sensitive information. This creates substantial risks regarding data over-collection, misuse, and unauthorized profiling. In R (Bridges) v Chief Constable of South Wales Police [2020], the Court of Appeal ruled that the use of facial recognition technology by police lacked sufficient legal oversight, transparency, and proportionality, thereby violating data protection standards [7].

In Australia, the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs), especially APPs 1 and 11, govern the collection, use, and security of personal information by AI systems [13][14]. The Office of the Australian Information Commissioner underscores the need for human oversight, transparency, and privacy-by-design approaches to mitigate these risks [15].

B. Algorithmic Discrimination and Bias

AI can perpetuate or amplify societal biases, particularly in areas like recruitment, credit scoring, or customer analytics. This may lead to indirect or systemic discrimination, even without intentional harm. In IW v City of Perth (1997), the High Court recognized that indirect discrimination may occur regardless of intent, laying the foundation for interpreting algorithmic bias under Australian anti-discrimination laws [16].

Applicable statutes include the Sex Discrimination Act 1984 (Cth), Racial Discrimination Act 1975 (Cth), and state-based laws such as the Equal Opportunity Act 2010 (Vic) and Anti-Discrimination Act 1977 (NSW) [17][18][19][20]. Unchecked AI systems may violate these laws if outputs disproportionately affect protected groups.

C. Employment Law and Workplace Surveillance

AI tools used for monitoring employee behavior, assessing productivity, or automating dismissal decisions pose risks under employment law and privacy rights. In Lopez Ribalda v Spain [2019], the European Court of Human Rights held that covert video surveillance breached Article 8 ECHR (right to privacy), setting an important precedent for balancing workplace monitoring with individual rights [21].

In Australia, AI systems may conflict with provisions of the Fair Work Act 2009 (Cth) and Surveillance Devices Act 2007 (NSW) if used without employee consultation or transparent policies [22][23].

D. Consumer Protection and Contractual Liability

AI systems that fail to meet performance guarantees may expose companies to liability under contract and consumer law. Misleading representations of AI capabilities could constitute deceptive conduct. In ACCC v Trivago N.V. [2020], the Federal Court found that algorithmic manipulation of hotel rankings amounted to misleading conduct under the Australian Consumer Law (ACL) [24][25].

In contract law, parties may rely on doctrines of misrepresentation if AI-generated outputs were central to the bargain but proven inaccurate or biased (see Misrepresentation Act 1967 (UK), s 2(1)) [26]. Australian law requires accurate disclosure of AI limitations, especially when used in high-risk applications.

E. Cybersecurity Threats

AI systems are vulnerable to novel threats including adversarial attacks, data poisoning, and model inversion. These risks may result in data breaches, regulatory violations, or national security threats. The Security of Critical Infrastructure Act 2018 (Cth) and APP 11 mandate organizations to implement measures to secure AI systems that manage personal or critical infrastructure data [27][28].

Leadership must conduct AI-specific threat assessments and build cybersecurity resilience into AI governance frameworks.

F. Lack of Explainability and Transparency

"Black box" AI systems pose risks to accountability and user trust, particularly when used in decision-making that affects individual rights. Although Australia does not provide a general "right to explanation"

akin to GDPR Article 22, a failure to explain AI outcomes may violate administrative fairness, privacy obligations, and consumer protection laws [2].

Aaronson, stresses that governments and corporations must conduct credible evaluations of AI systems to foster trust and ensure legal compliance, yet fewer than 1% of global AI initiatives had been meaningfully evaluated as of 2022 [11].

G. Regulatory Uncertainty

Australia lacks a comprehensive AI Act. Instead, businesses operate within a fragmented legal framework of privacy, consumer protection, and anti-discrimination laws. The AI Ethics Framework and OAIC guidelines offer voluntary principles but are not legally binding [29][30]. This regulatory ambiguity creates compliance uncertainty and increases exposure to litigation or reputational harm.

H. Environmental Governance and Greenwashing Risks

AI is increasingly integrated into ESG reporting, particularly for monitoring environmental impacts such as emissions, waste management, and resource consumption. However, if these systems produce inaccurate, manipulated, or unverifiable data, companies may be exposed to greenwashing claims. Misrepresenting environmental performance, whether intentionally or due to the use of flawed AI, may violate consumer law and mislead investors or regulators [31].

I. Energy Consumption and Environmental Externalities of AI

AI systems, particularly those using large-scale machine learning models (e.g. deep learning), consume significant energy and water resources. Training large language models, such as GPT-4, or running AI-enabled logistics operations can exacerbate carbon emissions and resource depletion, thereby undermining corporate climate targets and environmental sustainability efforts.

*J.*Supply Chain and Human Rights Due Diligence Failures

AI used in procurement, logistics, and supplier monitoring may overlook or misrepresent ESG risks within global supply chains, such as modern slavery, environmental violations, or unsafe labor practices [32].

V. How Organizations Can Manage The Risks Of AI: Governance Strategies And Recommendations

The deployment of Artificial Intelligence (AI) in corporate environments introduces legal, ethical, operational, and reputational challenges. These risks span privacy violations, algorithmic discrimination, unfair labor practices, consumer deception, and cybersecurity breaches. In response, organizations must adopt a structured, multi-layered governance approach grounded in statutory compliance, best practices, and emerging international norms. The following expanded strategies offer actionable governance recommendations supported by legal precedent and global standards.

A. Establish Comprehensive AI Governance Frameworks

AI governance frameworks are necessary to ensure that AI systems align with ethical principles, legal standards, and organizational goals. These frameworks must address accountability, transparency, stakeholder engagement, and the allocation of oversight responsibilities.

The UTS Human Technology Institute proposes eight foundational elements for effective AI governance, including stakeholder co-design, ethical infrastructure, and human rights alignment [33]. Similar principles are endorsed in the OECD AI Principles [5] and UNESCO's Recommendation on the Ethics of AI [34].

Telstra's Risk Council for AI & Data (RCAID) exemplifies board-level oversight, with clear reporting lines and AI-specific risk registers [35].

Section 180 of the Corporations Act 2001 (Cth) imposes a duty of care and diligence on directors, which now arguably includes oversight of AI risks.

Recommendation: Form AI oversight committees that report directly to the board, incorporating ethics officers, technologists, and legal counsel. Codify AI governance principles in organizational charters and risk management policies.

B. Implement AI Impact Assessments (AIAs)

AIAs are formal tools to evaluate and mitigate potential harms associated with AI systems before and during deployment. They are especially critical in high-stakes sectors like healthcare, finance, and criminal justice.

For example, Microsoft's Responsible AI Impact Assessment framework includes risk scoring, stakeholder consultation, and mitigation strategies [36]. International standard ISO/IEC 42005:2023 provides a structure for AI risk identification and treatment [37].

In R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058, the court criticized the absence of structured impact assessments for facial recognition, emphasizing the need for pre-deployment legal scrutiny [7].

Recommendation: Make AIAs mandatory for high-risk systems and integrate them with Privacy Impact Assessments (PIAs) and Human Rights Impact Assessments (HRIAs) to ensure holistic legal coverage [38][39].

C. Embed Privacy-by-Design and Data Governance

AI systems must comply with the Privacy Act 1988 (Cth) and Australian Privacy Principles (APPs). APPs 1 and 11 require open data practices and robust information security [12][13]. The OAIC also advises on algorithmic transparency and human oversight [40].

In R (Bridges) v Chief Constable of South Wales Police [2020], facial recognition technology was ruled unlawful for lacking sufficient transparency and proportionality [7].

Recommendation: Conduct regular Data Protection Impact Assessments (DPIAs) and implement transparent consent, opt-out mechanisms, and data minimization practices [41].

D. Preventing Algorithmic Discrimination

AI systems trained on biased data may violate the Sex Discrimination Act 1984 (Cth), Racial Discrimination Act 1975 (Cth), and Age Discrimination Act 2004 (Cth). Discrimination may be indirect, even without intent, as held in IW v City of Perth (1997) 191 CLR 1 [[16]17][18][42].

In IW v City of Perth (1997) 191 CLR 1, the High Court of Australia affirmed that indirect discrimination can be unlawful irrespective of the discriminator's intent, establishing a foundational principle that extends to algorithmic decision-making where biased outcomes may result from seemingly neutral processes. This is reinforced by the Sex Discrimination Act 1984 (Cth), Racial Discrimination Act 1975 (Cth), and Age Discrimination Act 2004 (Cth), which impose strict liability on organizations for discriminatory practices, regardless of intent, if their actions disproportionately disadvantage protected groups.

Recommendation: Conduct algorithmic bias audits, ensure the use of diverse and representative datasets, and embed "human-in-the-loop" decision-making for critical applications.

E. Address Workplace Surveillance Lawfully

AI-driven employee monitoring tools, such as keystroke logging, facial recognition, and sentiment analysis, can infringe upon workers' privacy rights, particularly when implemented without their knowledge or consent. The legal risks of such surveillance are underscored by the decision in Lopez Ribalda and Others v Spain (2019), where the European Court of Human Rights found that covert video surveillance of supermarket employees violated Article 8 of the European Convention on Human Rights, which protects the right to private life [21].

In Australia, similar principles are embedded in domestic legislation. The Fair Work Act 2009 (Cth) requires fair and lawful treatment of employees, while the Surveillance Devices Act 2007 (NSW) mandates explicit consent and transparency in the use of surveillance technologies in the workplace [22][23]. Accordingly, organizations must ensure that AI-enabled monitoring systems are deployed lawfully, with clear policies, prior consultation, and informed consent to avoid breaching statutory and common law privacy protections.

Recommendation: Engage employees and unions in policy development. Disclose the nature, purpose, and limits of surveillance tools. Avoid covert deployments.

F. Minimize Consumer and Contractual Liability

AI-generated outputs that mislead or unfairly disadvantage consumers can expose organizations to liability under the Australian Consumer Law (ACL), as set out in Schedule 2 of the Competition and Consumer Act 2010 (Cth) [24].

In ACCC v Trivago N.V. [2020] FCA 16, the Federal Court held that Trivago's algorithm, which falsely represented the cheapest hotel options breached section 18 of the ACL by engaging in misleading or deceptive conduct [25]. This precedent demonstrates that the use of AI does not exempt companies from

consumer protection obligations, particularly where algorithmic decisions influence purchasing behavior. Furthermore, if representations about the accuracy or performance of AI systems are later found to be false or misleading, organizations may also be liable under contract law doctrines, including misrepresentation. While the Misrepresentation Act 1967 (UK) provides a statutory remedy in the UK [26], equivalent common law principles apply in Australia, exposing vendors and service providers to potential claims where consumers rely on inaccurate AI-driven outputs.

Recommendation: Ensure marketing claims about AI accuracy or benefits are validated and disclosed. Draft AI-specific contract clauses that allocate liability, set performance standards, and include fallback procedures.

G. Implement Cybersecurity-by-Design

AI models are vulnerable to adversarial attacks, data poisoning, and security breaches, which can compromise the integrity, confidentiality, and reliability of AI outputs. These risks are particularly acute when AI is applied to critical infrastructure, personal data processing, or high-stakes decision-making. Under Australian Privacy Principle 11 (APP 11) and the Security of Critical Infrastructure Act 2018 (Cth), organizations are legally required to implement reasonable steps to protect personal and sensitive information from misuse, interference, loss, and unauthorized access [14][27].

Recommendation: Apply ISO 27001 and ISO/IEC 42001 for AI-specific cybersecurity and resilience [43][44]. Regularly audit third-party AI tools and implement anomaly detection systems for AI behavior.

H. Foster Public Engagement and Co-Design

The Human Technology Institute emphasizes that involving impacted communities strengthens accountability and innovation [45]. Meaningful stakeholder engagement is essential to enhancing the legitimacy, trustworthiness, and effectiveness of AI systems. Involving users, affected communities, and civil society organizations in the design, deployment, and oversight of AI fosters transparency, reduces the risk of harm, and builds public confidence.

The UTS Human Technology Institute states that participatory governance not only improves accountability but also strengthens the social licence to operate, particularly in high-impact contexts such as health, justice, and employment [45].

Internationally, both the OECD AI Principles [5] and UNESCO's Recommendation on the Ethics of Artificial Intelligence [34] advocate for inclusive and deliberative processes in AI policymaking and system development, recognising that community co-design is a cornerstone of ethical and sustainable AI governance.

Recommendation: Establish advisory boards, ethics committees, and customer councils to incorporate stakeholder input into design and oversight of AI systems. Follow the participatory model of "consult, involve, collaborate, empower".

I. Monitor, Audit, and Continuously Improve

AI performance must be monitored beyond deployment. Organizations should adopt live monitoring, incident reporting, internal audits, and independent reviews.

An example was where KPMG's KymChat was assessed using Microsoft's Responsible AI template, evaluating transparency, reliability, privacy, and inclusiveness [36].

Recommendation: Create audit trails for AI decision-making, define KPIs for ethical use, and report outcomes to boards and regulators.

J. Prepare for Mandatory Regulation

Proactively preparing for forthcoming AI regulation is critical to mitigating legal exposure, avoiding costly system overhauls, and preserving organizational reputation. The Australian Government's interim response to AI regulation explicitly recognizes significant gaps in the existing legal framework and foreshadows the introduction of mandatory safeguards for high-risk and "frontier" AI systems [46]. To remain compliant and competitive, organizations must begin aligning their AI governance structures with emerging regulatory expectations.

Internationally, the EU Artificial Intelligence Act offers a robust comparative benchmark, classifying AI systems by risk tier and imposing mandatory conformity assessments for high-risk applications [47]. Complementing this, the NIST AI Risk Management Framework (USA) provides a flexible, voluntary tool for identifying, assessing, and managing AI risks throughout the system lifecycle [50].

Recommendation: Organizations should conduct strategic gap analyses comparing their current AI practices to international standards such as the EU AI Act, NIST AI RMF, and ISO/IEC 42001 [43][44][47][48]. Participation in regulatory sandboxes can further facilitate safe and compliant innovation by allowing companies to test AI systems under supervised conditions [49]. Engaging in scenario planning and aligning development protocols with these evolving standards will position organizations to navigate Australia's impending AI regulatory landscape with agility and confidence [50].

VI. CONCLUSIONS

As Artificial Intelligence continues to reshape the Australian corporate landscape, it presents both transformative opportunities and significant legal challenges. This paper has examined the multifaceted legal risks associated with AI adoption, including issues of data privacy, algorithmic discrimination, workplace surveillance, employment law, consumer protection, cybersecurity vulnerabilities, and regulatory uncertainty. These risks are not merely peripheral, they strike at the core of corporate accountability, requiring leaders to go beyond traditional compliance models and adopt a proactive, integrated governance approach.

To mitigate AI-related risks, organizations must integrate legal compliance, ethical foresight, and operational oversight into every stage of the AI lifecycle, from design and deployment to monitoring and decommissioning. Legal compliance alone is insufficient; instead, corporations must develop comprehensive AI governance structures that anticipate legislative developments, respond to community expectations, and foster public trust. This involves forming cross-functional governance teams that bring together legal, technical, and ethical expertise, institutionalizing regular risk assessments and audits, and fostering a culture of human-centered innovation grounded in fairness, transparency, and explainability. Corporate leaders must build organizational capacity for AI literacy across all levels of leadership, ensuring informed and ethically responsible decision-making. Active engagement with evolving domestic and international regulatory frameworks, such as the proposed Australian AI regulations and the EU AI Act, is essential. Rather than waiting for binding legislation, forward-thinking organizations should adopt best practices from international standards, such as ISO/IEC 42001 and the NIST AI Risk Management Framework, and participate in regulatory sandboxes to pilot high-risk AI innovations safely.

AI governance must also address environmental responsibilities. As AI becomes embedded in systems that impact environmental outcomes, such as smart grids, logistics, or industrial automation, corporate leaders must ensure that AI strategies align with sustainability goals, emissions reduction targets, and environmental reporting obligations. Integrating ESG principles into AI governance to ensure that legal compliance also supports Australia's broader environmental stewardship efforts [51].

Transparency and accountability should be operationalized through clear reporting mechanisms that disclose AI system performance, limitations, and ethical safeguards to regulators and stakeholders. By doing so, organizations not only mitigate legal exposure but also establish themselves as responsible innovators, setting benchmarks for the ethical use of AI in the corporate sector. Ultimately, the responsible deployment of AI in Australia will depend on leadership's ability to integrate legal risk management with a visionary commitment to ethical and inclusive digital transformation.

REFERENCES

[1] L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, V. Dignum, C. Luetge, ... and E. Vayena, "AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations," Minds and Machines, vol. 28, no. 4, pp. 689–707, 2018.

[2] A. Daly, "AI and the law in Australia: A critical review," UTS Law Review, vol. 44, pp. 25–49, 2022.

[3] E. Glikson and A. Woolley, "Human trust in artificial intelligence: Review of empirical research," Academy of Management Annals, vol. 14, no. 2, pp. 627–660, 2020.

[4] T. Birkstedt, R. Gustafsson, R. Hekkala, and K. Smolander, "AI governance: Themes, knowledge gaps and future agendas," Internet Research, vol. 33, no. 7, pp. 133–156, 2023.

[5] Organisation for Economic Co-operation and Development (OECD), Recommendation of the Council on Artificial Intelligence, Paris: OECD, 2019.

[6] R. (on the application of the Open Rights Group) v The Secretary of State for the Home Department [2021] EWHC 2094 (Admin), High Court of Justice, UK, 2021.

[7] R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058, Court of Appeal, UK, 2020.

[8] European Union, General Data Protection Regulation (GDPR), Brussels: European Union, 2016.

[9] UK Government, Human Rights Act 1998, London: The Stationery Office, 1998.
[10] Information Commissioner's Office. (2020). Explaining decisions made with AI.
[11] Aaronson, S. A. (2023). Building trust in AI: A landscape analysis of government AI programs (CIGI Paper No. 272). Centre for International Governance Innovation.
[12] E. Callaway, "DeepMind's AI predicts structures for a vast trove of proteins," Nature, vol. 595, pp. 635–636, Jul. 2021.
[13] Australian Government, Privacy Act 1988 (Cth), Canberra: Office of the Parliamentary Counsel, 1988.
[14] Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines (Privacy Act 1988), Sydney: OAIC, 2021.
[15] Office of the Australian Information Commissioner, Guide to Data Analytics and the Privacy Act, Sydney: OAIC, 2021.
[16] IW v City of Perth (1997) 191 CLR 1, High Court of Australia, 1997.
[17] Australian Government, Sex Discrimination Act 1984 (Cth), Canberra: Office of the Parliamentary Counsel, 1984.
[18] Australian Government, Racial Discrimination Act 1975 (Cth), Canberra: Office of the Parliamentary Counsel, 1975.
[19] Victorian Government, Equal Opportunity Act 2010 (Vic), Melbourne: Victorian Legislation, 2010.
[20] NSW Government, Anti-Discrimination Act 1977 (NSW), Sydney: NSW Legislation, 1977.
[21] Lopez Ribalda and Others v Spain, App. Nos. 1874/13 & 8567/13, European Court of Human Rights, 17 Oct. 2019.
[22] Australian Government, Fair Work Act 2009 (Cth), Canberra: Office of the Parliamentary Counsel, 2009.
[23] NSW Government, Surveillance Devices Act 2007 (NSW), Sydney: NSW Legislation, 2007.
[24] Australian Consumer Law (Competition and Consumer Act 2010 (Cth), Schedule 2), Canberra: Office of the Parliamentary Counsel, 2010.
[25] ACCC v Trivago N.V. [2020] FCA 16, Federal Court of Australia, 2020.
[26] UK Government, Misrepresentation Act 1967 (UK), s 2(1), London: The Stationery Office, 1967.
[27] Australian Government, Security of Critical Infrastructure Act 2018 (Cth), Canberra: Office of the Parliamentary Counsel, 2018.
[28] Office of the Australian Information Commissioner, Australian Privacy Principles (APPs) Guidelines, Sydney: OAIC, 2021.
[29] Australian Government Department of Industry, Science, Energy and Resources, AI Ethics Framework, Canberra: DISER, 2019.
[30] Office of the Australian Information Commissioner, Guide to Data Analytics and the Privacy Act, Sydney: OAIC, 2021.
[31] Australian Securities and Investments Commission. (2023, May 10). ASIC Report 763: ASIC's recent greenwashing interventions.
[32] McMillan, J.A., 2023. Report of the statutory review of the Modern Slavery Act 2018 (Cth): The first three years. Australian Government.
[33] Human Technology Institute, AI Governance Snapshot #1: Essential Components of AI Governance, Sydney: University of Technology Sydney, 2024.
[34] UNESCO, Recommendation on the Ethics of Artificial Intelligence, Paris: United Nations Educational, Scientific and Cultural Organization, 2021.
[35] Telstra Corporation Ltd., Risk Council of AI & Data (RCAID): Governance Framework Overview, Sydney: Telstra, 2024.
[36] Microsoft, Responsible AI Impact Assessment Template, Microsoft, 2022.
[37] International Organization for Standardization, ISO/IEC 42005:2023 – Artificial Intelligence — Risk Management Framework, ISO, 2023.
[38] Office of the Australian Information Commissioner, Guide to Undertaking Privacy Impact Assessments, Sydney: OAIC, 2021.
[39] United Nations Office of the High Commissioner for Human Rights, Human Rights Impact Assessments: A Toolkit for Business, Geneva: UN, 2022.
[40] Office of the Australian Information Commissioner, Algorithmic Transparency and Accountability: A Guide for AI Systems, Sydney: OAIC, 2021.
[41] Office of the Australian Information Commissioner, Guide to Undertaking Privacy Impact Assessments, Sydney: OAIC, 2021.
[42] Australian Government, Age Discrimination Act 2004 (Cth), Canberra: Office of the Parliamentary Counsel, 2004.
[43] International Organization for Standardization, ISO/IEC 27001:2022 – Information Security Management, ISO, 2022.
[44] International Organization for Standardization, ISO/IEC 42001:2023 – Artificial Intelligence Risk Management, ISO, 2023.
[45] Human Technology Institute, AI Governance Snapshot #2: Putting People at the Centre of AI, Sydney: University of Technology Sydney, 2024.
[46] Australian Government Department of Industry, Science, and Resources, Safe and Responsible AI in Australia – Interim Response, Canberra: DISR, 2024.
[47] European Union, EU Artificial Intelligence Act, Brussels: European Union, 2023.
[48] National Institute of Standards and Technology, AI Risk Management Framework (AI RMF) Version 1.0, Gaithersburg, MD: NIST, 2023.
[49] OECD, Regulatory Sandboxes in Artificial Intelligence, Paris: Organisation for Economic Co-operation and Development, 2023.
[50] OECD, Strategic Foresight and Scenario Planning for Artificial Intelligence Governance, OECD Working Paper DSTI/DPC/AIGO(2024)10/FINAL, 2024.
[51] Task Force on Climate-related Financial Disclosures. (2017). Recommendations of the Task Force on Climate-related Financial Disclosures.