**From Soft Law to Hard Law: A Comparative Analysis of AI Regulation in the European Union and Canada**

**Introduction**

Artificial intelligence (AI) tools, once a product of science fiction, are now used widely in the public domain. Recent advancements in technology have allowed AI and other autonomous systems to become readily accessible to end-users across the sectors of education, healthcare, transportation, and more (Ulnicane, 2022, p.254)[[1]](#footnote-2). According to the OECD [what’s the OECD], an AI system is[[2]](#footnote-3). While there has been greater uptake of AI and big data due to the potential for social and economic benefits, concerns regarding an adverse impact on society persist (Ulnicane, 2022, p.254)[[3]](#footnote-4). For instance, machine learning algorithms are capable of discriminating based on race and gender (Buolamwini & Gebru, 2018, p.1)[[4]](#footnote-5) and AI technology can alter images, audio, and videos in highly realistic ways to present fake information online (Chesney & Citron, 2018, p.1757)[[5]](#footnote-6).

The regulation of AI technology presents a significant challenge because the industry is developing more rapidly than law-making can keep pace with. For instance, the proposed Artificial Intelligence and Data Act (AIDA) in Canada can come into effect no sooner than 2025 (Government of Canada, 2023a)[[6]](#footnote-7), leaving a regulatory gap in oversight in the interim. Given this complex regulatory landscape, how can AI technologies be employed in a manner that does not cause societal harm? What forms of oversight are in place to ensure its ethical use in the public and private sectors? Many countries have pledged to become global standards for the regulation of AI in this regard, but few have taken the lead.

This paper seeks to compare the regulatory framework on AI in the European Union (EU) and Canada, given that both jurisdictions have made attempts to become global leaders in the AI industry. While the EU has recently passed the Artificial Intelligence Act (AIA), Canada continues to debate the framework proposed within the AIDA. These frameworks have been under development for years and progress has been slow, especially compared to the pace and scope of AI advancement. It is thus crucial to understand the state of AI regulation in both jurisdictions, identify gaps, and propose recommendations for effective governance. The legal domain also has characteristics that make it particularly interesting and challenging for AI (Rissland et al., 2003, p.2)[[7]](#footnote-8). To list a handful, the legal system is hierarchical due to varying degrees of authority (such as courts at the trial and appellate level), laws can exist at both the level of individual nations and the level of supranational bodies like the EU, and legal rules and statutory interpretation differ according to the civil or common law makeup of the country (Rissland et al., 2003, p.3)[[8]](#footnote-9). These characteristics suggest complexity, but also synergy between the law and AI, given that the legal domain can act as an intermediary between the technical environment in which AI is developed and the everyday experience of consumers (Rissland et al., 2003, p.5)[[9]](#footnote-10).

Originating in the field of international law, the term “soft law” denotes agreements, principles, and instruments that are not legally binding (ECCHR, n.d.)[[10]](#footnote-11), such as guidelines, codes of conduct, and non-binding standards (Bosi, 2021)[[11]](#footnote-12). Conversely, “hard law” refers to binding obligations that can be legally enforced in court (ECCHR, n.d.), such as international treaties and domestic legislation (Bosi, 2021). This paper argues that the EU has adopted a hard law approach in its regulation of AI, embedded in the key principles of the precautionary principle, a risk-based approach, and a human-centric approach. It further argues that Canada demonstrates a soft law framework, despite the entrenchment of privacy as a human right due to the relatively ill-defined “high-impact” systems in the AIDA and a reliance on non-binding tools such as the AIDA Companion Document, Voluntary Codes of Conduct, and other Directives. It will be beneficial for Canada to implement a hard law approach similar to the EU given the potential for stronger powers of enforceability to ensure the principles of trust, accountability, and non-discrimination that both the AIA and the AIDA boast.

* Revised Thesis: The paper argues that the European Union's adoption of a hard law approach to AI regulation—grounded in the precautionary principle, a risk-based framework, and a human-centric focus—is more effective in ensuring ethical and accountable AI development. In contrast, Canada's reliance on soft law mechanisms and ill-defined regulations in the AIDA undermines enforceability and fails to adequately protect society from potential AI harms. Therefore, Canada should adopt a hard law approach similar to the EU to enhance its AI governance and safeguard public interests.

The paper is divided into two main sections. First, we examine policy development on AI in the EU and Canada through a review of key principles and compare the two jurisdictions. In the second section, we discuss the key challenges and opportunities that the EU and Canada are faced with in the field of AI technology, with potential learnings for Canada given the relative infancy of the AIDA as compared to the EU’s AIA.

*Policy development in the EU is grounded in hard law and key principles: The precautionary principle, a risk-based approach, and a human-centric approach*

While it is true that proposed legal frameworks such as the AIA in the EU and the AIDA in Canada remain under development and have yet to be formally implemented, the perception that AI regulation is still in its infancy with few clear rules, statutes, or standards available to guide developers and users – coined the “infancy thesis” – is simply untrue (Viljanen & Parviainen, 2022, p.1)[[12]](#footnote-13). Legal instruments such as the precautionary principle, the EU Fundamental Rights Charter, the General Data Protection Regulation (GDPR), and EU Member State constitutions already constrain AI development and use (Viljanen & Parviainen, 2022, p.5)[[13]](#footnote-14). The issue is that while regulation may be dense regarding a specific use for AI, with hard law obligations backed by credible sanctions, regulation is non-existent for other uses. For instance, personal data is subject to stringent regulation under the GDPR, but data use in industrial AI applications with no implications for personal data is only governed by database rights, trade secrecy rules, and competition law norms (Viljanen & Parviainen, 2022, p.6)[[14]](#footnote-15). Since the regulatory intensity over AI regulation varies across applications, such as the difference in intensity for data regulation between health care applications and industrial applications, and there exists a difference in scope such as the wide applicability of the GDPR as compared to data rules affecting only specific sectors, AI law remains emergent with many details unclear (Viljanen & Parviainen, 2022, p.9)[[15]](#footnote-16).

The precautionary principle speaks to such lack of clarity. Originating in environmental law for protection against the unpredictable consequences of climate change, the precautionary principleestablished by the EU seeks to avoid potential harms before they occur (European Union, 2016)[[16]](#footnote-17). The principle can be invoked when a phenomenon, product, or process has a dangerous effect, but its risk cannot be determined with sufficient certainty. Depending on the level of risk, authorities may decide to put in place measures such as legal action, financing research programmes, and public information campaigns (European Union, 2016)[[17]](#footnote-18). Given the risks and uncertainties presented by AI systems, the sector arguably meets the threshold for the use of the precautionary principle in the digital environment. In the context of AI, governments that are in line with the precautionary principle put requirements or guidelines in place before the deployment of a system – like the EU has done with the AIA (Neschke et al., 2022, p.11)[[18]](#footnote-19).

The precautionary principle is also intrinsically linked to risk analysis and management, given that it is triggered following an evaluation of risk and the potential consequences of inaction (European Union, 2016)[[19]](#footnote-20). As such, the framing of the AIA within a “risk-based” approach signals the co-optation of the precautionary principle in the current regulatory framework.

A risk-based approach is important for ensuring that regulatory intervention is appropriate and does not deter innovation. However, this requires clear criteria to differentiate AI applications from low and high risk (European Commission, 2020, p.3)[[20]](#footnote-21). High risk AI applications would be subject to prior conformity assessment such as testing, inspection, and certification. A risk-based AI regulation would also have consideration for mandatory legal requirements such as data and record keeping, robustness and accuracy, and human oversight (European Commission, 2020, p.23)[[21]](#footnote-22).The draft AIA introduced three risk-based categories that outline varying obligations for AI system providers: unacceptable risks, high risks, and low or minimal risks (Veale & Borgesius, 2021, p.98)[[22]](#footnote-23).

**Unacceptable Risk**

The top of the risk pyramid contains prohibited practices which create unacceptable risks that go against EU values or fundamental rights. For instance, AI applications with the potential to manipulate persons and exploit vulnerable groups in a manner that causes physical or psychological harm are considered unacceptable. “Social scoring” by public authorities to measure the trustworthiness of people based on their social behaviour in an unrelated context from the input data is one such banned purpose (Lilkov, 2021, p.168)[[23]](#footnote-24). This is in direct contrast to other global actors such as China who enact a “social credit system”. The EU is thus signaling its human-centered approach, and that such a system poses an unacceptable risk for European citizens (Lilkov, 2021, p.168)[[24]](#footnote-25). However, social scoring is undertaken by the public sector (eg. law enforcement, welfare support) as well as private companies (eg. line of credit assessments, employment background checks). By this logic, it does not make sense to restrict the social scoring prohibition to the public sector. In this case, the European Artificial Intelligence Board proposed within the AIA would be responsible for clarifying whether an assessment is within context, but its guidance would be solely advisory (Veale & Borgesius, 2021, p.100)[[25]](#footnote-26). Biometric identification systems such as facial ID in public spaces for law enforcement purposes are also banned under unacceptable risk, with exceptions to search for victims of crime, identify criminal perpetrators, and prevent an imminent threat to life or safety of persons. This is a contentious issue for civil society groups who advocate for a more stringent ban on facial recognition in public as it has the potential to discriminate against certain vulnerable groups (Lilkov, 2021, p.168)[[26]](#footnote-27). Only real-time systems are captured in the prohibition, implying that systems could be used in retrospect to analyze footage and identify individuals (Veale & Borgesius, 2021, p.101)[[27]](#footnote-28).

**High Risk**

The next category in the risk pyramid is high-risk AI systems. The European Commission argues that an AI application should be considered high risk based on whether the sector and the intended use involves significant risks from the perspective of safety, consumer rights, and fundamental rights (European Commission, 2020, p.17)[[28]](#footnote-29). Within a risk-based framework, AI applications would be considered high risk if they meet two criteria. First, the AI application is employed in a sector where activities undertaken are expected to have significant risks occur – for instance, healthcare, transportation, and energy. Second, the AI application is used in such a manner that significant risks are likely to arise. An example to measure the threshold of significant risk is that while healthcare is generally a high-risk sector, an error in the appointment scheduling system does not pose significant harm. Rather, if the application is used in a manner where the risk of injury, death, or significant material damage is likely to occur, the application can be deemed high risk (European Commission, 2020, p.17)[[29]](#footnote-30). It is also stipulated that there may be exceptional circumstances where the use of an AI application is deemed high risk even if the sector in which it is employed is not of concern. For instance, recruitment processes impacting workers’ rights, remote biometric identification, and intrusive surveillance technologies should always be considered high-risk (European Commission, 2020, p.18)[[30]](#footnote-31).

The draft AIA also contains an extensive list pertaining to the accuracy, robustness, and cybersecurity of high-risk systems with special attention to the potential for discrimination based on machine learning applications that build on data they are inputted. Providers are responsible for producing technical documentation with information for user transparency, facilitating logging to allow tracing of a system’s risks (eg. biometric systems require logged information on the period of use), and building for human oversight where two “natural” persons sign off on actions to minimize risks to health, safety, and fundamental rights (Veale & Borgesius, 2021, p.103)[[31]](#footnote-32).

**Minimal Risk**

Lastly, the bottom of the risk pyramid contains AI systems that pose limited risks such as chatbots, but users should be made fully aware that they are interacting with a machine (Lilkov, 2021, p.169)[[32]](#footnote-33). For minimal risk systems, member states are encouraged to adopt voluntary codes of conduct facilitated by the Commission but are not beholden to mandatory requirements like high-risk systems are (Veale & Borgesius, 2021, p.98)[[33]](#footnote-34).

Most respondents in stakeholder consultations favoured a risk-based approach in the EU, preferring it over a blanket regulation for all AI systems regardless of technical capacity (Justo-Hanani, 2022, p.149)[[34]](#footnote-35). The European industry lobby was particularly active in the policymaking process. Interest groups such as Digitising European Industry (DEI) (represents the digital technology industry in Europe through national hubs), the European Round Table of Industrialists (ERT), BUSINESSEUROPE (represents enterprises of various size in Europe), the Paris Artificial Intelligence Research Institute (PRAIRIE), and the AI4EU (private sector and academic institutions from EU member states) participated as key players in meetings called for by the President of the European Commission on the regulatory approach to AI (Justo-Hanani, 2022, p.149)[[35]](#footnote-36).

In line with industry preferences, the EU acknowledges that different systems pose varying levels of risk, and demands a proportionate response for the severity of the impact. A concrete risk methodology for high-risk AI systems in particular will help deter significant risks to the health, safety, and fundamental rights of persons, ensuring a “human-centric” approach that fosters trust in AI technology (European Commission, 2021, p.3)[[36]](#footnote-37).

Following the precautionary principle and risk-based framework, the third approach used by the EU in the deployment of AI systems is the human-centric approach. The language around a human-centric approach has been circulated since the early stages of policy development on AI in the EU. For instance, the Ethics Guidelines for Trustworthy AI were published in April of 2019, following consultation with the High-Level Expert Group (HLEG) on AI (European Commission, 2024)[[37]](#footnote-38). The HLEG asserts that an ethical AI regime is based on the fundamental rights enshrined in the EU treaties, the EU Charter, and international human rights laws. As such, respect for human dignity, individual freedoms, democracy and rule of law, justice, non-discrimination, and citizens’ rights should inform a human-centric approach to AI. Society will only be able to fully reap the benefits of such technology when it is confident in its trustworthiness. Consistency with fundamental rights should thus be a foundational ambition to regulating AI (European Commission, 2019, p.2)[[38]](#footnote-39).

In December 2023, the European Parliament reached an agreement with the Council on the draft AIA. The Act was formally adopted by the Parliament in March 2024[[39]](#footnote-40) and it is considered to be the world’s first comprehensive AI law. Both the Parliament’s Internal Market and Civil Liberties committees voted on the agreement (European Parliament, 2023)[[40]](#footnote-41). During the plenary debate of the Law, the Internal Market Committee co-rapporteur [Brando Benifei (S&D, Italy)](https://www.europarl.europa.eu/meps/en/124867/BRANDO_BENIFEI/home) said: “We finally have the world’s first binding law on artificial intelligence, to reduce risks, create opportunities, combat discrimination, and bring transparency. Thanks to Parliament, unacceptable AI practices will be banned in Europe and the rights of workers and citizens will be protected. The AI Office will now be set up to support companies to start complying with the rules before they enter into force. We ensured that human beings and European values are at the very centre of AI’s development”. Civil Liberties Committee co-rapporteur [Dragos Tudorache (Renew, Romania)](https://www.europarl.europa.eu/meps/en/197665/DRAGOS_TUDORACHE/home) said: “The EU has delivered. We have linked the concept of artificial intelligence to the fundamental values that form the basis of our societies. However, much work lies ahead that goes beyond the AI Act itself. AI will push us to rethink the social contract at the heart of our democracies, our education models, labour markets, and the way we conduct warfare. The AI Act is a starting point for a new model of governance built around technology. We must now focus on putting this law into practice”.[[41]](#footnote-42)

Overall, the EU has adopted a hard law approach that is grounded in the AIA legislation with the embedded key principles of the precautionary principle, a risk-based approach, and a human-centric approach. The precautionary principle is a recognized legal principle in the EU, and the risk-based and human-centric approaches are enshrined within the formal and binding text of the proposed AIA.

*Soft law mechanisms on AI in Canada*

While the EU has made significant progress in introducing an AI legislation, there has been greater hesitancy in Canada, despite Canada being the first country to create a national strategy for AI in 2017 (Government of Canada, 2023a)[[42]](#footnote-43). Instead of embracing a hard-law approach, Canada has chosen to regulate AI technology through means of soft-law tools. Soft laws refer to policies such as standards, best practices, and guidelines which are less enforceable by the government yet flexible, while hard laws are government-enforced mechanisms such as legislation which may impose higher compliance burden with slower adoption (Neschke et al., 2022, p.10)[[43]](#footnote-44). “Soft” tools aim to define the boundaries of ethical AI innovation while avoiding less flexible legislation (Martin-Bariteau & Scassa, 2021, p.6)[[44]](#footnote-45).

In conjunction with soft tools, the Canadian AI regulatory framework implements a harm-based approach in contrast to the risk-based approach in the EU, while a human-centric approach is prevalent in both jurisdictions. To start with, the *harm-based approach* in the AIDA adopts a single tier of “high-impact” AI systems requiring legal oversight. However, the criteria for high-impact systems in the AIDA with the potential of posing serious harm still needs to be defined in regulation. Canada’s AIDA is thus scarce on many key details, posing a problem for developers and distributors with AI products in the making (Beardwood, 2023, p.65)[[45]](#footnote-46). The AIDA is described as “agile”, alluding to the ability to rapidly respond to changes in the business and technical sectors. The Canadian government interprets this as the ability to draft laws that can be easily changed through regulations (over statutory provisions), made evident in the fact that the core terms and obligations of AIDA are yet to be determined, and oversight remains within the Minister’s office rather than an independent regulatory body (Scassa, 2023a, p.7)[[46]](#footnote-47). However, leaving the finer details such as the definition of high-impact systems to future regulation is not agile, given that regulations can take longer than anticipated to develop, or fail to materialize at all. Agile regulations should also be iterative and data-driven, with the ability to measure impact – it is unclear whether the AIDA will include such terms (Scassa, 2023b)[[47]](#footnote-48).

Clarity on the definition of a high-impact system is particularly important because the AIDA has adopted a single-tier of high-impact as compared to the EU’s AIA with three levels of risk including unacceptable risk, high-risk, and low or minimal risk (Beardwood, 2023, p.67)[[48]](#footnote-49). The AIA is specific regarding examples of each risk-based activity as well. For instance, certain biometric identification systems pose an unacceptable risk; activities related to employment, vocational training, and others pose a high-risk, and chatbots pose a minimal risk. Each risk-level has proportionate interventions (Veale & Borgesius, 2021, p.98)[[49]](#footnote-50).

A key contribution of the AIDA Companion Document, which is a plain language resource from Innovation, Science, and Economic Development Canada providing additional details missing within the in-text proposal of the AIDA, is a list of characteristics that would be examined when determining which AI systems are considered high-impact (Beardwood, 2023, p.67)[[50]](#footnote-51). Since the document is not a part of an official regulation defining high-impact systems, it is effectively a soft tool being used to signal future direction without the government taking a legal (binding) stance on the matter. Characteristics to be considered for classifying high-impact systems include evidence of risks of harm to health and safety or a risk of adverse impact on human rights, the severity of potential harms, the scale of use, the nature of harms or adverse impacts that have already taken place, the extent to which for practical or legal reasons it is not possible to opt-out from that system, imbalances of economic or social circumstances, and the degree to which the risks are adequately regulated by another law (Government of Canada, 2023a)[[51]](#footnote-52). The Canadian government justifies its choice to define the criteria for high-impact systems in later regulation by stating that it allows for “interoperability with international frameworks such as the EU AIA, and for updates to occur as the technology advances” (Government of Canada, 2023a)[[52]](#footnote-53). In other words, the Canadian government is taking a “wait and see” approach to give itself the flexibility to align with the EU’s approach once it is finalized.

To illustrate another soft tool, the Treasury Board of Canada Secretariat published a Directive on Automated Decision-Making in April 2019 (Government of Canada, 2023b)[[53]](#footnote-54). The directive states that the Government of Canada is anticipating greater co-optation of AI to improve the delivery of services, and claims that the government is committed to ensuring that the use of AI complies with principles of administrative law including transparency, accountability, and procedural fairness. The directive applies to any system, tool, or statistical model used to make an administrative decision or a related assessment about a client, but it is not legally binding (Government of Canada, 2023b)[[54]](#footnote-55). Another associated soft tool, the Algorithmic Impact Assessment (AIA), is a mandatory questionnaire used to determine the level of impact of an automated decision system (Government of Canada, 2023c)[[55]](#footnote-56).

The prevalence of soft laws has created a vacuum in existing legislation to address concerns with AI systems. This gap has been attempted to be filled through court challenges, where individuals have challenged the discriminatory outcome of AI systems. *Ewert v Canada* (2018) demonstrates how an algorithmic assessment tool may infringe on a racialized individual’s freedom through biased output. The appellant challenged the use of psychological and actuarial risk assessment tools used by Correctional Services Canada (CSC) on the basis that the tools were developed and tested on predominantly non-Indigenous populations, barring the tool from holding validity when applied to Indigenous persons (Thind, 2023, p.21)[[56]](#footnote-57). Additionally, in *Barre v Canada* *(Citizenship and Immigration)* (2022), the Minister of Citizenship and Immigration submitted photo evidence to assert that two refugee claimants were Kenyan and not Somali citizens who arrived in Canada on study permits before their refugee claim was made. The applicants objected to the photos, claiming that a questionable facial recognition software “Clearview AI” had been used by the Canadian Border Services Agency (CBSA) to generate a photo comparison (Thind, 2023, p.19)[[57]](#footnote-58). As these court cases demonstrate, the use of AI software can be used against vulnerable groups such as refugees, the output of which is often based off a limited data set.

Furthermore, recommendations to embed privacy and data protection laws within the AI regulatory framework represent a *human-centric approach* in Canada. As an important institutional actor that has been heavily involved in recognizing the need for clear legal principles in the field of AI, the Office of the Privacy Commissioner of Canada (OPC) published recommendations to reform the Personal Information Protection and Electronic Documents Act (PIPEDA) in November of 2020 (OPC, 2020a)[[58]](#footnote-59).

The OPC recognizes that consent forms the basis of data protection laws including PIPEDA. AI challenges the consent principle since it is capable of making inferences based on personal information, and data that is gathered may be used for purposes different than intended at the time of collection (OPC, 2020a). The OPC thus recommended changes to the PIPEDA such as a privacy impact assessment, a balancing test similar to the GDPR in the EU for legitimate interests in the use of AI, and de-identification when using information without consent for research purposes (OPC, 2020a). In terms of recognizing privacy as a human right, the PIPEDA should be amended to clarify that it encompasses inferences drawn about an individual, given that AI can collect personal information to make predictions about their behaviour. Such systems, as a result of machine learning, can produce discriminatory outcomes. Specific provisions to mitigate discriminatory results by algorithms include the right to meaningful explanation and the right to contest automated decisions. Lastly, the PIPEDA should include a right to demonstrable accountability for individuals for all processing of personal information, supported by a record keeping requirement similar to the GDPR (OPC, 2020a).

These recommendations are based on consultation with stakeholders and experts on how to benefit from the use of AI while protecting the fundamental right to privacy (OPC, 2020a). Interested stakeholders were asked to consider ten proposals regarding a rights-based approach, privacy as a fundamental human right, and meaningful consent (OPC, 2020c)[[59]](#footnote-60). The OPC does not identify who they consulted with specifically, but cite feedback from industry, academia, civil society, and the legal community, among others (OPC, 2020b)[[60]](#footnote-61). The Ontario Society of Professional Engineers (OSPE) is one such interest group who submitted a proposal for consideration following the call for public consultation (OSPE, n.d.)[[61]](#footnote-62).

It is important to note that the OPC is a non-partisan body that conducted consultations to offer independent recommendations to reform the PIEPEDA to Parliament. In contrast, there are criticisms around the public consultation process for the AIDA. In a report submitted to the House of Commons’ Standing Committee on Industry and Technology, the Canadian Labour Congress (CLC) asserted that the AIDA was introduced without public consultation with unions and civil society organizations, leaving glaring problems with the proposal (CLC, 2023, p.2)[[62]](#footnote-63). Concerns with discrimination, the potential infringement of privacy and civil liberties, deepened inequities for vulnerable groups, and the lack of human rights or privacy impact assessment in the development of AI systems are raised in the report (CLC, 2023, p.2)[[63]](#footnote-64). Additionally, the Canadian government has exempted itself from the AIDA, given that the legislation does not apply to a product, service, or activity under the purview of certain federal and provincial departments prescribed in regulation such as the Department of National Defence. The irony is that a number of these exempted institutions administer “high-impact” AI systems such as decision-making regarding immigration (CLC, 2023, p.3)[[64]](#footnote-65). It is argued that the government has prioritized the commercial development and competitiveness of the AI industry, thus opting for a light-touch to regulation – or soft laws – such as voluntary codes of conduct over binding regulations (CLC, 2023, p.5)[[65]](#footnote-66). In the future, it is crucial that the Government of Canada connect with a range of interest groups to conduct informed consultation on AI.

Furthermore, the Digital Charter is another soft tool that forms the basis of the proposed draft Bill C-27: Digital Charter Implementation Act (2022), which contains AIDA, currently undergoing its second reading in the House (Parliament of Canada, n.d.)[[66]](#footnote-67). Canada’s Digital Charter lays out principles to ensure that privacy is protected, innovation is human-centred, and Canadian organizations can lead global innovation (Government of Canada, 2023d)[[67]](#footnote-68). It contains ten principles, with principles 3) control and consent over personal data being used and shared, 4) transparency with clear access to data and the ability to share it without undue burden, 7) data and digital for good through the ethical use of data, and 10) strong enforcement and accountability through clear and meaningful penalties for violations of the law (Government of Canada, 2023d)[[68]](#footnote-69) directly relating to a human-centric approach.

Both of the AIA and AIDA frameworks claim to advance a human-centric approach to AI regulation, with particular attention to privacy as a fundamental human right. Within the stated objectives of the EU AIA, it is argued that AI should be a force for good in society with the ultimate goal of increasing human well-being. As such, rules for developing AI should be human-centric to foster trust in the safe use of the technology and establish respect for fundamental rights (European Commission, 2021, p.1)[[69]](#footnote-70). As for Canada, the Digital Charter claims to set out principles to ensure privacy protection and human-centred innovation (Government of Canada, 2023d)[[70]](#footnote-71).

Given current projections on consultation and development of draft regulations needed before Royal Assent can be received, the AIDA provisions would come into force no sooner than 2025 (Government of Canada, 2023a)[[71]](#footnote-72) – slow paced as compared to the EU hurtling towards formal adoption of the AIA this year. Overall, Canada adopts a soft law approach to AI regulation, as demonstrated by tools such as the AIDA Companion Document, the Directive on Automated Decision Making and the Algorithmic Impact Assessment, and the Digital Charter. Canada employs a harm-based approach while the EU employs a risk-based approach within their respective high-impact and multi-tiered risk frameworks, with Canada proposing a less robust framework due to the lack of a clear definition for “high-impact” systems within the AIDA.

**Comparing the AI Regulatory Frameworks in the EU and Canada**

As a starting point in comparing the two jurisdictions we will look at the approaches that they have adopted in developing AI policies, namely the EU’s risk-based approach vs Canada’s harm-based approach. Key elements of comparison include regulations or laws (such as those related to privacy and data protection) and the availability of voluntary codes of conduct for lower-risk systems. We notice the preference for soft laws in Canada as opposed to hard laws in the EU.

*Risks, harm, and the protection of privacy*

As mentioned above, the EU uses a risk-based approach in the AIA, while Canada uses a harm-based approach to classify systems in the AIDA (Baldridge et al., 2024)[[72]](#footnote-73). Both terms are multi-faceted, as “risk” alludes to unintended social consequences such as biased algorithms or the erosion of privacy, and “harm” transcends physical damage to include psychological, ethical, and socio-political dimensions (Baldridge et al., 2024)[[73]](#footnote-74).

The AIDA prioritizes a harm-based approach by referencing two main forms of harm:

(a) “‘harm’ means (i) physical or psychological harm to an individual; (ii) damage to an individual’s property; or (iii) economic loss to an individual”(Beardwood, 2023, p.66)[[74]](#footnote-75); and

(b) “‘biased output’ means content that is generated, or a decision, recommendation or prediction that is made, by an artificial intelligence system and that adversely differentiates, directly or indirectly and without justification, in relation to an individual on one or more of the prohibited grounds of discrimination set out in section 3 of the Canadian Human Rights Act, or on a combination of such prohibited grounds” (Beardwood, 2023, p.66)[[75]](#footnote-76).

Both types of harm are referenced inconsistently across the AIDA and the AIDA Companion Document (Beardwood, 2023, p.66)[[76]](#footnote-77). Additionally, “harm” is defined in AIDA as affecting an individual, but the AIDA Companion Document references the concept of collective harm which can be experienced broadly by a protected class such as gender or race (Beardwood, 2023, p.66)[[77]](#footnote-78). Harm suffered by individuals is too narrow as a definition, given that AI can have broader impacts beyond the individual such as environmental harms and systemic discrimination (Scassa, 2023b)[[78]](#footnote-79).

While it is important to address both risks and harms, risk should take precedence given the unpredictable nature of AI and the unintended consequences its use could present in the future. Prioritizing risk within an AI regulatory framework also aligns with the precautionary principle by preventing serious harm from materializing to begin with (Baldridge et al., 2024)[[79]](#footnote-80). This sentiment is echoed by the European Parliamentary Research Service (EPRS) in its analysis of the GDPR and how it may be applied to AI (EPRS, 2020)[[80]](#footnote-81).

When it comes to privacy and data protection, the EU GDPR is a landmark legislation referred to as a model by global actors – including within the recommendations for reforms to PIPEDA made by the Privacy Commissioner of Canada (OPC, 2020a)[[81]](#footnote-82). Although the GDPR only applies to Canadian actors that handle the personal data of individuals in the EU (Sanchez, n.d., p.1)[[82]](#footnote-83), coming into compliance with requirements beyond what is stipulated under domestic legislation like the PIPEDA presents an opportunity to improve the overall privacy and security risk posture in Canada (Sanchez, n.d., p.6)[[83]](#footnote-84). The GDPR is also widely held as the strictest data protection law in the world – the Canadian ambition to entrench privacy as a fundamental human right within AI regulation (OPC, 2020a)[[84]](#footnote-85) can thus be achieved through greater alignment with the GDPR and its provisions on data protection and privacy.

A study conducted by the European Parliamentary Research Service (EPRS) on the impact of the GDPR on AI, given that the GDPR was not developed with intelligent and autonomous systems in mind, found that risk-based approaches to data protection are capable of addressing AI-related risks (EPRS, 2020, p.66)[[85]](#footnote-86). A risk-based approach focuses on harm prevention through organizational and technological measures, and considers whether data protection measures should be differentiated based on the financial and technical capacity of system providers. It is recommended that risk prevention and mitigation measures be allocated based on the severity of the risk and whether personal data impacting a large set of individuals is being processed (EPRS, 2020, p.67)[[86]](#footnote-87).

A risk-based approach is particularly significant for AI, considering the impact that automated decision-making such as credit scoring systems may have on the trajectory of a person’s life, while other systems such as chatbots are relatively harmless (EPRS, 2020, p.66)[[87]](#footnote-88). The EU AIA follows through on the recommendation regarding a risk-based approach with varied requirements based on the level of potential risk, considering the tiered classification of AI systems and proportionate interventions outlined in the Act. The AIDA would benefit from a similar tiered framework, as the current proposal fails to define high-impact and minimal risk systems.

*Soft law and hard law mechanisms*

The EU casts a wider net to capture AI systems of various risk levels within the AIA through its multi-tiered system, embodying a hard law approach. This includes unacceptable risk, high risk, and low or minimal risk systems, encompassing “unacceptable risk” activities from biometric and facial identification systems to “minimal risk” appointment scheduling systems (European Commission, 2021)[[88]](#footnote-89). This reflects the legally recognized principle of the precautionary principle in the EU, where steps must be taken to minimize the threat of the unknown (European Union, 2016)[[89]](#footnote-90), as well as an embedded human-centric approach that prioritizes human dignity and individual freedoms. In contrast, Canada only addresses “high-impact” systems in the AIDA, which are not clearly defined, with all other AI systems falling within an unspecified or minimal risk category covered by a temporary and non-binding voluntary code of conduct (Government of Canada, 2023a)[[90]](#footnote-91). This reflects Canada’s preference for a soft law approach in comparison.

Regulatory frameworks in both jurisdictions provide the option to abide by voluntary codes of conduct. In Canada, the Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems came into effect in September 2023 (Government of Canada, 2024)[[91]](#footnote-92). It identifies measures to be undertaken while the AIDA is in draft phase for all firms developing or managing the operations of a generative AI system. However, once the AIDA comes into effect, the Voluntary Code of Conduct will no longer apply. The code entails the commitment to achieving accountability, safety as the systems are subject to risk assessments, fairness and equity, transparency as information is published to allow consumers to make informed decisions regarding risk, human oversight and monitoring, and validity and robustness to ensure the system operates as intended (Government of Canada, 2024)[[92]](#footnote-93).

The key difference is that Canada’s voluntary code of conduct is to be used temporarily until formal regulation is in effect to strengthen the public’s confidence in AI systems. In contrast, the EU encourages minimal risk systems to adopt voluntary codes of conduct as a supplement to the lack of legal obligations under the AIA (European Commission, 2023)[[93]](#footnote-94). The EU presents a more robust framework, even for minimal risk systems that do not have to abide by legal requirements, by encouraging the use of the voluntary code of conduct independent of formal regulation coming into effect. It will be prudent for Canada to consider lengthening the lifespan of its own voluntary code past AIDA implementation as a form of “best practice” for industry. Even if there is no legal obligation to adopt the voluntary code, continued encouragement of its use signals the human-centered ethos of AI service provision to business actors. In addition, given that the current draft AIDA focuses on high-impact AI systems, the retention of the voluntary code of conduct can help keep low-impact systems accountable in the absence of legal requirements, similar to the EU’s approach.

**Key Challenges and Opportunities**

This section identifies key challenges and opportunities for AI regulation in the EU and Canada. Challenges include the potential for AI to discriminate based on protected characteristics, such as race and gender (Buolamwini & Gebru, 2018), the digital divide and widening of inequality in the EU (Caradaica, 2020), “deep fakes” pumping false information into the market (Chesney & Citron, 2018), and the challenge of regulating in a federal context for Canada (Martin-Bariteau & Scassa, 2020).

The first challenge is that machine-learning algorithms are capable of discriminating based on race and gender. After evaluating three commercial gender classification systems based on a balanced facial analysis dataset (gender and skin type), it was found that darker-skinned females are the most misclassified group by AI facial recognition technology (Buolamwini & Gebru, 2018, p.1)[[94]](#footnote-95). While AI technology is not trained to perform high-stakes tasks such as rendering a legal decision, secondary tasks such as facial recognition software used to identify suspects forms potential input for high stakes decisions. An error in the output of a facial recognition algorithm thus has serious consequences when used as input for other tasks. Additionally, given that many AI systems rely on machine learning algorithms, there is the risk that the systems will be trained by biased data. (Buolamwini & Gebru, 2018, p.1)[[95]](#footnote-96).

Facial recognition systems displaying bias against women and people of color, resulting in discriminatory or harmful outcomes, demonstrates cause for the erosion of trust in AI systems. The aforementioned study conducted by Buolamwini & Gebru (2018)[[96]](#footnote-97) has been referenced by the Government of Canada (2023a)[[97]](#footnote-98) in its AIDA Companion Document to explain the potential for bias in AI systems. The Canadian government subsequently claims that the AIDA is the first legal framework in Canada to address the adverse impacts of systemic bias in AI systems in a commercial context by providing individuals with recourse for discrimination under the Canadian Human Rights Act (CHRA). However, depending on the level of transparency of the AI system, individuals subject to biased output from AI may never be aware that it has occurred (Government of Canada, 2023a)[[98]](#footnote-99), and seeking redress after the fact can be a costly endeavor.

The government also claims that the AIDA would address the risk of high-impact AI systems causing harm to historically marginalized communities on a large scale by requiring businesses to assess and mitigate risks of harm or biased output under the CHRA and AIDA regulatory requirements. Although biased output has been clearly identified as an issue, such accountability mechanisms still need to be determined through regulation. This means that there are no clear accountabilities in Canada for what businesses should do to ensure that high-impact AI systems are safe and non-discriminatory, and we remain at ground zero (Government of Canada, 2023a)[[99]](#footnote-100). It is proposed that obligations for high-impact systems in the AIDA will align with international norms on AI governance such as human oversight of AI systems, monitoring, transparency on the nature of the AI system, and accountability (Government of Canada, 2023a)[[100]](#footnote-101).

The vagueness around “high-impact” systems and accountability mechanisms for businesses in the draft AIDA makes it increasingly difficult to mitigate systemic bias. Comparatively, in the EU’s draft AIA, AI systems used in education and vocational training for assigning persons to educational institutions, or to evaluate persons on tests as a precondition for their education, are one of the many activities defined as high-risk. Such results can determine the professional course of a person’s life and their subsequent ability to secure a livelihood, and the improper use of AI in this scenario may perpetuate existing patterns of discrimination against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origin (European Commission, 2021, p.26)[[101]](#footnote-102). Given the specific context of education and vocational training among the many high-risk systems outlined in the draft, it is recommended that legal requirements related to data governance, documentation and record keeping, human oversight, robustness, accuracy, and security are imposed. Furthermore, there are specific requirements proposed that aim to minimize the risk of algorithmic discrimination, including the design and quality of data sets used for the development of AI systems, in conjunction with obligations for testing, risk management, documentation, and human oversight throughout the system’s lifecycle (European Commission, 2021, p.4)[[102]](#footnote-103).

As such, it is important for Canada to fleshout the high-impact category for AI systems to effectively mitigate systemic bias and human rights concerns. Canada could consider implementing a conformity assessment procedure, where an independent body or notifying authority provides accreditation for a high-impact system (European Commission, 2021, p.59)[[103]](#footnote-104) similar to the EU, rather than requiring businesses to self-assess to mitigate bias. Voluntary, self, or co-regulation in the realm of privacy has had a poor track record due to recurring issues with stakeholders and regulatory bodies becoming dominated by the interests they regulate. Additionally, certification, codes of conduct, and requirements to demonstrate compliance may lead to ungenuine practices rather than the sincere protection of the public (EPRS, 2020, p.69)[[104]](#footnote-105). Independent accreditation for high-impact systems can help overcome such issues with self-assessment.

Secondly, there is a concern that AI has the potential to exacerbate inequality and widen the “digital divide”. The OECD (2001) refers to the “digital divide” as “the gap between individuals, households, businesses and geographic areas at different socioeconomic levels with regard both to their opportunities to access information communication technology (ICT) and to their use of the Internet for a wide variety of activities” (as cited in Carter et al., 2020, p.257)[[105]](#footnote-106). This definition implies that parts of the world population cannot access ICT, creating a disparity in the quality of life and opportunities available to the technology enabled and non-technologically enabled (Carter et al., 2020, p.257)[[106]](#footnote-107). Although beneficial, digital innovations thus result in unintentional adverse effects – namely, inequities that separate those who have access to technology and those who do not (Carter et al., 2020, p.255)[[107]](#footnote-108). In the context of AI, innovations advantage those who can capitalize on the technology, while leaving those who lack the necessary technological skills to harness it behind.

Caradaica (2020)[[108]](#footnote-109) analyzes the national AI strategies of 20 EU Member States to argue that potential sources of inequality exist in education, jobs, the private sector, the public sector, and in Member States’ global approach. Since the EU has asked Member States to design their own national strategies in addition to supranational regulation, resulting strategies are very diverse and have the potential to widen the “digital divide”. This refers to the idea that economic and social gaps are generated each time a new technology is broadly implemented in society (Caradaica, 2020, p.14)[[109]](#footnote-110).Furthermore, among the varying categories and implementation of AI, narrow AI includes clever programming and machine learning. Narrow AI is a program that can achieve intelligent behaviour such as computer-controlled characters in a video game, and machine learning entails algorithms learning from large amounts of data such as driverless cars or facial recognition. Achievements in these fields have transformed society and our way of life by automating manual and mental work. This advancement has produced disparate impacts for medium and low-skilled workers through stagnated incomes, downward pressure on unskilled workers’ wages, and a reduced share of income for labour across many Western countries. In addition, the digital divide may be deepened due to the inability to afford new devices or software, or understand their use (Caradaica, 2020, p.14)[[110]](#footnote-111). A shift in demand for jobs involving advanced digital skills could also result in wage increases for jobs requiring digital literacy, creating further inequalities between individuals who are AI literate and those who are not (Carter et al., 2020, p.259)[[111]](#footnote-112).

The EU Strategy for AI (European Commission, 2018)[[112]](#footnote-113) acknowledges the socioeconomic aspect of the digital divide by providing for the impact of automation on employment. The strategy claims that no one should be left behind, and that the European Commission will support Member States by setting up training schemes, conducting analyses on anticipated labour market changes and the subsequent mismatch in skills, supporting digital traineeships in advanced digital skills for students, integrating AI within curricula to develop a talent pool for AI, and more (European Commission, 2018, p.13)[[113]](#footnote-114).

In contrast, as part of the Pan-Canadian AI Strategy (Government of Canada, 2022)[[114]](#footnote-115), which is the national strategy on AI in Canada, the Government of Canada committed $208 million over ten years to fund programs to attract, retain, and develop academic research talent. There is an opportunity for Canada to implement a strategy to address the digital divide through dedicated resources to support training and traineeship programs similar to those proposed in the EU Strategy for AI and ensure the equitable and “human-centered” uptake of AI technology. The 2024 federal budget has earmarked $50 million over five years to support workers who could be affected by artificial intelligence (The Canadian Press, 2024), but the details on how workers will be supported are not yet available.

Thirdly, “deep fakes” pose legal and policy challenges by creating and disseminating information that is difficult for end-users to determine the falsehood of. Deep fakes refer to AI technology used to alter images, audio, and video in a highly realistic manner, often maliciously (Chesney & Citron, 2018, p.1757)[[115]](#footnote-116). For instance, deep fakes may be used in election campaigns to tarnish the reputation of potential candidates, eroding the democratic process (Chesney & Citron, 2018, p.1757)[[116]](#footnote-117). There is also potential for governments to utilize the technology for hostile or intelligence purposes. Thus, industry, academia, and the government have an interest in pushing the technology forward for personal, intellectual, and state gains. Deep fakes are arguably the most well-known AI software among the general public, contributing to the conception of AI as untrustworthy and exploitative. To address the concerns around deep fakes, in the EU, the draft AIA contains a provision on the disclosure of synthetic content, also known as deep fakes. Users of AI systems that generate or manipulate image, audio, or video in a way that mimics existing people, objects, places, or events to falsely appear as authentic must disclose their artificial nature. However, there are exemptions in place for legally authorized crime prevention (Veale & Borgesius, 2021, p.108)[[117]](#footnote-118).

However, the AIA provision on disclosure is far from perfect. Placing the onus on users to disclose artificial content raises questions regarding enforcement, particularly around the investigation of undisclosed deep fakes, whether the authorities can investigate users of AI platforms, and whether the digital forensics expertise exists to analyze such material online (Veale & Borgesius, 2021, p.108)[[118]](#footnote-119). Comparatively, in Canada there is no explicit mention of such technology and its malicious potential in the draft AIDA, presenting a gap in the regulation (Parliament of Canada, 2022)[[119]](#footnote-120). The AIDA proposal is in its infancy relative to the draft AIA proposed by the EU, largely due to the fact that many requirements and definitions have been resolved to be established later in regulation. For instance, the AIDA proposes that AI regulation should “prohibit reckless and malicious uses of AI that cause serious harm to Canadians and their interests through the creation of new criminal law provisions” (Government of Canada, 2023a)[[120]](#footnote-121) without specifying what “reckless” or “malicious” use entails. Unless safeguards against synthetic content generated by AI is enshrined in the AIDA, it is unlikely that Canada can achieve an approach to AI systems based in trust and accountability. To reduce the risk of recidivism, interventions against deep fakes can be determined on a case-by-case basis, with consideration for the type of sanction (eg. imprisonment, community service, fine), probation, parole, and eligibility for programs such as training and education (Custers & Fosch-Villaronga, 2022, p.211)[[121]](#footnote-122).

Lastly, the federal and constitutional setting in Canada means that there will be shared jurisdiction across national and sub-national governments in the regulation of AI, presenting challenges with effective coordination and streamlined guidelines for industry. A range of subject matter that is not always within federal jurisdiction, or is shared jurisdiction, will be brought into question by AI, such as privacy and data protection, health, and human rights. Competition law and intellectual property are managed federally, while consumer protection law, property law, and torts are managed provincially. Another example is biased data being used to train AI algorithms, which has privacy, human rights, and consumer protection implications – each governed by different legislation in different agencies (Martin-Bariteau & Scassa, 2020, p.9)[[122]](#footnote-123).

There have also been strides to reform different regulatory frameworks to accommodate the growing use of AI by varying actors. In 2020, the Privacy Commissioner of Canada published recommendations to reform the PIPEDA to address AI-related concerns. There have also been changes at the provincial level, such as private sector privacy laws emerging in Quebec, reforms to the Personal Information Protection Act in British Columbia, and a private sector data protection law that would likely address AI concerns being contemplated in Ontario (Martin-Bariteau & Scassa, 2020, p.8)[[123]](#footnote-124).

While the EU differs from Canada as a supranational authority, its reliance on national supervisory authorities to oversee the implementation of harmonised rules proposed within the AIA embodies a quasi-federal structure (Lilkov, 2021, p.170)[[124]](#footnote-125). The proposed rules will be enforced through governance at the Member State level while building on existing structures, and cooperation at the EU level will be ensured through the establishment of a European Artificial Intelligence Board (European Commission, 2021, p.3)[[125]](#footnote-126). There is also an emphasis on harmonised rules in the draft AIA to ensure consistency with existing policy provisions. As such, the new proposal aligns itself with a host of harmonised legislation listed under Annex II of the draft AIA, as well as the EU Charter of Fundamental Rights, the GDPR, and the Law Enforcement Directive (European Commission, 2021, p.4)[[126]](#footnote-127).

To facilitate collaboration across jurisdictions and ensure a smooth transition process as industry comes into compliance with proposed legislation, Canada should consider creating a horizontal and cross-cutting policy-making body similar to the European Artificial Intelligence Board. In the AIA, it is proposed that the Board will operate at the Union level and will be composed of representatives from Member States and the European Commission. It will be responsible for contributing to the implementation of the AIA by facilitating cooperation between national supervisory authorities overseeing the implementation of the AIA within their respective jurisdictions and sharing best practices among member states (European Commission, 2021, p.15)[[127]](#footnote-128).

In contrast, the current draft AIDA proposes the instatement of an AI and Data Commissioner, as well as an Advisory Committee to assist the Minister of Innovation, Science, and Industry with the administration of the proposed legislation (Parliament of Canada, 2022)[[128]](#footnote-129). The responsibilities of the AI and Data Commissioner have yet to be defined, but it is proposed in vague terms that they will be empowered to monitor compliance and intervene if necessary to ensure that AI systems are safe and non-discriminatory (Government of Canada, 2023e)[[129]](#footnote-130). The Commissioner’s work would also include coordinating with other regulators to ensure consistent application across different contexts and tracking systemic effects of AI systems to inform policy decisions. Defining the work of the Commissioner through public consultation has been identified as a priority following the royal assent of Bill C-27 (Government of Canada, 2023a)[[130]](#footnote-131).

To facilitate cooperation in AI regulation in the federal context in Canada, an AI Board that draws from the expertise of sub-national representatives (parallel to national supervisory authorities in the EU) representing their respective province or territory could be implemented under the purview of the Commissioner. The Board would thus contribute to the tracking and policy advising function of the Commissioner. The regulation of AI is a massive undertaking, and an AI board with territorial representation could provide for effective collaborative work.

**Conclusion**

AI has been ubiquitous in our digital activities for decades – search engines like Google are stark proof of this – but its recent accessibility through applications such as ChatGPT, and its deployment in more proximal sectors of the labour market, has increased public consciousness of its existence and generated the need for a regulatory regime more than ever before. This paper sought to compare the regulatory frameworks proposed within the EU and Canada, given that they are two jurisdictions that have pledged to become global leaders in the AI industry. We have argued that the EU has demonstrated a preference for a hard law approach through a robust risk-based tiered framework in the AIA, and embedded principles such as the precautionary principle and a human-centric approach. In contrast, Canada is inclined towards a soft law approach, due to the lack of specificity around “high-impact” systems in the AIDA, and the reliance on non-binding tools such as companion documents, voluntary codes of conduct, and directives in the regulation of AI. Given that a hard law approach is more legally binding, it is better suited to enforceability and the protection of the public, giving the EU an edge in its regulatory framework. Although Canada implements a harm-based approach in its consideration for high and minimal impact systems, and reflects a human-centric approach through the ambition to entrench privacy as a fundamental human right similar to the GDPR, the EU is more successful in implementing the future-oriented outlook needed to address the unanticipated consequences for AI systems by prioritizing risk over harm in policy development.

This paper has also aimed to compare the current regulatory frameworks on AI in the EU and Canada to identify challenges, subsequent gaps, and make recommendations for effective governance. Canadian governance of AI vis-à-vis the EU AIA would benefit from a clearer definition of AI systems that constitute as high-impact, a third-party conformity assessment procedure rather than self-assessment for human rights compliance by businesses, the imposition of a tiered risk-based approach similar to the EU rather than a single-tier for high impact systems, delegated resources to address the digital divide with the growth of AI through skills training and traineeship programs, safeguards against synthetic content such as deep fakes within the draft AIDA, and a horizontal policymaking body to encourage cooperation across government departments and sub-national jurisdictions.

**References**

Baldridge, D., Coleman, B., & Sandhu J. A. (2024, February 14). *The terminology of AI regulation: Preventing “harm” and mitigating “risk”*. Schwartz Reisman Institute for Technology and Society. <https://srinstitute.utoronto.ca/news/terminology-regulation-risk-harm>

Beardwood, J. (2023). Heads Up: The Companion Document to the Canadian Artificial Intelligence and Data Act – AIDA Companion provides answers to some key questions but then raises others. *Computer Law Review International, 24*(3), 65-72. <https://doi.org/10.9785/cri-2023-240302>

Bosi, G. (2021, November 30). *Overcoming the “Soft vs Hard Law” Debate in the Development of New Global Health Instruments*. OpinioJuris. <https://opiniojuris.org/2021/11/30/overcoming-the-soft-vs-hard-law-debate-in-the-development-of-new-global-health-instruments/>

Buolamwini, J. & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research, 81*, 1-15. <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>

Caradaica, M. (2020). Artificial Intelligence and Inequality in European Union. *Europolity: Continuity and Change in European Governance, 14*(1), 5-31. <https://www-ceeol-com.myaccess.library.utoronto.ca/search/viewpdf?id=906412>

Carter, L., Liu, D., & Cantrell, C. (2020). Exploring the Intersection of the Digital Divide and Artificial Intelligence: A Hermeneutic Literature Review. *AIS Transactions on Human-Computer Interaction, 12*(4), 253-275. <https://doi.org/10.17705/1thci.00138>

Chesney, R. & Citron, K. D. (2018). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review,* *107*(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J.

Custers, B., & Fosch-Villaronga, E. (2022). AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law. In *Law and Artificial Intelligence* (Vol. 35). T.M.C. Asser Press.

European Center for Constitutional and Human Rights. (n.d.). *Definition: Hard law/soft law*. <https://www.ecchr.eu/en/glossary/hard-law-soft-law/>

European Commission. (2018, April 25). *Artificial Intelligence for Europe*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237>

European Commission. (2024, January 31). *Ethics guidelines for trustworthy AI*. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

European Commission. (2019, April 8). *Ethics Guidelines for Trustworthy AI*. High-Level Expert Group on Artificial Intelligence. <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419>

European Commission. (2020, February 19). *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*. <https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf>

European Commission. (2023, December 12). *Artificial Intelligence – Questions and Answers.* <https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683>

European Commission. (2021, April 21). *Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*. <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF>

European Parliament. (2023). *Artificial Intelligence Act: Deal on comprehensive rules for trustworthy AI*. <https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai>

European Parliamentary Research Service. (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. European Parliament. <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf>

European Union. (2016, November 30). *The precautionary principle*. <https://eur-lex.europa.eu/EN/legal-content/summary/the-precautionary-principle.html>

Evans, M., White, L., & Sinclair, M. (2023, December 12). *The EU’s AI Act: the position is agreed.* Norton Rose Fulbright. <https://www.dataprotectionreport.com/2023/12/the-eus-ai-act-the-position-is-agreed/>

Government of Canada. (2023a, March 13). *The Artificial Intelligence and Data Act (AIDA) – Companion document*. <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document>

Government of Canada. (2023b, April 25). *Directive on Automated Decision-Making.* <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>

Government of Canada. (2023c, April 25). *Algorithmic Impact Assessment Tool*. <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>

Government of Canada. (2023d, March 13). *Canada’s Digital Charter*. <https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world>

Government of Canada. (2023e, September 27). *Artificial Intelligence and Data Act*. <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act>

Government of Canada. (2024, January 12). *Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems*. <https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems>

Government of Canada. (2022, July 20). *Pan-Canadian Artificial Intelligence Strategy*. <https://ised-isde.canada.ca/site/ai-strategy/en>

Justo-Hanani, R. (2022). The Politics of Artificial Intelligence Regulation and Governance Reform in the European Union. *Policy Sciences,* *55*(1),137–59. <https://doi.org/10.1007/s11077-022-09452-8>.

Lilkov, D. (2021). Regulating artificial intelligence in the EU: A risky game. *European View, 20*(2), 166-174. <https://doi.org/10.1177/17816858211059248>

Martin-Bariteau, F., & Scassa, T. (2020). Introduction. *Artificial Intelligence and the Law in Canada*. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3734675>

Neschke, S., Soroushian, J., & Pesner, J. (2022). *Artificial Intelligence Policy and the European Union*. Bipartisan Policy Center. [bipartisanpolicy.org/download/?file=/wp-content/uploads/2022/08/AI-Policy-and-EU-Final-Paper.pdf](https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2022/08/AI-Policy-and-EU-Final-Paper.pdf)

Office of the Privacy Commissioner of Canada. (2020a, November 12). *A Regulatory Framework for AI: Recommendations for PIPEDA Reform*. <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/>

Office of the Privacy Commissioner of Canada. (2020b, November 12). *Consultation on artificial intelligence*. <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/>

Office of the Privacy Commissioner of Canada. (2020c, January 28). *Seeking views on the OPC’s recommendations to Government/Parliament*. <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pos_ai_202001/#fn1-rf>

Parliament of Canada. (n.d.). *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other acts*. <https://www.parl.ca/LegisInfo/en/bill/44-1/c-27>

Parliament of Canada. (2022, June 16). *Bill C-27 An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*. House of Commons of Canada. <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading>

Rissland, E. L., Ashley, K. D., & Loui, R. P. (2003). AI and Law: A fruitful synergy. *Artificial Intelligence*, *150*(1), 1–15. <https://doi.org/10.1016/S0004-3702(03)00122-X>

Sanchez, I. R. (n.d.). *GDPR and Canadian organizations: Addressing key challenges*. Deloitte. <https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-gdpr-for-canadian-businesses-article-aoda.pdf>

Scassa, T. (2023a). Regulating AI in Canada: A Critical Look at the Proposed Artificial Intelligence and Data Act. *Canadian Bar Review,* *101*(1). <https://cbr.cba.org/index.php/cbr/article/view/4817/4539>

Scassa, T. (2023b, August 16). *Canada’s Draft AI Legislation Needs Important Revisions*. Centre for International Governance Innovation. <https://www.cigionline.org/articles/canadas-draft-ai-legislation-needs-important-revisions/>

Thind, J. (2023). Artificial Impartiality: The Insidious Role of AI in Reinforcing White Supremacy in Canada. Faculty of Law, University of Manitoba. <https://mspace.lib.umanitoba.ca/server/api/core/bitstreams/952f23e4-2d56-45dc-974e-a03c3a1acdd9/content>

The Canadian Press. (2024, April 16). *Some of the key highlights from the Liberal government’s 2024 federal budget.* Yahoo! Finance. <https://ca.finance.yahoo.com/heres-liberals-already-promised-todays-080000996.html>

Ulnicane, I. (2022). Artificial intelligence in the European Union: Policy, ethics and regulation. In Hoerber, T., Weber, G., & Cabras I. (Eds.), *The Routledge Handbook of European Integrations* (pp. 254-269). Routledge. 10.4324/9780429262081-1

Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International, 22*(4), 97-112. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852>

Viljanen, M., & Parviainen, H. (2022). AI Applications and Regulation: Mapping the Regulatory Strata. *Frontiers in Computer Science (Lausanne)*, *3*. <https://doi.org/10.3389/fcomp.2021.779957>

1. “Artificial intelligence in the European Union: Policy, ethics and regulation,” in T. Hoerber, G. Weber, & I. Cabras, (Eds.), 2022, *The Routledge Handbook of European Integrations*, p.254. <https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/52622/9780429262081_10.4324_9780429262081-19.pdf?sequence=1&isAllowed=y> [↑](#footnote-ref-2)
2. “The EU’s AI Act: the position is agreed,” M. Evans, L. White, & M. Sinclair, 2023, Norton Rose Fulbright. <https://www.dataprotectionreport.com/2023/12/the-eus-ai-act-the-position-is-agreed/> [↑](#footnote-ref-3)
3. “Artificial intelligence in the European Union: Policy, ethics and regulation,” 2022, in *The Routledge Handbook of European Integrations*, p.254. <https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/52622/9780429262081_10.4324_9780429262081-19.pdf?sequence=1&isAllowed=y> [↑](#footnote-ref-4)
4. “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” by J. Buolamwini & T. Gebru, 2018, *Proceedings of Machine Learning Research, 81*, p.1. <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> [↑](#footnote-ref-5)
5. “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,” by R. Chesney & K. D. Citron, 2018, *California Law Review,* *107*(6), p.1757. <https://doi.org/10.15779/Z38RV0D15J> [↑](#footnote-ref-6)
6. “The Artificial Intelligence and Data Act (AIDA) – Companion document,” Government of Canada, 2023a. <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document> [↑](#footnote-ref-7)
7. “AI and Law: A fruitful synergy,” E. L. Rissland, K. D. Ashley, & R. P. Loui, 2003, *Artificial Intelligence*, *150*(1), p.2. <https://doi.org/10.1016/S0004-3702(03)00122-X> [↑](#footnote-ref-8)
8. Ibid, p.3 [↑](#footnote-ref-9)
9. Ibid, p.5 [↑](#footnote-ref-10)
10. “Definition: Hard law/soft law,” European Center for Constitutional and Human Rights, n.d. <https://www.ecchr.eu/en/glossary/hard-law-soft-law/> [↑](#footnote-ref-11)
11. “Overcoming the “Soft vs Hard Law” Debate in the Development of New Global Health Instruments,” G. Bosi, 2021, OpinioJuris. <https://opiniojuris.org/2021/11/30/overcoming-the-soft-vs-hard-law-debate-in-the-development-of-new-global-health-instruments/> [↑](#footnote-ref-12)
12. “AI Applications and Regulation: Mapping the Regulatory Strata,” M. Viljanen & H. Parviainen, 2022, *Frontiers in Computer Science (Lausanne)*, *3,* p.1. https://doi.org/10.3389/fcomp.2021.779957 [↑](#footnote-ref-13)
13. Ibid, p.5 [↑](#footnote-ref-14)
14. Ibid, p.6 [↑](#footnote-ref-15)
15. Ibid, p.9 [↑](#footnote-ref-16)
16. “The precautionary principle,” by European Union, 2016. <https://eur-lex.europa.eu/EN/legal-content/summary/the-precautionary-principle.html> [↑](#footnote-ref-17)
17. Ibid. [↑](#footnote-ref-18)
18. “Artificial Intelligence Policy and the European Union,” by S. Neschke, J. Soroushian, & J. Pesner, 2022, Bipartisan Policy Center, p.11. <https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2022/08/AI-Policy-and-EU-Final-Paper.pdf> [↑](#footnote-ref-19)
19. “The precautionary principle,” by European Union, 2016. <https://eur-lex.europa.eu/EN/legal-content/summary/the-precautionary-principle.html> [↑](#footnote-ref-20)
20. “White Paper on Artificial Intelligence – A European Approach to Excellence and Trust,” by European Commission, 2020, p.3. <https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf> [↑](#footnote-ref-21)
21. Ibid, p.23. [↑](#footnote-ref-22)
22. “Demystifying the Draft EU Artificial Intelligence Act,” by M. Veale, & F. Z. Borgesius, 2021, *Computer Law Review International, 22*(4), p.98. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852> [↑](#footnote-ref-23)
23. “Regulating artificial intelligence in the EU: A risky game,” by D. Lilkov, 2021, *European View, 20*(2), p.168. <https://doi.org/10.1177/17816858211059248> [↑](#footnote-ref-24)
24. Ibid, p.168. [↑](#footnote-ref-25)
25. Veale and Borgesius, 2021, “Demystifying the Draft EU Artificial Intelligence Act,” p.100. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852> [↑](#footnote-ref-26)
26. Lilkov, 2021, “Regulating artificial intelligence in the EU: A risky game,” p.168. <https://doi.org/10.1177/17816858211059248> [↑](#footnote-ref-27)
27. Veale and Borgesius, 2021, “Demystifying the Draft EU Artificial Intelligence Act,” p.101. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852> [↑](#footnote-ref-28)
28. “White Paper on Artificial Intelligence – A European Approach to Excellence and Trust,” by European Commission, 2020, p.17. <https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf> [↑](#footnote-ref-29)
29. Ibid, p.17 [↑](#footnote-ref-30)
30. Ibid, p.18. [↑](#footnote-ref-31)
31. Veale and Borgesius, 2021, “Demystifying the Draft EU Artificial Intelligence Act,” p.103. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852> [↑](#footnote-ref-32)
32. Lilkov, 2021, “Regulating artificial intelligence in the EU: A risky game,” p.169. <https://doi.org/10.1177/17816858211059248> [↑](#footnote-ref-33)
33. Veale and Borgesius, 2021, “Demystifying the Draft EU Artificial Intelligence Act,” p.98. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852> [↑](#footnote-ref-34)
34. “The politics of Artificial Intelligence regulation and governance reform in the European Union,” R. Justo-Hanani, 2022, *Policy Sciences, 55*(1), p.149. <https://doi.org/10.1007/s11077-022-09452-8> [↑](#footnote-ref-35)
35. Ibid, p.149 [↑](#footnote-ref-36)
36. “Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,” by European Commission, 2021, p.3. <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF> [↑](#footnote-ref-37)
37. “Ethics guidelines for trustworthy AI, European Commission, 2024, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> [↑](#footnote-ref-38)
38. Ibid, p.2. [↑](#footnote-ref-39)
39. IAPP, (March 2024) [European Parliament approves landmark AI Act, looks ahead to implementation (iapp.org)](https://iapp.org/news/a/with-eu-ai-act-on-the-books-lawmakers-look-ahead/) [↑](#footnote-ref-40)
40. European Parliament. (2023). *Artificial Intelligence Act: Deal on comprehensive rules for trustworthy AI*. <https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai> [↑](#footnote-ref-41)
41. # European Parliament. (13.03.2024) *Artificial Intelligence Act: MEPs adopt landmark law*

    [Artificial Intelligence Act: MEPs adopt landmark law | News | European Parliament (europa.eu)](https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law) [↑](#footnote-ref-42)
42. “The Artificial Intelligence and Data Act (AIDA) – Companion document,” Government of Canada, 2023a <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document> [↑](#footnote-ref-43)
43. “Artificial Intelligence Policy and the European Union,” by S. Neschke, J. Soroushian, & J. Pesner, 2022, Bipartisan Policy Center, p.10. <https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2022/08/AI-Policy-and-EU-Final-Paper.pdf> [↑](#footnote-ref-44)
44. “Artificial Intelligence and the Law in Canada,” by F. Martin-Bariteau & T. Scassa, 2021, p.6. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3734675> [↑](#footnote-ref-45)
45. “Heads Up: The Companion Document to the Canadian Artificial Intelligence and Data Act – AIDA Companion provides answers to some key questions but then raises others,” J. Beardwood, 2023, *Computer Law Review International, 24*(3), p.65. <https://doi.org/10.9785/cri-2023-240302> [↑](#footnote-ref-46)
46. “Regulating AI in Canada: A Critical Look at the Proposed Artificial Intelligence and Data Act,” Scassa, 2023a, *Canadian Bar Review,* *101*(1), p.7. <https://cbr.cba.org/index.php/cbr/article/view/4817/4539> [↑](#footnote-ref-47)
47. “Canada’s Draft AI Legislation Needs Important Revisions,” Scassa, 2023b. <https://www.cigionline.org/articles/canadas-draft-ai-legislation-needs-important-revisions/> [↑](#footnote-ref-48)
48. Ibid, p.67 [↑](#footnote-ref-49)
49. Veale and Borgesius, 2021, “Demystifying the Draft EU Artificial Intelligence Act,” p.98. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852> [↑](#footnote-ref-50)
50. Beardwood, 2023, ““Heads Up: The Companion Document to the Canadian Artificial Intelligence and Data Act – AIDA Companion,” p.67, <https://doi.org/10.9785/cri-2023-240302> [↑](#footnote-ref-51)
51. “The Artificial Intelligence and Data Act (AIDA) – Companion document,” Government of Canada, 2023a. <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document> [↑](#footnote-ref-52)
52. Ibid. [↑](#footnote-ref-53)
53. “Directive on Automated Decision-Making,” by Government of Canada, 2023b, <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592> [↑](#footnote-ref-54)
54. Ibid. [↑](#footnote-ref-55)
55. “Algorithmic Impact Assessment Tool,” Government of Canada, 2023c, <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html> [↑](#footnote-ref-56)
56. “Artificial Impartiality: The Insidious Role of AI in Reinforcing White Supremacy in Canada,” J. Thind, 2023, Faculty of Law, University of Manitoba, p.21. <https://mspace.lib.umanitoba.ca/server/api/core/bitstreams/952f23e4-2d56-45dc-974e-a03c3a1acdd9/content> [↑](#footnote-ref-57)
57. Ibid, p.19 [↑](#footnote-ref-58)
58. “A Regulatory Framework for AI: Recommendations for PIPEDA Reform,” Office of the Privacy Commissioner of Canada, 2020a. <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/> [↑](#footnote-ref-59)
59. “Seeking views on the OPC’s recommendations to Government/Parliament,” Office of the Privacy Commissioner of Canada, 2020c. <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pos_ai_202001/#fn1-rf> [↑](#footnote-ref-60)
60. “Consultation on artificial intelligence,” Office of the Privacy Commissioner of Canada, 2020b. <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/> [↑](#footnote-ref-61)
61. “RE: Consultation on Artificial Intelligence,” Ontario Society of Professional Engineers, n.d., <https://ospe.on.ca/wp-content/uploads/2020/03/Office-of-the-Privacy-Commissioner-of-Canadas-Consultation-on-Artificial-Intelligence.pdf> [↑](#footnote-ref-62)
62. “The Artificial Intelligence and Data Act (AIDA),” Canadian Labour Congress, 2023, p.2 <https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12711885/br-external/CanadianLabourCongress-e.pdf> [↑](#footnote-ref-63)
63. Ibid, p.2 [↑](#footnote-ref-64)
64. Ibid, p.3 [↑](#footnote-ref-65)
65. Ibid, p.5 [↑](#footnote-ref-66)
66. “An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other acts,” Parliament of Canada, (n.d.). <https://www.parl.ca/LegisInfo/en/bill/44-1/c-27> [↑](#footnote-ref-67)
67. “Canada’s Digital Charter,” Government of Canada, 2023d. <https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world> [↑](#footnote-ref-68)
68. Ibid. [↑](#footnote-ref-69)
69. “Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,” by European Commission, 2021, p.1. <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF> [↑](#footnote-ref-70)
70. “Canada’s Digital Charter,” Government of Canada, 2023d. <https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world> [↑](#footnote-ref-71)
71. “The Artificial Intelligence and Data Act (AIDA) – Companion document,” Government of Canada, 2023a. <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document> [↑](#footnote-ref-72)
72. “The terminology of AI regulation: Preventing ‘harm’ and mitigating ‘risk’”, D. Baldridge, B. Coleman, & J. A. Sandhu, 2024, Schwartz Reisman Institute for Technology and Society. <https://srinstitute.utoronto.ca/news/terminology-regulation-risk-harm> [↑](#footnote-ref-73)
73. Ibid. [↑](#footnote-ref-74)
74. Beardwood, 2023, ““Heads Up: The Companion Document to the Canadian Artificial Intelligence and Data Act – AIDA Companion,” p.66, <https://doi.org/10.9785/cri-2023-240302> [↑](#footnote-ref-75)
75. Ibid, p.66 [↑](#footnote-ref-76)
76. Beardwood, 2023, ““Heads Up: The Companion Document to the Canadian Artificial Intelligence and Data Act – AIDA Companion,” p.66, <https://doi.org/10.9785/cri-2023-240302> [↑](#footnote-ref-77)
77. Ibid, p.66. [↑](#footnote-ref-78)
78. “Canada’s Draft AI Legislation Needs Important Revisions,” Scassa, 2023b. <https://www.cigionline.org/articles/canadas-draft-ai-legislation-needs-important-revisions/> [↑](#footnote-ref-79)
79. “The terminology of AI regulation: Preventing ‘harm’ and mitigating ‘risk’”, D. Baldridge, B. Coleman, & J. A. Sandhu, 2024, Schwartz Reisman Institute for Technology and Society. <https://srinstitute.utoronto.ca/news/terminology-regulation-risk-harm> [↑](#footnote-ref-80)
80. “The impact of the General Data Protection Regulation (GDPR) on artificial intelligence,” European Parliamentary Research Service, 2020. <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> [↑](#footnote-ref-81)
81. “A Regulatory Framework for AI: Recommendations for PIPEDA Reform,” Office of the Privacy Commissioner of Canada, 2020a. <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/> [↑](#footnote-ref-82)
82. “GDPR and Canadian organizations: Addressing key challenges,” I. R. Sanchez, n.d., Deloitte, p.1. <https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-gdpr-for-canadian-businesses-article-aoda.pdf> [↑](#footnote-ref-83)
83. Ibid, p.6 [↑](#footnote-ref-84)
84. “A Regulatory Framework for AI: Recommendations for PIPEDA Reform,” Office of the Privacy Commissioner of Canada, 2020a. <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/> [↑](#footnote-ref-85)
85. “The impact of the General Data Protection Regulation (GDPR) on artificial intelligence,” European Parliamentary Research Service, 2020, p.66. <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> [↑](#footnote-ref-86)
86. Ibid, p.67 [↑](#footnote-ref-87)
87. Ibid, p.66 [↑](#footnote-ref-88)
88. “Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,” by European Commission, 2021. <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF> [↑](#footnote-ref-89)
89. “The precautionary principle,” by European Union, 2016. <https://eur-lex.europa.eu/EN/legal-content/summary/the-precautionary-principle.html> [↑](#footnote-ref-90)
90. “The Artificial Intelligence and Data Act (AIDA) – Companion document,” Government of Canada, 2023a. <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document> [↑](#footnote-ref-91)
91. “Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems,” Government of Canada, 2024. <https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems> [↑](#footnote-ref-92)
92. Ibid. [↑](#footnote-ref-93)
93. “Artificial Intelligence – Questions and Answers,” European Commission, 2023. <https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683> [↑](#footnote-ref-94)
94. “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” by J. Buolamwini & T. Gebru, 2018, *Proceedings of Machine Learning Research, 81*, p.1. <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> [↑](#footnote-ref-95)
95. Ibid, p.1 [↑](#footnote-ref-96)
96. Ibid. [↑](#footnote-ref-97)
97. “The Artificial Intelligence and Data Act (AIDA) – Companion document,” Government of Canada, 2023a. <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document> [↑](#footnote-ref-98)
98. Ibid. [↑](#footnote-ref-99)
99. Ibid. [↑](#footnote-ref-100)
100. Ibid. [↑](#footnote-ref-101)
101. “Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,” by European Commission, 2021, p.26. <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF> [↑](#footnote-ref-102)
102. Ibid, p.4 [↑](#footnote-ref-103)
103. Ibid, p.59 [↑](#footnote-ref-104)
104. “The impact of the General Data Protection Regulation (GDPR) on artificial intelligence,” European Parliamentary Research Service, 2020. <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> [↑](#footnote-ref-105)
105. “Exploring the Intersection of the Digital Divide and Artificial Intelligence: A Hermeneutic Literature Review,” L. Carter, D. Liu, & C. Cantrell, 2020, *AIS Transactions on Human-Computer Interaction, 12*(4), p.257 <https://doi.org/10.17705/1thci.00138> [↑](#footnote-ref-106)
106. Ibid, p.257 [↑](#footnote-ref-107)
107. Ibid, p.255 [↑](#footnote-ref-108)
108. “Artificial Intelligence and Inequality in European Union,” M. Caradaica, M, *Europolity: Continuity and Change in European Governance, 14*(1), 5-31. <https://www-ceeol-com.myaccess.library.utoronto.ca/search/viewpdf?id=906412> [↑](#footnote-ref-109)
109. Ibid, p.14 [↑](#footnote-ref-110)
110. Ibid, p.14 [↑](#footnote-ref-111)
111. “Exploring the Intersection of the Digital Divide and Artificial Intelligence: A Hermeneutic Literature Review,” L. Carter, D. Liu, & C. Cantrell, 2020, *AIS Transactions on Human-Computer Interaction, 12*(4), p.259 <https://doi.org/10.17705/1thci.00138> [↑](#footnote-ref-112)
112. “Artificial Intelligence for Europe,” European Commission, 2018. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237> [↑](#footnote-ref-113)
113. Ibid, p.13 [↑](#footnote-ref-114)
114. “Pan-Canadian Artificial Intelligence Strategy,” Government of Canada, 2022. <https://ised-isde.canada.ca/site/ai-strategy/en> [↑](#footnote-ref-115)
115. “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,” by R. Chesney & K. D. Citron, 2018, *California Law Review,* *107*(6), p.1757. <https://doi.org/10.15779/Z38RV0D15J> [↑](#footnote-ref-116)
116. Ibid, p.1757 [↑](#footnote-ref-117)
117. Veale and Borgesius, 2021, “Demystifying the Draft EU Artificial Intelligence Act,” p.108. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852> [↑](#footnote-ref-118)
118. Ibid, p.108 [↑](#footnote-ref-119)
119. “Bill C-27 An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts,” Parliament of Canada, 2022. <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading> [↑](#footnote-ref-120)
120. “The Artificial Intelligence and Data Act (AIDA) – Companion document,” Government of Canada, 2023a <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document> [↑](#footnote-ref-121)
121. “AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law,” B. Custers & E. Fosch-Villaronga, 2022, p.211, In *Law and Artificial Intelligence* (Vol. 35). [↑](#footnote-ref-122)
122. “Artificial Intelligence and the Law in Canada,” by F. Martin-Bariteau & T. Scassa, 2021, p.9. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3734675> [↑](#footnote-ref-123)
123. Ibid, p.8 [↑](#footnote-ref-124)
124. Lilkov, 2021, “Regulating artificial intelligence in the EU: A risky game,” p.170. <https://doi.org/10.1177/17816858211059248> [↑](#footnote-ref-125)
125. “Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,” by European Commission, 2021, p.3. <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF> [↑](#footnote-ref-126)
126. Ibid, p.4 [↑](#footnote-ref-127)
127. Ibid, p.15 [↑](#footnote-ref-128)
128. “Bill C-27 An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts,” Parliament of Canada, 2022. <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading> [↑](#footnote-ref-129)
129. “Artificial Intelligence and Data Act,” Government of Canada, 2023e. <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act> [↑](#footnote-ref-130)
130. “The Artificial Intelligence and Data Act (AIDA) – Companion document,” Government of Canada, 2023a. <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document> [↑](#footnote-ref-131)