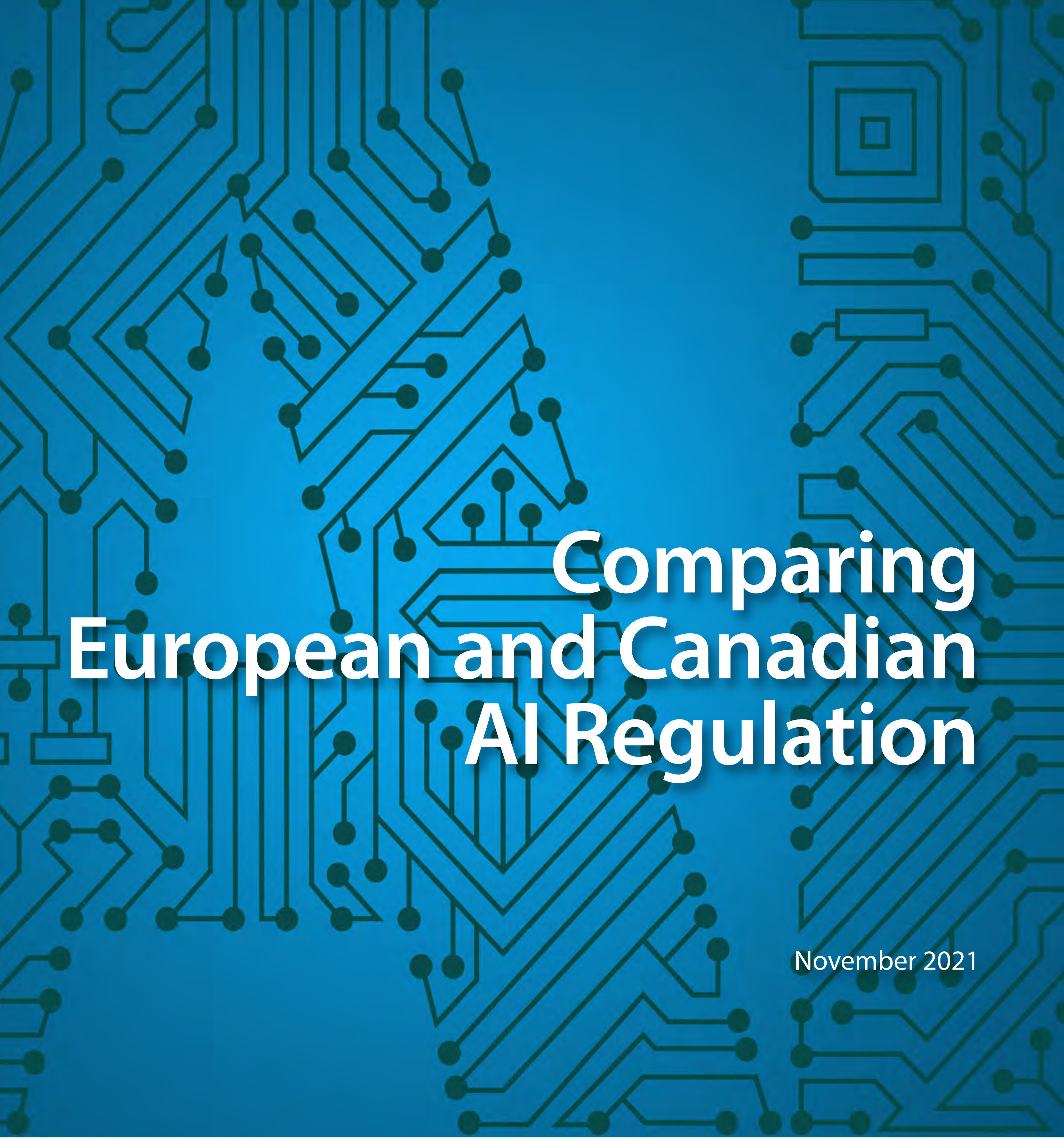

Comparing European and Canadian AI Regulation

November 2021

LCO
CDO
LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO

CHAIRE DE RECHERCHE
I.A. RESPONSABLE
À L'ÉCHELLE MONDIALE

CONTENTS

INTRODUCTION

Regulation of AI and ADM systems has become a pressing issue in Canada and across the world. The Government of Canada's Directive on Automated Decision-making ("the Canada ADM Directive") is the most significant initiative to directly regulate AI and ADM in Canada to date. Many other governments, including the Government of Ontario, have begun to consider AI and ADM regulation as well.

The Law Commission of Ontario and others have noted that AI regulation is a complex undertaking that raises difficult and far-reaching questions and choices about the objective, form and substance of regulation. The LCO's April 2021 Issue Paper, *Regulating AI: Critical Issues and Choices*, identifies many of these issues and choices.[1]

Much has changed since the LCO's paper was published in April 2021. Most significantly, the European Commission has proposed a comprehensive set of rules to govern the use of AI and related technologies in the European Union.[2] The European Commission's proposed AI rules ("the EC Proposal") is perhaps the most comprehensive and important international effort to regulate AI and related technologies to date. In many respects, the EC Proposal represents a very different approach to AI regulation than the Canada ADM Directive.

In this paper, the Law Commission of Ontario and the Research Chair on Accountable Artificial Intelligence in a Global Context have come together to address the following questions:

- How does the EC Proposal compare to the Canada ADM Directive?
- What are the strengths and weaknesses of each approach?
- What lessons can Canadian policymakers learn from the EC approach?

The paper will compare and contrast the Canada ADM Directive and EC Proposal from the perspective of key AI regulation issues, including the definition of AI, risk assessment, bias, disclosure, oversight and enforcement. The LCO and Research Chair on Accountable AI will not discuss the background to these issues in this paper, as each organization has written extensively about these topics elsewhere.[3]

Our goal, rather, is to identify key regulatory choices, illuminate similarities and differences, and the strengths and weaknesses of each approach.

ABOUT THE AUTHORS

The Chair on Accountable AI in a Global Context

The Research Chair on Accountable Artificial Intelligence in a Global Context [4] is led by Professor **Céline Castets-Renard** at the University of Ottawa, in the Civil Law Faculty. The Chair is coordinated by **Eleonore Fournier-Tombs**, Adjunct Professor at the University of Ottawa and data scientist. **Anne-Sophie Hulin** is a Post-Doctoral Researcher and **Claire Boine** is a Doctoral researcher within the Chair.

The Chair explores the social challenges of artificial intelligence (AI) from a legal perspective. The research work is related to social inequalities, with a focus on race, gender, and intersectionality. The Chair also studies inequalities between the Global North and South, and the deployment and design of AI in Africa. Finally, the Chair analyses an area that is still largely unexplored: the risks of AI on humanitarian actions, human rights, and international relations. The aim is to identify inequalities and promote technical and legal solutions to overcome them.

In addition to publishing theoretical analyses, the Chair also conducts action-research through its interdisciplinary center combining law and data science: the Inclusive Technology Lab, led by Eleonore Fournier-Tombs and the Data Trust Lab led by Anne-Sophie Hulin where technical tools are produced at the service of law and society.

Building on its team of experts on Canada, the E.U. and the U.S., as well as its team of external partnerships, the Chair conducts comparative legal and policy studies to guide legislators' action on AI and automated decision-making systems.

The unique and innovative nature of the Chair is due to two main factors: (1) interdisciplinarity combining law and data science in the fight against inequalities; and (2) the construction of a corpus of knowledge in a comparative law perspective on the contributions and limits of AI in the world and its social consequences, to inform policy making on the issue.

The Law Commission of Ontario

The Law Commission of Ontario (LCO) is Ontario's leading law reform agency.[5] The LCO provides independent, balanced and authoritative advice on complex and important legal policy issues. Through this work, the LCO promotes access to justice, evidence-based law reform and public debate.

LCO reports are a practical and principled long-term resource for policymakers, stakeholders, academics and the general public. LCO's reports have led to legislative amendments and changes in policy and practice. They are also frequently cited in judicial decisions, academic articles, government reports and media stories.

This report is part of the LCO's ongoing *AI, ADM and the Justice System* project. The first phase of this project brings together policymakers, legal professionals, technologists, NGOs and community members to discuss the development, deployment, regulation and impact of AI and algorithms on access to justice, human rights, and due process. The LCO's project considers this technology in both the criminal and civil/administrative law justice systems. Completed initiatives within this project include:

- *Regulating AI: Critical Issues and Choices.*
- LCO/Ontario Digital Service Workshop.

- *The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada.*
- LCO Forum on AI and ADM in the Civil and Administrative Justice System.
- LCO Forum on AI in Ontario's Criminal Justice System (with The Citizen Lab, Criminal Lawyers Association and the International Human Rights Program, Faculty of Law, University of Toronto).
- *AI, Automated Decision-Making: Impact on Access to Justice and Legal Aid*.
- *AI for Lawyers: A Primer on Artificial Intelligence in Ontario's Justice System* with Element AI and Osgoode Hall Law School.
- Roundtable on Digital Rights and Digital Society with the Mozilla Foundation.

The LCO is also undertaking projects respecting protection orders, the *Last Stages of Life*, the *Indigenous Last Stages of Life*, and environmental accountability.

BACKGROUND

Artificial intelligence technologies in different areas of application, whether it is predictive analytics, natural language technologies, computer vision, robotics, or another area, have been used increasingly by governments and the private sector in the last decade. Today, AI is one of Canada's fastest growing industries, with Montreal and Toronto respectively having the highest concentration of deep learning start-ups globally.[6] Both the Canadian government and industry have invested a significant amount of money over the last few years in the advancement of this sector, partnering to create innovation hubs, research chairs, and millions of dollars in grants. During the Covid-19 pandemic, many sectors that were severely hit by the crisis, such as the aviation industry in Montreal, used AI funding to retrain their staff and upgrade their technologies, to better prepare for a changing market. AI, however, is still an under-regulated sector, with a combination in Canada of applicable legal frameworks, ethics declarations and best practices covering parts of a very broad and complex technology. Globally, the European Commission was the first regulatory body to attempt a comprehensive legislation to address AI. Others will follow suit soon, selecting regulatory approaches that are best suited for their specific context.

The Growth of AI

Currently, artificial intelligence touches most industries in Canada, spanning from health, to education, supply chains, manufacturing, and even culture. Originally developed as a concept by Alan Turing in the 1950s to bring complex calculations to machines in an approximation of human thinking, its potential has since increased due in large part to improvements in computing power and data storage. Machine learning, a sub-field of artificial intelligence, has notably incorporated learning components when models can be automatically updated to increase their accuracy.

Not only has Canada had a considerable impact on global innovation in AI, through its development of a vibrant start-up ecosystem, but it has also fostered several deep learning experts, attracting research centers from large US-based software companies such as Google, Microsoft and Facebook.

Building Trust and Protecting Human Rights

Artificial intelligence technologies have had important societal impacts, for the good and the bad. While there have been enormous increases in speed and accuracy, from cancer detection, manufacturing optimization and content dissemination, there have also been serious concerns about data protection, biases and consent. The challenge for regulators around the world has therefore been to foster trusted artificial intelligence technologies for innovation while also protecting human rights.

In Canada, stakeholders in research and industry have collaborated to create important ethical frameworks that would aim to inform a possible comprehensive legislation. These include the Montreal Declaration for Responsible AI,[7] as well as the Toronto Declaration Protecting the Right to Equality in Machine Learning.[8]

In the European Union, the Commission created a Digital Single Market,[9] which aims to harmonize digital services in its 27 countries, to allow for interoperability of data and digital innovation. It has also appointed a high-level expert group on artificial intelligence (AI HLEG) to work on Ethics Guidelines for Trustworthy AI.[10] Moreover, the European Commission presented a comprehensive legal framework on AI on April 21, 2021.[11] The legislation is complemented by new rules on Machinery, which aim to adapt the safety rules of products to new AI developments. Together, the AI Law and the Machinery Law aim to increase the safety and fairness of models and machines for both public and industrial use.

Innovation and Safety

While legislation has sometimes been presented as a barrier to innovation, it should, to the contrary, foster innovation by ensuring its safety and appropriateness for the public, increasing the usefulness and trustworthiness of AI. Issues have arisen, often unintentionally, as effects of AI systems, such as discriminatory effects, inaccuracies, and errors, while products that lacked technical maturity were released to the public with little oversight. The government and private sector in Canada have invested heavily in AI research, and will now, it is hoped, begin to pivot towards securing those investments by ensuring that the technologies are trustworthy. To achieve this objective, it is likely that a more thorough approach to AI legislation in Canada, including the development of new legal frameworks, will be required.

Range of Regulatory Options

There are several options from a regulatory perspective.[12] On the one hand, in the European Union, the initiative for regulation lies with the European Commission. It has chosen to propose new rules within the proposed regulation of April 21, 2021, and not just interpret existing ones. It has also decided to have a broad regulatory approach and not a sectoral approach, even if a double approach is pursued within this text. Finally, of the two possible legislative instruments, a regulation and a directive, the regulation has been chosen.

The United States, on the other hand, decided not to create new rules on AI, but rather maintain a sectoral approach. The Federal Trade Commission reminded the rules applicable to consumer and credit law (Fair Credit Reporting Law), especially the Section 5 of the FTC Act.[13]

WHAT IS THE STATE OF THE LAW IN CANADA?

The only comprehensive effort to regulate AI and automated decision-making systems in Canada to date is the Government of Canada's *Directive on Automated Decision-making* ("the Canada ADM Directive").[14] Many other governments, including the Government of Ontario, have begun to consider AI and ADM regulation, but have not yet passed or implemented comprehensive or dedicated regulations.

This is not to say that Canadian governments or policymakers have been inactive. For example, the Government of Canada has introduced Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act*, which could have an impact on privacy protections and AI systems. Similarly, PL 64 in Québec on data protection include new provisions on automated decision-making. Finally, the Government of Ontario has embarked on a major initiative to develop a "Trustworthy AI" framework in Ontario.[15]

The Canada ADM Directive

The Canada ADM Directive was created following an important White Paper and limited public consultations.[16] The Directive applies "systems, tools, or statistical models used to recommend or make an administrative decision about a client of a federal government department."[17]

The Canada ADM Directive requirements are linked to "core administrative law principles such as transparency, accountability, legality, and procedural fairness"[18] and are divided into five categories or stages of use of automated decision-making:

- Performing an Impact Assessment[19]
- Transparency[20]
- Quality Assurance[21]
- Recourse[22]
- Reporting[23]

The Directive requires an algorithmic impact assessment for every automated decision-making system (ADM), including the impact on rights of individuals or communities.

The Canada ADM Directive came into force on April 1st, 2020.[24]

Purpose and Objectives

The purpose of the Canada ADM Directive is set out in section 4, which states:

> 4.1.1. *The objective of this Directive is to ensure that Automated Decision Systems are deployed in a manner that reduces risks to Canadians and federal institutions, and leads to more efficient, accurate, consistent, and interpretable decisions made pursuant to Canadian law.*
>
> 4.2.2. *The expected results of this Directive are as follows:*
>
> 4.2.1. *Decisions made by federal government departments are data-driven, responsible, and comply with procedural fairness and due process requirements.*
>
> 4.2.2. *Impacts of algorithms on administrative decisions are assessed and negative outcomes are reduced, when encountered.*
>
> 4.2.3. *Data and information on the use of Automated Decision Systems in federal institutions are made available to the public, where appropriate.*

Scope

Unlike the proposed EC AI rules, the Canadian Canada ADM Directive is very limited in scope. Most significantly, the Canadian Canada ADM Directive is *not* a rule of general application governing all, or even most, AI, automated decision-making and related systems across Canada. Rather, the scope of the Canada ADM Directive is limited to a restricted class of systems and activities within the Canadian federal government.

Section 5 of the Canadian Canada ADM Directive states that:

> 5.1. *This Directive applies only to systems that provide external services as defined in the Policy on Service and Digital.*

> *5.2. This Directive applies to any system, tool, or statistical models used to recommend or make an administrative decision about a client.*
>
> *5.3. This Directive applies only to systems in production, and excludes Automated Decision Systems operating in test environments.*
>
> *5.4. As per the Policy on Service and Digital, this Directive does not apply to any National Security Systems.*
>
> *5.5. This Directive applies to any Automated Decision System developed or procured after April 1, 2020.*

The Directive's scope and application are thus subject to a number of important exceptions and limitations:

Most significantly, the Canada ADM Directive only regulates systems in the federal government and federal agencies. It does not apply to systems used by provincial governments, municipalities, or provincial agencies such as police services, child welfare agencies and/or many other important public institutions. Nor does the Canadian Canada ADM Directive apply to private sector AI or ADM systems.

Further, the Canada ADM Directive only applies to "any *system, tool, or statistical models used to recommend or make an administrative decision about a client."* Although seemingly broad, Professor Teresa Scassa reminds us why we must also consider the impact of systems that are *outside* of formal definitions:

> *[The Canada ADM Directive] focusses on decision-making…[It] is important to retain sight of the fact that there may be many more choices/actions that do not formally qualify as decisions and that can have impacts on the lives of individuals or communities. These fall outside the [Directive] and remain without specific governance."* [25]

Even within the federal sphere, the extent of the limitations on the Canada ADM Directive are significant. For example, the Canada ADM Directive does not govern:

- Systems that support government non-administrative decisions and/or decisions that are not "about a client."
- Systems could be deployed in the criminal justice system or criminal proceedings.
- National security applications are explicitly exempt from the Directive,[26] as are the Offices of the Auditor General, the Chief Electoral Officer, the Information Commissioner of Canada and the Privacy Commissioner of Canada and others.[27]
- Several agencies, crown corporations, and Agents of Parliament that outside the core federal public service may enter into agreements with the Treasury Board to adopt the Directive's requirements but are not required to do so.[28]
- Systems that do not "provide external services." [29]
- Systems that were in "production" prior to the time the Directive came into effect.[30]

Form of Regulation

The Canada ADM Directive does not have the legal status of a statute or a regulation. Nor is it a voluntary, self-assessing "ethical AI" guideline or best practise. Rather, the Directive falls somewhere in between. As Professor Teresa Scassa notes in her paper analyzing the Directive,

> *While directives are important policy documents within the federal government, and while there are accountability frameworks to ensure compliance, the requirements to comply with directives are internal to government, as are the sanctions. Directives do not create actionable rights for individuals or organizations.*[31]

Risk Assessment

The Canada ADM Directive is a risk-based governance model.

The Canada ADM Directive establishes four levels of risk, judged by the impact of an automated decision determined after an Algorithmic Impact Assessment (discussed below). The Directive then establishes requirements for each impact level, including greater or lesser levels of:

- Notice before ADM decisions and explanations after ADM decisions
- Peer review.
- Employee training; and,
- Human intervention.[32]

In this manner, the Canada ADM Directive effectively establishes a sliding-scale of requirements and due diligence depending on the level of risk identified.

The Algorithmic Impact Assessment (AIA) tool is to help federal officials assess and determine the impact of a system.[33]

Significantly, the Directive establishes baseline requirements that apply to all ADM systems, regardless of their impact level,[34] including:

- Access, diligence, testing and auditability requirements for licensed software.
- Release of custom source code that is owned by the Government of Canada.
- Quality assurance and monitoring requirements, including:
  - –Testing "before launching into production…[to ensure ADM systems] are "tested for unintended data biases and other factors that may unfairly impact outcomes."[35];
  - – Monitoring "outcomes of ADM Systems to safeguard against unintentional outcomes and verify compliance with institutional and program legislation."[36];
  - – Validating the quality of data collected and used.
  - – Consultations with government legal services to ensure the use of the ADM complies with applicable laws.
  - – Providing individuals with "recourse options that are available to challenge the administrative decision"[37]; and,
  - – Reporting information on effectiveness and efficiency.

The Directive requires an Algorithmic Impact Assessment for every automated decision-making system within the Directive's scope, including an assessment of "the impact on rights of individuals or communities." The Directive further requires that Algorithmic Impact Assessments be released publicly.[38]

The AIA is a fundamental component of the Canada ADM Directive. The AIA asks persons or organizations considering an ADM system to address approximately 60 questions designed to evaluate the appropriate risk level for a proposed system.[39] The questions address issues such as project details, the impact of a system and proposed mitigation measures. Once responses to these questions have been input into the AIA, a report is produced indicating the proposed systems' Impact Level and associated requirements for peer review, notice, explanation, and other factors. A final version of the AIA is then required to be publicly posted on Government of Canada websites or as may be required by the Canada ADM Directive on Open Government.

Questions set out in the AIA include the following:

- Capabilities of system?
- Factor(s) motivating introduction of automation into decision-making process?
- Is project is area of intense public scrutiny and/or frequent litigation?
- Are clients in the relevant "line of business particularly vulnerable?"
- Are stakes of decisions very high?
- Will project have major impacts on numbers of staff or their rolls?
- Will project require new policy authority?
- Whether algorithm used is a (trade) secret?
- Whether the algorithmic process is difficult to interpret or explain?
- Will system assist or replace human decision-maker?
- Impact of system on the rights and freedoms of individuals, the health and well-being of individuals, the economic interests of individuals, and the ongoing sustainability of an environmental ecosystem?
- Is impact reversible and how long will impact last?
- Who collected data?
- De-risking and mitigation data quality measures, including existence of "documented processes in place to test datasets against biases and other unexpected outcomes."
- De-risking and mitigation procedural fairness measures, including audit trails.
- Is system capable of producing reasons for its decisions/recommendations when required?
- "Recourse process" planned or established for clients that wish to challenge the decision?
- Human override of system decisions?

Disclosure

The Canada ADM Directive includes a mandatory disclosure requirement. Government agencies are required to provide notice on websites when decisions will be made by or with the assistance of AI or ADS, regardless of the applicable impact level;[40] those notices must be in plain language and prominently displayed.[41] Agencies are similarly required to provide meaningful explanations of their ADS-informed decisions to affected individuals.[42] In addition, for ADS with Impact Levels of III or IV, agencies must "publish documentation on relevant websites about how the [ADS] works, in plain language.

Bias

The Canada ADM Directive does not explicitly require AI or ADM systems to comply with the *Charter* or Canadian human rights legislation. Rather, the Directive states that its objective is to:

> *…ensure that Automated Decision Systems are deployed in a manner that reduces risks to Canadians and federal institutions, and leads to more efficient, accurate, consistent, and interpretable decisions made pursuant to Canadian Law.*[43]

By way of contrast, the Canada ADM Directive is explicit about the requirement to comply with "administrative law principles."[44] The Directive further states that its expected results are that

> *Decisions made by federal government departments are data-driven, responsible, and complies with procedural fairness and due process requirements.*[45]

The Canada ADM Directive also explicitly requires the developers of all federal AI systems to consult with government legal services to ensure the use of the ADM comply with "applicable" laws.[46]

Due Process and Procedural Fairness

The Canada ADM Directive explicitly states that an objective of Directive is that "[d]ecisions made by federal government departments are data-driven, responsible, and compl[y] with procedural fairness and due process requirements."[47] For example, the Directive states that a government department using an ADM system must

- Provide "notice on relevant websites that the decision rendered will be undertaken made in whole or in part by an Automated Decision System."[48]
- Provide "a meaningful explanation to affected individuals of how and why the decision was made."[49]
- Provide "clients with any applicable recourse options that are available to them to challenge the administrative decision."[50]

The Directive further notes that

> *Procedural fairness is a guiding principle of government and quasi-government decision-making. The degree of procedural fairness that the law requires for any given decision-making process increases or decreases with the significance of that decision and its impact on rights and interests.*[51]

The administrative law-orientation of the Directive is confirmed in the AIA, which includes questions such as

- Will the audit trail identify the authority or delegated authority identified in legislation?
- Will the system provide an audit trail that records all the recommendations or decisions made by a system?
- Will the audit trail show who the authorized decision maker is?
- Will the system be able to produce reasons for its decisions or recommendations when required?

- Will there be a recourse process planned or established for clients that wish to challenge the system?
- Will the system enable human override of system decisions?[52]

Oversight and Enforcement

The Canada ADM Directive permits external, independent review, but does not require it. Rather, the Directive requires "peer review" for systems determined to be Levels II to IV on its impact assessment scale. The extent of the peer review depends upon the identified risk of the system. An ADM system with a "moderate" impact (Level II) must be peer reviewed by at least one expert. Systems with a potentially "very high impact" (Level IV) must include at least two experts. Independent review is possible, but not guaranteed as the Directive states that experts can include "specialists internal to government," academics, representatives from an NGO, from a "third-party vendor", or an expert from an advisory board established by the federal Treasury Board.

The Directive also requires the monitoring of outcomes of ADS for decisions for all systems, irrespective of the level of impact, "on an ongoing basis to safeguard against unintentional outcomes".

The European Commission AI Regulation Proposal

History

The European Commission has already invested in research and innovation and created a Digital Single Market.[53] For instance, the GDPR (General Data Protection Regulation) has been enacted in this context.[54] The European Commission presented new AI binding rules on April 21st, 2021.[55] The new Coordinated Plan with Member states[56] seeks to strengthen AI uptake, investment and innovation across the EU. The new rules on Machinery[57] will complement this approach by adapting safety rules of robotic products integrating AI. While the AI Regulation will address the safety risks of AI systems, the new Machinery Regulation will ensure the safe integration of the AI system into the overall machinery.

The first step was the publication of the European AI strategy in 2018 under the former European Commission chaired by Jüncker. The High-Level Expert Group on Artificial Intelligence developed guidelines for trustworthy AI in 2019, and an assessment list for trustworthy AI in 2020. These guidelines only contained ethical principles, but the Expert Group was already calling for the development of a legal framework.

Then, under the new presidency of Ursula von der Leyen, the European Commission continued its work by publishing a White Paper in February 2020 in which it set out its vision for "AI in Europe: an ecosystem of excellence and trust", announcing the rules published in April 2021. Three years have therefore passed between the publication of the Strategy and the proposed regulation.

A public consultation on the AI White Paper was initiated between February and June 2020 to invite citizens and stakeholders to provide input on the next policy and regulatory steps for artificial intelligence.

The final report was published in November 2020 and indicates that the consultation received broad participation from around the world. It attracted 1,250 contributions through an online survey. 84% of the contributions came from the EU Member States. Other responses came mainly from the UK, US, Switzerland, Norway, Japan, India, Turkey, and China. Four hundred and fifty position papers were also submitted during the consultation. Additional stakeholder workshops and events were organized.

Status

A regulation is the binding model that leaves the least flexibility to the Member States. Directives lay down certain results that must be achieved but each Member State is free to decide how to transpose directives into national laws (binding but indirect effect). On the contrary, regulations have binding legal force inside every Member State and enter into force on a set date in all the Member States without the need to translate the regulation into national law. A single norm therefore applies in principle to the entire European Union when the choice of a regulation is made (direct and binding effect).

Regarding the legislative process, the European Commission regulation on AI is still a proposal which needs to be approved in the same words by the Council of the European Union and European Parliament to become law.[58] Given that European law is constructed in a co-legislative process involving three institutions (the European Parliament, the Council of the EU, and the European Commision), they must agree on a common version of the proposal. It is possible that a trialogue will be necessary with representatives from the three institutions discussing the wording of the text. Article 85(1) of the Proposal states that: "This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*. Article 85(2) of the Proposal adds that: "This Regulation shall apply from [24 months following the entering into force of the Regulation].

Legal Basis

It is also important to mention the legal basis of the EC proposal for a regulation. The main legal basis of the text is article 114 (internal market) of the Treaty on the Functioning of the European Union (TFEU), which corresponds perfectly to the objective of the proposal which is to harmonize rules for the placing on the market, the putting into service and the use of artificial intelligence systems in the Union (art. 1(1) of the EC proposal). This implies that the main objective of the proposal is to encourage the market of AI systems. However, a second legal basis has been added. Article 16 of the TFEU covers the protection of personal data and is justified by the measures on facial recognition for law enforcement purposes (article 5 of the EC proposal). The objective is therefore not only commercial, but also to limit the risks on health, safety and fundamental rights. Nevertheless, the proposed regulation is mostly centered around the placing on the market of AI systems.

Purpose and Objectives

The Commission puts forward the proposed regulatory framework on Artificial Intelligence with the following specific objectives:

- ensure that AI systems placed and used on the Union market are safe and respect existing law on fundamental rights and Union values;
- ensure legal certainty to facilitate investment and innovation in AI;
- enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- facilitate the development of a single market for lawful, safe, and trustworthy AI applications and prevent market fragmentation.

The new rules will be applied directly in the same way across all Member States. They follow a risk-based approach.

According to article 1 of the EC Proposal (Subject matter), this Regulation lays down: (a) harmonized rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union; (b) prohibitions of certain artificial intelligence practices; (c) specific requirements for high-risk AI systems and obligations for operators of such systems; (d) harmonized transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorization systems, and AI systems used to generate or manipulate image, audio or video content; (e) rules on market monitoring and surveillance.

The main objective is to organize the AI market and to establish pre-market obligations. It is not a question of laying down ethical principles or recognizing the rights of the people to whom the AI systems will be applied. Obligations on the suppliers of AI systems who put them on the market will therefore be created. 'Placing on the market' means the first making available of an AI system on the Union market (art. 3(9)).

Material Scope

The EC Proposal is a comprehensive regulation (*omnibus*), including private sector and public sector (EU public authorities and bodies as well as national public authorities and bodies). This comprehensive approach is a transversal (horizontal) approach and not limited by activity sector or AI method. The material scope is based on the impact of AI systems and to frame the possible risks for fundamental rights, health or safety of people regardless of technologies, methods or application sectors.

However, this regulation is not applicable to AI systems developed or used exclusively for military purposes (art. 2(3)). This can be explained by the fact that military matters are not the competence of the Union but of the Member States (cooperation in defense matters). This regulation is not applicable either to public authorities in a third country nor to international organizations (art. 2(4)), where those authorities or organizations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States. This exclusion is justified by the respect of the sovereignty of other States or the independence of international organizations.

Some sectorial rules have also been enacted within the EC Proposal, regarding credit institutions, immigration, or law enforcement purposes for instance. Moreover, the EC proposal does not apply directly to high-risk AI systems that are products or systems (or their safety components) falling within the scope of the acts which are listed in the Annex II (article 2(2)) because these are regulated by other EU regulations and directives which will incorporate the content of the new Commission proposal. Annex II is a list of Union harmonization legislation based on the New Legislative Framework (NLF) (toys, medical devices…), including the Directive 2006/42/EC on "machinery" which is also reformed by the New Proposal Regulation (section A). Annex II, Section B, lists other Union harmonization legislation mostly related to the transport sector. In all these cases, only Article 84 of the EC Proposal on Evaluation and Review shall apply.

Consequently, the AI Regulation will be integrated into existing sectoral safety legislation to avoid over-regulation. Articles 75 to 81 enact provisions on amendments of the Acts listed in the section B, Annex II. The proposed regulation is a first reform of other reforms that will come. Finally, the proposed regulation can be seen as combining a comprehensive approach with a sectoral approach.

Definitions

As this Regulation lays down harmonized rules for the placing on the market, the putting into service and the use of artificial intelligence systems ("AI systems") in the Union, the first point is to define "AI systems".

Article 3 paragraph 1 defines an "artificial intelligence system" as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."

Annex I

a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

c) Statistical approaches, Bayesian estimation, search and optimization methods.

Technological neutrality

The material scope is particularly broad. This definition accurately apprehends artificial intelligences by materializing the plurality of possible methods. Both machine learning and expert or statistical systems are concerned, which covers a very broad technological spectrum, more or less complex and mastered by designers and developers. It is also irrelevant whether the learning is supervised, unsupervised or reinforcement based. Obviously, the European legislator did not want to go into the details of the technique and respect the principle of technological neutrality.

Such an approach is to be welcomed as it will avoid the need for users of these technologies, and the people to whom they will be applied to, to have to research the type of technique used, at the risk of being excluded. Moreover, while machine learning and, within it, deep learning are currently "fashionable", other methods may become more prevalent in the future.

The results produced by a simple expert or statistical system are in principle easier to explain than those of machine learning. But the fact remains that these systems can have a discriminating effect on certain categories of populations, because of age, race, gender, or ability criteria. Seemingly simpler systems are therefore not inherently less socially dangerous. Finally, public administrations more often use expert or statistical systems, and it would have been harmful to exclude them from compliance with these standards.

The definition of AI set forth by the proposal is also broad in the objectives pursued by systems that can be programmed to create predictions and recommendations, to make decisions or assist in the process, but also to generate outputs such as content. This fourth objective is not systematically considered in ethical charters or studies on AI and the Commission shows its willingness to integrate the risks generated by the manipulation of "deep fakes" type content. It proves that the goal is to address individual risks of manipulation, as well as social risks for democracy.

Territorial Scope

The territorial scope is very broad and "in light of their digital nature, certain AI systems should fall within the scope of this Regulation even when they are neither placed on the market, nor put into service, nor used in the Union" (recital 11). According to article 2(1), the EC proposal applies to:
(a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country; (b) users of AI systems located within the Union; (c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union.

This last criterion of territorial application must allow to "prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union" (recital 11).

Consequently, Canadian AI companies would be subject to the rules if they sold AI products into Europe or if the output produced by their system were used in the Union.

What Activities and Agencies Does It Apply To?

The EC Proposal is a comprehensive regulation (*omnibus*), including both the public and private sectors (EU public authorities and bodies as well as national public authorities and bodies).

The question of which activities and agencies the text applies to is tantamount to asking who will be made responsible for the obligations imposed by the proposed regulation. The liability mechanism is set out in Articles 24 to 29 and concern all kind of activities (private and public sector) depending on the risks.

The ***provider*** is the main liable party. It designates "a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge" (article 3(2)). It could be a micro or a small enterprise.

The ***user*** means "any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity" (article 3(4)).

The ***importer*** means "any natural or legal person established in the Union that places on the market or puts into service an AI system that bears the name or trademark of a natural or legal person established outside the Union" (article 3(6)).

The ***distributor*** means "any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market without affecting its properties" (art. 3(7)).

All of them are designated as "***operators***" (article 3(8)), including the "***authorized representative***" who is "any natural or legal person established in the Union who has received a written mandate from a provider of an AI system to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation" (article 3(5)).

By principle, the ***provider*** is the main liable (article 16). In particular, if the provider places a "high risk" AI system on the market, he/she has to ensure that the AI systems are compliant with the requirements set out in Chapter 2 of Title III.

However, "where a high-risk AI system related to products to which the legal acts listed in Annex II, section A, apply, is placed on the market or put into service together with the product manufactured in accordance with those legal acts and under the name of the product manufacturer, the ***manufacturer*** of the product shall take the responsibility of the compliance of the AI system with this Regulation and, as far as the AI system is concerned, have the same obligations imposed by the present Regulation on the provider" (article 24). This rule is in accordance with the fact that the AI Regulation will address the safety risks of AI systems and the new Machinery Regulation will complement this approach by adapting safety rules of products and is related to the robotics integrating AI. The new Machinery Regulation, and more broadly the New Legislative Framework listed in Annex II, will ensure the safe integration of the AI system into the overall machinery. In this case and consequently, the manufacturer is made responsible.

Moreover, article 28(1) states that "any distributor, importer, user or other third-party shall be considered a provider for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances: (a) they place on the market or put into service a high-risk AI system under their name or trademark; (b) they modify the intended purpose of a high-risk AI system already placed on the market or put into service; (c) they make a substantial modification to the high-risk AI system."

If these circumstances occur, the provider that initially placed the high-risk AI system on the market or put it into service shall no longer be considered a provider for the purposes of this Regulation" (Article 28(2)). Consequently, they are no longer available.

Limitations and Exclusions

Regarding the exclusions, the Proposal shall not apply to AI systems developed or used exclusively for military purposes (article 2(3)) or to public authorities in a third country nor to international organizations, where those authorities or organizations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States (article 2(4)).

Several limitations apply. For instance, there are specific rules about the activities "carried out by law enforcement authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" (article 3(41)). First, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of *law enforcement* is prohibited, except for three objectives set out in the law. Second, the provider who brings an AI system to market for law enforcement purposes cannot choose any notified body (article 43(1)). For the purpose of the conformity assessment procedure (Annex VII), the competent data protection supervisory authorities under Directive (EU) 2016/680, or Regulation 2016/679 or the national competent authorities supervising the activities of the law enforcement, shall act as a notified body (article 63(5)). Third, article 52 imposes transparency obligations on the use of certain AI systems such as chatbots, emotional recognition systems or image manipulation systems. By exception, these obligations shall not apply to AI systems authorized by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.

Form of Regulation

The EC proposal for a regulation is a form of accountability. It is the provider's responsibility to comply with the requirements of Chapter 2 of Title III when placing high-risk AI system on the market and to prove compliance. This can be done by conformity self-assessment procedure based on internal control (annex VI) or by conformity based on external auditing (annex VII).

Regarding the conformity assessment, for high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has applied harmonized standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall follow one of the following procedures: (a) the conformity assessment procedure based on internal control referred to in Annex VI; (b) the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation (article 11 and annex IV), with the involvement of a notified body, referred to in Annex VII (article 43(1)).

Besides, this proposal is a combination of an *ex-ante* risk self-assessment and an *ex-post* for high-risk AI system. Most of the obligations must be fulfilled before placing the system on the market *ex-ante* or pre-market obligations. Title VIII states some ex-post or post-market obligations for monitoring (article 61), information sharing on incidents and malfunctioning (article 62) and market surveillance (article 63).

Finally, this proposal is a combination of hard law and soft law, as several references to harmonized standards (article 40), common specifications (article 41) and codes of conduct (article 69) can be noted. The Commission and the Member States encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems other than high-risk AI systems of the requirements set out in Title III, Chapter 2 on the basis of technical specifications and solutions that are appropriate means of ensuring compliance with such requirements in light of the intended purpose of the systems (art. 69(1)).

Moreover, ethical values such as transparency, human oversight, accuracy, robustness and cybersecurity are embedded in articles 13 to 15.

Risk Assessment

Unacceptable risks and high risks are defined based on a sectorial approach (Annexes II and III). Four categories of risks are identified in the EC Proposal: unacceptable, high, limited, and minimal risks.

Unacceptable Risk (Article 5)

The risks of AI systems are unacceptable when such systems generate a clear threat to the safety, livelihoods, and rights of people. These systems must be banned.

Four categories of AI systems are unacceptable: (1) AI systems or applications that manipulate human behavior to circumvent users' free will (e.g. toys using voice assistance encouraging dangerous behavior of minors); (2) AI system that exploits the vulnerabilities of a specific group of people because of their age or physical or mental disability, in order to manipulate their behavior; (3) the systems that enable "social scoring" by governments; and (4) "real-time" remote biometric identification systems[59] in publicly accessible spaces for the purpose of law enforcement. There are exceptions to this last rule.[60]

Exceptions are defined and regulated, where strictly necessary to search for a missing child, to prevent a specific and imminent terrorist threat, or to detect, locate, identify or prosecute a perpetrator or suspect of a serious criminal offence. In this last case, 32 crimes are listed, including economic crimes, such as fraud and corruption, which ultimately makes the exceptions broader than they appear.

It should be noted that these exceptions are governed by safeguards and conditions. The use of these systems is subject to authorization by a judicial or other independent body and to appropriate limits in time, geographic reach and the data bases searched.

High Risk (Article 6): Annex II and III

An AI system shall be considered high-risk (***Annex II***) where both of the following conditions are fulfilled:

a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonization legislation listed in Annex II;

b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonization legislation listed in Annex II.

AI systems identified as high-risk (***Annex III)*** include AI technology used in:

- Critical infrastructures (e.g. transport), that could put the life and health of citizens at risk;
- Educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
- Safety components of products (e.g. AI application in robot-assisted surgery);
- Employment, workers management, and access to self-employment (e.g. CV-sorting software for recruitment procedures);
- Essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan);
- Law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence);
- Migration, asylum and border control management (e.g. verification of authenticity of travel documents);
- Administration of justice and democratic processes (e.g. applying the law to a concrete set of facts).

High-risk AI systems will be subject to strict obligations before they can be put on the market:

- Adequate risk assessment and mitigation systems: a risk management system shall be established and consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating, in order to mitigate the risks;
- High quality of the datasets feeding the system to minimize risks and discriminatory outcomes: An appropriate data governance shall consider possible bias and the datasets shall be relevant and representative;
- Logging of activity to ensure traceability of results: the AI system has to be designed in a way that automatically records its activity;
- Detailed documentation providing all necessary information on the system and its purpose for authorities to assess its compliance: a technical document shall be drawn up before that system is placed on the market and be kept up-to date.
- Clear and adequate information to the user has to be provided, as well as an appropriate human oversight to minimize risk and a high level of robustness, security and accuracy;
- Appropriate human oversight measures to minimize risk;
- High level of robustness, security and accuracy.

The European Commission considers that the proposed minimum requirements are already state-of-the-art for many diligent operators and the result of two years of preparatory work. These are the main requirements and there are many detailed rules for their implementation.

Limited Risks

Specific transparency obligations apply to certain AI systems such as chatbots. Users should be made aware that they are interacting with a machine so they can make an informed decision to continue or step back.

Article 52(1) of the EC Proposal states that "providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use." This obligation shall not apply to AI systems authorized by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence. Moreover, users of an emotion recognition system or a biometric categorization system shall inform of the operation of the system the natural persons exposed thereto (article 52(2)), as well as users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places, or other entities or events and would falsely appear to a person to be authentic or truthful ("deep fake") (article 52(3)).

Minimal Risks

The legal proposal allows the free use of applications such as AI-enabled video games or spam filters. The vast majority of AI systems fall into this category. The draft Regulation does not intervene here, as these AI systems represent only minimal or no risk for citizens' rights or safety.

Additionally, voluntary codes of conduct (article 69) are proposed for non-high-risk AI, as well as regulatory sandboxes to facilitate responsible innovation.

The Commission and the Member States shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems other than high-risk AI systems of the requirements set out in Title III, Chapter 2 on the basis of technical specifications and solutions that are appropriate means of ensuring compliance with such requirements in light of the intended purpose of the systems (art. 69(1)).

Codes of conduct may be drawn up by individual providers of AI systems or by organizations representing them or by both, including with the involvement of users and any interested stakeholders and their representative organizations. Codes of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems (art. 69(3)).

Disclosure

High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider (article 13(1)).

High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users and listed in article 13(3).

Due Process

Insofar as the purpose of the regulation is to establish conditions prior to the marketing of AIS, the circumstances of contestation and respect for the adversarial process are *de facto* limited.

One can only note the possibility of an appeal against decisions of notified bodies that the Member States shall ensure to parties having a legitimate interest in case of external procedure of conformity (article 45).

Oversight

For ensuring an external control based on a certification system, each Member State shall designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring (article 30). Notified bodies shall verify the conformity of high-risk AI system in accordance with the conformity assessment procedures (article 33).

The oversight is guaranteed by national and European authorities. National market surveillance authorities (article 63), including National Competent Authorities designated by each Member State, ensure the application and implementation of the Regulation (article 59). Moreover, the European Artificial Intelligence Board (articles 56 to 58) will contribute to the effective cooperation of the national supervisory authorities.

Amendment: Adaptability and Updating

The proposal empowers the Commission, by delegated acts, to adopt implementing acts to ensure uniform application of the regulation as well as to update or complement the lists in Annexes I to VII (article 73).

Moreover, the Commission shall organize an annual review and assess the need for amendment of the list in Annex III once a year following the entry into force of this Regulation (article 84(1)).

By three years after the date of application of the Regulation referred to in Article 85(2) and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public (article 84(2)).

A Deeper Look: Comparing and Contrasting the Canada ADM Directive and EC Proposal

Regulation in the Canadian Federal State vs the EU and its Member States

As noted above, the Canada ADM Directive only governs a limited range of ADM systems deployed by the Canadian federal government and federal agencies. Nor does the Directive govern private sector AI, ADM or related technologies. As a result, the development and deployment of AI and ADM by governments, public institutions and private sector actors is currently beyond the reach of the federal Directive. In a federal system like Canada, these exceptions would include provincial governments, municipalities, school boards, child welfare agencies, police services, universities, hospitals, courts, tribunals, and many others. As a result, many of the most consequential and controversial AI and ADM applications in use today could be deployed by literally hundreds (if not thousands) of public institutions across Canada without any dedicated regulatory framework.

In the European Union, the Commission chaired by Jüncker, adopted a strategy on Digital Single Market (2015-2019),[61] based on article 114 of the Treaty on the Functioning of the European Union (TFEU), which is a sort of an extension of the single market applicable to digital activities. The EU digital policy continues today with the European Commission chaired by Von der Layen who presented its guidelines entitled "Shaping Europe's digital future" for 2020-2024.

Article 4(1) of the TFEU states that "the Union shall share competence with the Member States where the Treaties confer on it a competence which does not relate to the areas referred to in Articles 3 and 6. Although the European Commission does not have exclusive competence in digital matters but only a shared competence with the Member States on areas, such as "internal market" and "consumer protection", the EU Commission has succeeded in imposing the adoption of numerous directives and regulations concerning the digital matter since several years (article 4(2)).[62] One of the main arguments used was to ensure the proper functioning of the internal market, which is a priority of the Union, and to avoid market fragmentation between member states.

Bias

High risk AI systems are those which are considered most likely to have biases adversely affecting vulnerable populations and minorities (article 10(2)). As acknowledged by the E.U. regulation, these biases can be addressed in a variety of technical ways, notably through the examination of the training, testing and validation data, along with appropriate validation methodologies. These biases would include any discrimination based on outcome, such as different results for women and men, or prejudice based on socio-economic status, race, or ethnicity, among others (article 10(3)). The data and algorithms used in these high-risk systems are therefore required to be relevant, representative, free of errors, and complete. How this is specifically interpreted will depend on each case, however the product owner must make a convincing case that biases have been addressed before obtaining certification.

Article 10(5) contains a particularly interesting new provision to help prove discrimination. It provides that: "*to the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679,*[63] Article 10 of Directive

(EU) 2016/680 [64] and Article 10(1) of Regulation (EU) 2018/1725,[65] subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymization, or encryption where anonymization may significantly affect the purpose pursued."

Furthermore, a person or group of persons are required to always oversee the AI system, to ensure that it does not become biased over time. This can happen when learning algorithms receive biased inputs, while in deployment, and have sometimes caused AI systems to have discriminatory effects completely independently of their original intent. The overseers are therefore required to remain aware of this possibility, and to beware of over-relying on the outputs produced by a high-risk AI system ("automation bias"). This is particularly the case in AI systems that are used to provide information or recommendations for decisions that should be made by natural persons. Overseers are also required to have the capacity to intervene in the operation of the system, notably by interrupting the system manually if the results appear biased or discriminatory in any way (article 14).

Risk Management and Impact Assessment

Article 8 of the EC's proposal states that providers who place on the market or put into service high-risk AIS must comply with the requirements established in Title III, chapter 2.

According to the EC Proposal, a risk management system shall be established, implemented, documented, and maintained in relation to high-risk AI systems (article 9). The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise several steps, such as identification and analysis of the known and foreseeable risks associated with each high-risk AI system. The risk management measures shall consider the acknowledged state of the art, including as reflected in relevant harmonized standards or common specifications. Identifying the most appropriate risk management measures supposed to ensure an elimination or reduction of risks as far as possible through adequate design and development.

Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures, and instructions, and shall include at least the aspects listed in article 17, such as a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system.

Moreover, Providers of high-risk AI systems shall comply to other obligations on data governance (article 10), technical documentation (article 11), record-keeping (article 12), transparency (article 13), human oversight (article 14), accuracy, robustness, and cybersecurity (article 15).

Data Governance

The combination of those articles 10 to 15 ensures high risks systems' acceptability and legality, and more specifically, prevent that AI systems based on training models become sources of discrimination, and so contrary to the objectives of the European Union regulation. For example, specific provisions are defined for training, validation, and test data sets (art. 10.3 to 10.5). For example, such sets must consider, to the extent necessary for the intended purpose, the characteristics, or elements specific to the geographical, behavioral, or functional context in which the AI system is intended to be used.

Here, the link with the Data Governance Act of 25 November 2020 (DGA)[66] a text of the European Union's data strategy and with which the AI Act must be connected- should be highlighted. For high-risk AIS to be based on high quality datasets, providers must be able to access sufficient or appropriate datasets for the intended purpose of the AIS and meet the requirements of accuracy and robustness. Thus, the structuring of the UE data market around independent sharing intermediaries facilitates the implementation of the requirements imposed on the deployment of high-risk AIS and helps to contain the risks inherent in them.

It is also important to note that article 10 and seq. drastically change the paradigm of data governance which will have many practical consequences for organizations. From a good practice left to the initiative and discretion of organizations, data governance is now part of a legally binding framework that tracks down discrimination that the lack of robustness of high-risk AIS is likely to generate.

This framework takes shape at two levels. On the one hand, without a well-established data governance, AI systems providers cannot self-declare compliance with the obligations at article 10 et seq. and thus benefit from the European marking of high-risk AI systems, a compulsory procedure for their marketing. Secondly, in case of non-compliance with the obligation to implement appropriate data governance practices, the supplier is exposed to highest level administrative sanctions according to article 71.3. Although the procedure for regulating high-risk AIS is intended to be flexible because of the possibility left to the players to regulate themselves, the amount of the sanctions is sufficiently high to encourage suppliers to comply with the provisions of Section 10, even more if the company has an international presence.

By doing so, the Commission not only shows that it is aware of this risk to fundamental rights, but also takes the lead in the legal means to try to counter this risk, where most States, such as Canada, have so far been content with ethical rules. In other words, the legalization of data governance is not only a change in culture and practice, but above all it is a quiet but crucial step towards the realization of a safe, reliable, and legally regulated AI.

Policing and Criminal Justice

AI and automated decision-making systems are used extensively by governments and police services in criminal justice systems around the world. Applications include:

- Photographic and video analysis, including facial recognition;
- DNA profiling and evidence, including predictive genomics;
- Predictive crime mapping (predictive policing);
- Mobile phone and extraction tools;
- Data mining and social media intelligence;
- Bail algorithms that predict likelihood of being arrested or failure to appear at a bail hearing;
- Sentencing algorithms that predict likelihood of being arrested;
- "Scoring at arrest" algorithms that advise how to charge an individual;
- "Scoring suspects" algorithms that analyze an individual's behaviour in the future;
- "Scoring victims" algorithms that predict likelihood of being a victim of crime; and,
- Correctional algorithms that predict likelihood of offending within an institution.

The LCO's *The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada* report discusses the risks of AI and automated decision-making systems in the criminal justice system at length. These risks include, but are not limited to: *Charter* violations, biased data, the "metrics of fairness", data transparency and opacity, "data scoring", algorithmic bias, lack of due process, and a lack of access to justice.[67]

In the United States, there has been an extraordinary backlash to the use of AI and related tools in American criminal justice. Importantly, American systems were invariably introduced *before* comprehensive regulation.[68]

Articles 6 and 7 and Annex III of the European Commission's proposed AI rules crystalize an emerging international standard of prohibited and high-risk AI systems, including facial recognition systems and systems used by law enforcement and systems used in the administration of justice and democratic processes. Annex III pre-emptively identifies the following types of systems as high-risk:

1. *Biometric identification and categorisation of natural persons:*
   - a) *AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;*

2. *Law enforcement:*
   - a) *AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;*
   - b) *AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;*
   - c) *AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);*
   - e) *AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;*
   - f) *AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing* personality traits and characteristics or past criminal behaviour of *natural persons or groups;*
   - g) *AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;*
   - h) *AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.*

3. *Administration of justice and democratic processes:*
   - a) *AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.*

In contrast to the EC proposed rules, there is a major gap in regulation of AI and automated decision-making technologies in policing and the criminal justice system:

- The Directive's focus on "administrative decisions" suggests that the Directive may not apply to ADM systems that could be deployed in the criminal justice system or criminal proceedings. As a result, it appears the federal government could adopt predictive policing algorithms, facial recognition technology, and/or automated risk assessments in bail and sentencing proceedings without having to comply with the Directive.[69]
- The Canada ADM Directive does not pre-emptively identify or prohibit the use of facial recognition technologies, nor it include detailed provisions identifying AI systems in "law enforcement" and the "administration of justice" as being pre-emptively high-risk, and thus subject to more detailed and expansive regulatory requirements.
- Most importantly, the Canada ADM Directive does not govern the use of AI or automated decision-making technologies in policing or the administration of justice that may be deployed by governments and public institutions far beyond the reach of the Canada ADM Directive, including provincial governments and police services. This means that the most consequential and controversial AI and ADM applications in use today could be deployed by literally hundreds (if not thousands) of public institutions across Canada without any dedicated regulatory framework.

Enforcement

The Canada ADM Directive does not include a dedicated enforcement or remedies provisions. Nor does the Directive establish fines or any administrative sanctions if the Directive is breached. In contrast, the Directive establishes a requirement that that the Assistant Deputy Minister responsible for a program using an ADM system is responsible for:

> *6.4.1 Providing clients with any applicable recourse options that are available to them to challenge the administrative decision.*

This commitment, while explicit, is not very specific. More importantly, while the Canada ADM Directive may acknowledge the need for remedies, the Directive does not actually *create* a legal right to a remedy. Professor Scassa notes that

> *While directives are important policy documents within the federal government, and while there are accountability frameworks to ensure compliance, the requirements to comply with directives are internal to government, as are the sanctions. Directives do not create actionable rights for individuals or organizations.*[70]

By way of contrast, the EC's proposal provides three levels of sanctions (Article 71):

1. In case of non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5 or non-compliance of the AI system with the requirements laid down in Article 10, the infringements shall be subject to administrative fines of up to 30 000 000 EUR or, if the offender is company, up to 6 % of its total worldwide annual turnover for the preceding fiscal year, whichever is higher:
2. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5 and 10, shall be subject to administrative fines of up to 20 000 000 EUR or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding fiscal year, whichever is higher.

3. The supply of incorrect, incomplete, or misleading information to notified bodies and national competent authorities in reply to a request shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is a company, up to 2% of its total worldwide annual turnover for the preceding fiscal year, whichever is higher.

Following a logic comparable to the one implemented with the GDPR, the European Commission sets out particularly strong sanctions in case of violation of the provisions. They are even higher than in the GDPR, which should encourage actors to respect the regulation. The high level of sanctions is intended to draw the attention of providers, even though AIS can generate significant and even unacceptable social risks. It also serves to hold accountable those actors who would choose to conduct internal monitoring of the requirements. The logic of self-compliance is accompanied by high penalties, taking the example of the regulation's approach more frequently used in the US.

National market surveillance authorities (article 63), including National Competent Authorities designated by each Member State, ensure the application and implementation of the Regulation (article 59). These authorities will be competent to apply the sanctions and will ensure the enforcement of the law.

Due Process and Procedural Fairness

The Canada ADM Directive explicitly states that an objective of Directive is that "[d]ecisions made by federal government departments are data-driven, responsible, and compl[y] with procedural fairness and due process requirements."[71] Professor Scassa notes that "…[the Directive] and AIA are, in fact, built upon norms for administrative decision-making that have their roots in common law principles of procedural fairness."[72] For example, the Directive states that a government department using an ADM system must

- Provide "notice on relevant websites that the decision rendered will be undertaken made in whole or in part by an Automated Decision System."[73]
- Provide "a meaningful explanation to affected individuals of how and why the decision was made."[74]
- Provide "clients with any applicable recourse options that are available to them to challenge the administrative decision."[75]

The Directive further notes that

> *Procedural fairness is a guiding principle of government and quasi-government decision-making. The degree of procedural fairness that the law requires for any given decision-making process increases or decreases with the significance of that decision and its impact on rights and interests.*[76]

The administrative law-orientation of the Directive is confirmed in the AIA, which includes questions such as:

- Will the audit trail identify the authority or delegated authority identified in legislation?
- Will the system provide an audit trail that records all the recommendations or decisions made by a system?
- Will the audit trail show who the authorized decision maker is?
- Will the system be able to produce reasons for its decisions or recommendations when required?

- Will there be a recourse process planned or established for clients that wish to challenge the system?
- Will the system enable human override of system decisions?[77]

Professors Scassa and Raso have both analyzed the Directive against Canadian administrative law principles and requirements, including the requirements for fairness, notice and disclosure, hearing and reasons.[78] Professor Scassa notes, for example, that "the [Directive] is an intriguing example of "procedural fairness by design" and that

> *A major contribution of the [Directive] and the AIA tool is their attempt to embed principles of fairness, transparency and accountability up front in system design – rather than relying upon judicial review to correct the problems with specific outcomes."*[79]

As far as the purpose of the EC's regulation is to establish conditions prior to the marketing of AIS, the circumstances of contestation and respect for the adversarial process are *de facto* limited. One can only note the possibility of an appeal against decisions of notified bodies that the Member States shall ensure to parties having a legitimate interest in case of external procedure of conformity (Article 45).

Consumer Protection

The main purpose of the EC's proposal of regulation is to lay down rules before AI systems are placed on the market and is not consumer oriented. Besides it should be noted that the EU has adopted several other regulations, not only aimed at protecting personal data (GDPR) but also at protecting consumers in an "omnibus" perspective (directive (EU) 2019/2161)[80] and more specifically on sales of good (directive (EU) 2019/771) [81] and digital services (directive (EU) 2019/770).[82] It is therefore appropriate to refer to these specific texts which concern consumer protection in a digital context and with which the proposed regulation will have to be articulated.

It should also be added that on December 15, 2020, the European Commission published two other texts intended to regulate the digital sector, both from the point of view of the digital market (Digital Market Act) and from the point of view of digital services and the responsibility of the major platforms known as "gatekeepers" (Digital Services Act). These texts will also indirectly protect consumers in the digital environment.

From a jurisdictional point of view, there is a major difference between Canada and the European Union. While consumer law is the jurisdiction of the provinces in Canada, the European Union has a shared competence with the Member States in the "consumer protection" area (Article 4f of the TFEU). The European Commission can thus implement a consumer law policy on the basis of article 169 of the TFEU. The specificity of European consumer law is in the fact that it pursues consumer protection objectives while at the same time being part of the more general perspective of Union law, which makes the proper functioning of the internal market a priority.

Comparing Models: Strengths and Weaknesses

The Canada ADM Directive

The Directive's first and perhaps most notable strength is its comprehensiveness. The Directive includes many (but not all) of the necessary elements of comprehensive "framework" regulation identified by the LCO and other organizations.[83] The Directive addresses an impressive range of issues, including: baseline requirements for many (likely most) federal government automated decision-making systems, irrespective of risk; strong protections for automated decision-making transparency; a mandatory register; a detailed and thoughtful risk assessment process; elements of a remedial regime; a commitment to procedural fairness; and an oversight regime. The Directive has several weaknesses, as will be discussed below. These weaknesses should not, however, take away from its many strengths.

Some of the Directive's specific strengths include:

- ***Dedicated Focus on Government Automated decision-making.*** Unlike the EC Proposal, the Canada ADM Directive is not a rule or regulation of general application aiming to regulate both government and private sector AI and ADM at the same time. As a result, the Canada ADM Directive addresses the issues and concerns about public sector ADM systems specifically. For example, the Canada ADM Directive is specifically designed to mitigate the risks of algorithmically-assisted government decision-making. Further most Government of Canada ministries and agencies are governed by the Directive. Given the breadth and depth of Government of Canada operations and responsibilities, this is a significant foundation for responsible AI and ADM development with Canada.
- ***Commitment to rights protection.*** The Canada ADM Directive is weighted heavily in favour of rights protection as opposed to promoting AI marketplace development or innovation. This weighing is demonstrated by the Directive's extensive commitments to procedural fairness, comprehensive risk assessment and mandatory disclosure.
- ***Sophisticated Risk-Based Model.*** The Canadian Canada ADM Directive establishes four levels of risk, judged by the impact of an automated decision determined after an Algorithmic Impact Assessment (discussed below). The Directive then establishes requirements for each impact level, including greater or lesser levels of:
  - – Notice before ADM decisions and explanations after ADM decisions
  - – Peer review.
  - – Employee training; and,
  - – Human intervention.[84]

  In this manner, the Canada ADM Directive effectively establishes a sliding-scale of requirements and due diligence depending on the level of risk identified.

  The Algorithmic Impact Assessment (AIA) tool is a similarly sophisticated tool to help federal officials assess and determine the impact of a system.[85]
- ***Explicit commitment/rules to protect procedural fairness.*** The Directive explicitly states that an objective of Directive is that "[d]ecisions made by federal government departments are data-driven, responsible, and compl[y] with procedural fairness and due process requirements."[86] This commitment and Directive's detailed rules are unique.

- ***Commitment to remedies.*** The federal Directive states that the Assistant Deputy Minister responsible for a program using an ADM system is responsible for "*Providing clients with any applicable recourse options that are available to them to challenge the administrative decision*".[87]
- ***Algorithmic Impact Assessment.*** The Directive requires an Algorithmic Impact Assessment for every automated decision-making system within the Directive's scope, including an assessment of "the impact on rights of individuals or communities." The Directive further requires that Algorithmic Impact Assessments be released publicly.[88] The AIA itself is comprehensive, asking persons or organizations considering an ADM system to address approximately 60 questions designed to evaluate the appropriate risk level for a proposed system.[89]
- ***Mandatory disclosure.*** The Canada ADM Directive includes a mandatory disclosure requirement. Government agencies are required to provide notice on websites when decisions will be made by or with the assistance of AI or ADS, regardless of the applicable impact level;[90] those notices must be in plain language and prominently displayed.[91] Agencies are similarly required to provide meaningful explanations of their ADS-informed decisions to affected individuals.[92] In addition, for ADS with Impact Levels of III or IV, agencies must "publish documentation on relevant websites about how the [ADS] works, in plain language. Finally, oonce completed, the AIA is required to be publicly posted on Government of Canada websites or as may be required by the federal Directive on Open Government.

On the other hand, the Canada ADM Directive also has several weaknesses or limitations. Unlike the EC Proposal, the Canada ADM Directive has a very limited scope. The Canada ADM Directive has a singular purpose: regulation of a specific range of federal government automated decision-making systems. This means that other kinds of AI and algorithmic systems are beyond its scope, including:

- ***Significant jurisdictional gaps.*** The Canada ADM Directive is limited to federal government automated decision-making systems. This means that whole areas of government and private sector AI and ADM development are outside the scope of AI governance and thus largely unregulated, including AI and ADM systems used by provincial governments, municipalities, (most) police services, public agencies and the private sector.
- ***Criminal justice.*** The Canada ADM Directive does not include AI or automated decision-making systems in the federal criminal justice system. In contrast, the European Commission Proposal include detailed provisions identifying AI systems in "law enforcement" and the "administration of justice" as being pre-emptively high-risk, and thus subject to more detailed and expansive regulatory requirements.

Additional weaknesses include:

- ***Prohibited and high-risk systems.*** Unlike the European Commission Proposal, the Canada ADM Directive does not explicitly identify prohibited or *a priori* "high-risk" systems subject to greater regulation.
- ***Directive, not legislation.*** The Canada ADM Directive is obviously not legislative. Legislation or formal regulations are necessary to provide the foundational governance framework for these systems. It would also ensure changes to the governance framework were subject to legislative and public review. Finally, legislation would establish a level of public and legal accountability commensurate with the issues and rights at stake.

The EC Proposal

Several strengths of the proposal are discernible.

First, the fact that the European Commission is the first in the world to consider regulation of this scale has the advantage of giving a direction that will be looked at by other states and will necessarily influence them. Moreover, the big AI players like the US, China and Canada cannot do without the European market and cannot refuse to comply with it. This is especially true, while the proposal has extraterritorial effect and applies even if the AIS provider is outside the territory of the European Union, as long as these systems are placed on the EU market or the output produced by the system is used in the Union.

Second, on the content of the proposal, the Commission is positioning itself according to its competence, i.e. its competence shared with the Member States (article 4a) of the TFEU) on the basis of Article 114 of the TFEU (internal market). Therefore, the main purpose of the regulation is to organize the rules for the placing on the market of goods or services incorporating AI and their use. Regulating the market and setting pre-market rules has the advantage of directly and mandatorily influencing the deployment of AI solutions, as the way dangerous products like drugs are marketed. In addition, imposing requirements before the market and not afterwards better protects users and those to whom the AIS will be applied.

Third, a risk-based approach instead of a sectorial approach is certainly a good method, if this approach makes it possible to specifically consider the risks to fundamental rights, health, and safety. It seems more relevant to consider the impact of AIS rather than to assume that one sector of activity is more dangerous than another. However, this statement must be nuanced by the fact that Annexes II and III, which identify AIS at risk, are based on a sectoral approach, targeting sectors such as education, human resources, law enforcement or public services and benefits, for example. This risk-based approach that leads to prohibiting certain uses of AI should be encouraged in principle, even if its content and scope are questionable. It seems essential that States position themselves by indicating the uses of AI that are not socially acceptable.

Fourth, the appropriateness of an "omnibus" approach that integrates the public and private sectors can be questioned. These two sectors may eventually merit different rules in the provision or use of AIS, but it is in any case crucial to require rules in both sectors. However, if we rely on the Canadian example, which distinguishes the two sectors in different areas (personal information, AIS of the federal public administration), we can see that private and public actors are increasingly partnering with each other in the area of digital and data exchange, which makes it difficult or even ineffective to enforce legislation. An "omnibus" approach that is also found in the GDPR facilitates the implementation and the efficiency of the regulation.

Fifth, it can be noted that the European legislator has tried to respond in advance to the criticism that regulation kills innovation by providing rules to encourage it by organizing regulatory sandboxes, as well as measures to support small companies and start-ups.

Sixth, it should also be noted that the European legislator is concerned about the risks of manipulation of opinion and emotions, as well as deep-fake content modifications. These issues are related to the protection of democracy, freedom of opinion but also to the dignity of the person. Even if these risks may seem future, it is fundamental to consider them now.

Seventh, the penalties are strong, and it is essential that they are so that regulation is taken seriously, especially by the already all-powerful digital American and Chinese giants in the AI markets.

On the other hand, several of the weaknesses of the proposal are also apparent.

A first weakness is that the European Commission's goal with this proposal is mainly to provide a framework for the placing of products on the market and not to protect individuals from the social risks that AI can generate. Fundamental rights are thus not very present in the proposal. In particular, the EU Charter of Fundamental Rights is mentioned in the "explanatory memorandum," but it has little place in the text. It appears in recitals 13, 28, 38, 41 and only once in the text itself in article 52 concerning the transparency of certain AIS.

Recital 28 states that: "the extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high-risk." Those rights include the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, and non-discrimination, consumer protection, workers' rights, rights of persons with disabilities, right to an effective remedy and to a fair trial, right of defense and the presumption of innocence, right to good administration. In addition to those rights, it is important to highlight that children have specific rights as enshrined in Article 24 of the EU Charter and in the United Nations Convention on the Rights of the Child (further elaborated in the UNCRC General Comment No. 25 as regards the digital environment), both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being. The fundamental right to a high level of environmental protection enshrined in the Charter and implemented in Union policies should also be considered when assessing the severity of the harm that an AI system can cause, including in relation to the health and safety of persons." The Charter is also applicable to law enforcement activities (recital 38).

These provisions in the recitals are important and interesting. However, it should be remembered that they are not binding, and they only help to interpret the text. The Court of Justice of the EU (CJEU) may rely on the recitals and may wish to give greater prominence to the Charter, as it has often done in digital matters and in the protection of personal data.

A second weakness is the limited scope of AIS that are prohibited because they are considered socially unacceptable. Article 5 foresees only four cases of application although many others would be just as likely to generate significant risks. Moreover, each of the cases is narrowly defined, excluding equally dangerous situations. For example, article 5(1)(c) prohibits the placing on the market, putting into service or use of social rating AISs by public authorities, even though private actors could make use of such AISs. It is difficult to see how this would be less dangerous and reprehensible.

A third weakness can be found in section 5(1)(d), which prohibits the use of 'real-time' remote biometric identification systems (facial recognition) in publicly accessible spaces for the purpose of law enforcement. Not only the circumstances are narrowly defined, but also three exceptions are provided. While the first two are acceptable (targeted search for specific potential victims of crime, including missing children and prevention of a specific, substantial, and imminent threat to the life or physical safety of natural persons or of a terrorist attack), the third opens the possibility of using facial recognition in thirty-two types of crimes, some of which are not directly related to national security and are more questionable, such as the economic crime of fraud.

A fourth weakness is that the high-risk AISs are listed restrictively in Appendices II and III. Listing them locks in the assumptions, especially since Annex III lists eight areas and defines the cases covered in each of them. For example, in the field of "education and vocational training," only two situations have been considered: (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions; (b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions. High-risk AIS are therefore narrowly defined. However, it should be noted that the European Commission will be empowered to adopt delegated acts (Article 73) to update the list in Annex III by adding high-risk AI systems within these eight areas, but also by adding new areas for AIS equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III (Article 7).

A fifth weakness is that the goal of the proposed regulation is to frame the requirements for putting AIS on the market and provides for minimum post-marketing obligations, such as a post-market monitoring and sharing of information on incidents and malfunctioning. However, these incidents have the potential to cause harm to the people to whom the AIS applies, and the proposed regulation does not provide liability rules in their favor. While it is understood that this is not the goal of the proposal, it would have been important to refer to liability rules as the Council Directive 85/374/EEC concerning liability for defective products,[93] which may apply but should nevertheless be amended.

A sixth weakness is that the governance rules are extremely complex. For example, "notifying bodies" will have to be set up to certify the AIS. In addition, "national supervisory authorities", national "market surveillance authorities" and a European AI board must cooperate and most of them are still to be created. It will take time and resources before the system functions properly.

A seventh weakness is that the current proposal is reactive rather than proactive or futureproof. The commission seems to have defined as high risks systems whose harm have already been documented at length in the past few years. However, there are many potential systems that could be high risk from their designs (e.g., misaligned AI, disloyal AI, general AI...) and given the current framing of the law, it is likely that they would only be added to Annex III once incidents have already occurred.

Finally, the Regulation will not be in effect soon. It shall only apply 24 months following the entering into force, the twentieth day following that of its publication in the *Official Journal of the European Union*.

Final Thoughts and Questions

The LCO and the Research Chair on Accountable Artificial Intelligence in a Global Context prepared this analysis in order to address the following questions:

- How does the EC Proposal compare to the Canada ADM Directive?
- What are the strengths and weaknesses of each approach?
- What lessons can Canadian policymakers learn from the EC approach?

As demonstrated above, the Canada ADM Directive and EC Proposal are both innovative and complex regulatory instruments. Both approaches represent sophisticated and thoughtful responses to the challenge of AI and ADM regulation in their respective jurisdictions. Some may believe that the scope and breadth of the EC Proposal, coupled with the jurisdictional complexity of EU governance, makes the EC Proposal too complex and unfamiliar to be of benefit to Canadian policymakers and stakeholders.

The LCO and Research Chair on Accountable Artificial Intelligence acknowledge these concerns, but believe this analysis provides some general lessons about best practices and priorities in AI regulation, including:

- ***AI Innovation Depends on Regulation and "Trustworthy AI."*** Governments in Canada and Europe have concluded that proactive regulation is necessary to support AI innovation, economic development, better public services, fairness, and the public legitimacy of AI systems.
- ***Governance Through Regulation, Not Ethical Directives.*** It is notable that both the Canadian government and European Commission have concluded that legal regulations or binding government directives are necessary to govern the use of AI. Both organizations have concluded, rightly in our view, that "ethical AI" guidelines or best practices are insufficient to addresses the proven risks and harms of this technology.
- ***There Are Baseline Elements to Thoughtful AI Regulation.*** Despite their differences, both the Canada ADM Directive and the EC Proposal address many of the same issues, including:
  - Mandatory disclosure of AI use and risks;
  - Explicit identification of risk assessment criteria and harm mitigation strategies;
  - Commitment to impact assessments;
  - Public identification, if not outright prohibition, of high-risk AI systems;
  - Acknowledgement of bias and need for bias mitigation;
  - Commitment to remedies; and,
  - Commitment to external oversight.

  To be clear, neither the LCO nor Research Chair on Accountable Artificial Intelligence believe that the Canada ADM Directive or EC Proposal represents the perfect solution to these issues. Nevertheless, we believe these topics are the baseline element of thoughtful AI regulation and represent an emerging standard for other Canadian governments and agencies.

- ***The EC Proposal Demonstrates Major Gaps in the Regulation of Unacceptable and High-Risk AI Systems in Canada.*** Though imperfect, the EC Proposal includes a commitment to publicly identify, regulate and in some cases prohibit a broad range of high-risk AI systems. Article 5 of the EC Proposal identifies several categories of AI systems that are deemed "unacceptable" and prohibited, including a limited class of biometric identification systems. Similarly, Annex III of the EC Proposal preemptively identifies a class of "high-risk" systems automatically subject to higher regulatory standards. "High-risk" systems include many systems used in law enforcement and the administration of justice, among others.

  In this respect, the EC Proposal represents a major advancement on Canada ADM Directive. As noted above, the Canada ADM Directive does not explicitly identify or prohibit AI systems with unacceptably high risk, including biometric systems such as facial recognition. Nor does the Canada ADM Directive regulate law enforcement or criminal justice AI applications. These are major gaps in AI regulation in Canada that must be addressed urgently

- ***Public and Private Sector AI Regulation Must Be Different.*** As noted above, the Canada ADM Directive and EC Proposal have much different focusses and priorities: The Canada ADM Directive is directed to ADM systems used by the Government of Canada. The EC Proposal, on the other hand, is largely designed to address AI systems used in the private sector within the European Union.

  To its credit, the Canada ADM Directive is designed specifically to address exclusively governmental legal issues and priorities, including administrative law priorities and public interest considerations not applicable in the private sector.

  The EC Proposal demonstrates that the reverse is true also: Private sector AI regulation raises dedicated issues and priorities that should be addressed in a dedicated framework. To state an obvious example, many of the issues and questions raised in the Government of Canada's Algorithmic Impact Assessment are simply not applicable to the private sector. The EC Proposal demonstrated the need to regulate AI systems in the private sector (both their placing on the market and their use). Although it introduces constraints for private actors, it gives them more precision on the applicable rules, and is necessary for trust and social acceptability toward AI, which the public often mistrusts.

- ***A new GDPR?*** It is worth asking if the EC Proposal represents a new General Data Protection Regulation i.e. a new international standard or norm that heavily influences AI regulation in North America. The LCO and Research Chair on Accountable Artificial Intelligence are doubtful this will be the case, at least for AI regulation in Canada. The law is a question of culture, context, and political will. Canada may be sensitive to the influence of Europe, but also of the United States and one may think that Canada will not want to go as far or will want to do it differently.

  In any case, the European Commission is the first legislator to publish a legal framework of this ambition and will necessarily influence other legislators around the world, whether to move towards or away from the topics addressed and the type of rule adopted. The normative choice of the European Commission to go beyond current law, as well as simple ethical principles of AI non-mandatory is obviously a very strong political positioning on the international scene.

Until now, the human-centered ethical principles (Montreal and Toronto Declarations) and the non-mandatory and sectorial norms (Treasury Board directive on automated decisions) have been preferred in Canada.

However, as Canada has invested heavily in AI and continues to do so within CIFAR and the AI pan-Canadian Strategy,[94] it is undoubtedly time to secure the stakeholders by setting clear and legal rules and creating a real responsibility of the chain of actors, as evoked by the Digital Charter.[95] Moreover, Canada is very active on the international AI scene such as the GPAI – which was launched in June 2020 as the fruition of an idea developed within the G7, under the Canadian and French presidencies.[96] Built around a shared commitment to the OECD Recommendation on Artificial Intelligence,[97] GPAI brings together engaged minds and expertise from science, industry, civil society, governments, international organizations and academia to foster international cooperation.[98]

Canada is a strong place of AI in terms of research, public and private investments, and training. Now is the time to secure these efforts by adopting legal standards. Canada will then be able to consolidate its place on the international scene and remain a key player.

More Information and How to Get Involved

The LCO believes that successful law reform depends on broad and accessible consultations with individuals, communities and organizations across Ontario. As a result, the LCO is seeking comments and advice on this report and our recommendations. There are many ways to get involved:

- Learn about the project on our project website;
- Contact us to ask about the project; or,
- Provide written submissions or comments.

The LCO can be contacted at:

Law Commission of Ontario
Osgoode Hall Law School, York University
2032 Ignat Kaneff Building
4700 Keele Street
Toronto, Ontario, Canada
M3J 1P3

Telephone:	**(416) 650-8406**
Toll-free:	**(866) 950-8406**
Email:	**LawCommission@lco-cdo.org**
Web:	**www.lco-cdo.org**
Twitter:	**@LCO_CDO**

ENDNOTES

1 Law Commission of Ontario, *Regulating AI: Critical Issues and Choices*, (2021) [Regulating AI], online: **https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/regulating-ai-critical-issues-and-choices/**.

2 European Commission, *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*, (2021), [EC AI Proposal], online: **https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206**.

3 See, for example, the LCO's *Regulating AI* report, cited above.

4 **https://chaireia.openum.ca**.

5 **www.lco-cdo.org**.

6 Canada – A leader in Artificial Intelligence, Invest In Canada, Gouvernement du Canada, online: **https://www.international.gc.ca/investors-investisseurs/assets/pdfs/download/Niche_Sector-AI.pdf**.

7 Montreal Declaration Responsible AI, online: **https://www.declarationmontreal-iaresponsable.com**.

8 The Toronto Declaration, Protecting the right to equality and non-discrimination in machine learning systems, online: **https://www.torontodeclaration.org/declaration-text/english/**.

9 A Europe fit for the digital age, Empowering people with a new generation of technologies, online: **https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en**.

10 Ethics guidelines for trustworthy AI, online: **https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai**.

11 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 (COM/2021/206 finalEurope fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, online: **https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682**.

12 See C. Castets-Renard, "AI and the Law in the European Union and the United States" in Artificial Intelligence and the Law in Canada, eds. Teressa Scassa and Florian Martin-Bariteau, (Lexis-Nexis Canada) (2021).

13 Aiming for truth, fairness, and equity in your company's use of AI, April 19, 2021, online: **https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai**.

14 Canada, *Directive on Automated Decision-Making*, (2019) [Canada ADM Directive], online: **https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592#appA**.

15 Consultation: Ontario's Trustworthy Artificial Intelligence (AI) Framework, online: **https://www.ontario.ca/page/ontarios-trustworthy-artificial-intelligence-ai-framework-consultations#section-1**.

16 *Responsible use of artificial intelligence (AI): Exploring the future of responsible AI in government*, September 9, 2019, [Canada AI White Paper], online: *Government of Canada* **https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai.html#toc2**.

17 Canada ADM Directive.

18 Canada AI White Paper.

19 Canada ADM Directive, s. 6.1.

20 *Ibid*, s. 6.2.

21 *Ibid*, s. 6.3.

22 *Ibid*, s. 6.4.

23 *Ibid*, s. 6.5.

24 *Ibid*, s. 1.1 and 1.2.

25 Teresa Scassa, *Administrative Law and the Governance of Automated Decision-Making: A Critical Look at Canada's Directive on Automated*

Decision-Making (October 30, 2020). Forthcoming, (2021) 54:1 University of British Columbia Law Review [Scassa], online: **https://ssrn.com/abstract=3722192** at 6-7.

26 Canada ADM Directive, s. 5.4.

27 *Ibid*, s. 9.1.1.

28 *Ibid*, s. 9.2.

29 *Ibid*, s. 5.1.

30 *Ibid*, s. 5.3.

31 Scassa at 11.

32 Canada ADM Directive, s. 6.

33 Canada, *Algorithmic Impact Assessment*, (2019) [Canada Algorithmic Impact Assessment], online: **https://www.canada.ca/en/government/system/d igital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html**. Canada Algorithmic Impact Assessment.

34 Canada ADM Directive, *s. 6.*

35 *Ibid*, s. 6.3.1.

36 *Ibid*, s. 6.3.2.

37 *Ibid*, s. 6.4.

38 *Ibid*, s. 6.1.

39 Canada Algorithmic Impact Assessment.

40 Canada ADM Directive, s 6.2.1.

41 *Ibid*, s. 6.2.2.

42 *Ibid*, s. 6.2.3.

43 *Ibid*, s. 4.1.

44 *Ibid*, Preamble.

45 *Ibid*, s. 4.2.1.

46 *Ibid*, s. 6.3.8.

47 *Ibid*, s. 4.2.1.

48 *Ibid*, s. 6.2.1.

49 *Ibid*, s. 6.2.3.

50 *Ibid*, s. 6.4.1.

51 *Ibid,* Appendix A – Definitions.

52 Canada Algorithmic Impact Assessment.

53 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single market Strategy for Europe, 6 May 2015, COM(2015) 192 final (2014-2019), online: **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192**. Commission von der Layen "Shaping Europe's digital future: A Europe fit for the Digital Age" (one of six priorities) (2020-2025), online: **https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en**.

54 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), online: **https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=FR**.

55 Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial intelligence Act) and amending certain Union legislative acts, online: **https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence**. For a short summary, in French see C. Castets-Renard, « Nouvelles règles et actions pour l'excellence et la confiance en l'IA », website of the chair Accountable AI in a Global Context, online: **https://chaireia.openum.ca/publications/la-commission-europeenne-propose-de-nouvelles-regles-et-actions-pour-lexcellence-et-la-confiance-dans-lintelligence-artificielle**.

56 Coordinated Plan on Artificial Intelligence 2021 Review, online: **https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review**.

57 Proposal for a Regulation of the European Parliament and of the Council on machinery products, April 21, 2021, online: **https://ec.europa.eu/docsroom/documents/45508**.

58 Ordinary legislative procedure, online: **https://www.europarl.europa.eu/infographic/legislative-procedure/index_en.html**.

59 The text does not mention the "facial recognition" technology what may be surprising. It is, however, covered by the expression remote biometric identification systems which means "an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified". This is exactly how a facial recognition system works.

60 A debate of the use of Facial Recognition has emerged since the white paper in February 2020 which did not contain such a ban, while earlier projects were more ambitious. Member states strongly requested the authorization to use this technology in favor of law enforcement that is the reason why two different sets of rules to regulate facial recognition have been enacted (unacceptable risks and high-risk regimes).

61 A Europe fit for the digital age, Empowering people with a new generation of technologies, online: **https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en**.

62 See (in French) C. Castets-Renard (2020), *Droit du marché unique numérique et de l'intelligence artificielle*, Bruylant, oct. 2020, 388 p., online: **https://www.larcier.com/fr/droit-du-marche-unique-numerique-et-intelligence-artificielle-2020-9782802764465.html**.

63 Article 9.1 of the *GDPR is about sensitive data, meaning personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*

64 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. This text was adopted on the same day as the GDPR. While the GDPR concerns civil and commercial matters, the directive deals with criminal matters and concerns the protection of personal data in the field of police and justice.

65 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. This text provides a framework for the protection of personal data by the institutions of the European Union, online: **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725**.

66 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), November, 25, 2020 COM(2020) 767 final, online: **https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN**.

67 See generally, *The Rise and Fall of Algorithms.*

68 See generally, *Regulating AI.*

69 Note, however, that the Directive could apply to certain aspects of policing done by the RCMP, and to certain decisions made by the Correctional Services Canada and the Parole Board of Canada.

70 *Scassa at 11.*

71 Canada ADM Directive, s. 4.2.1.

72 Scassa at 2.

73 Canada ADM Directive, s. 6.2.1.

74 *Ibid,* s. 6.2.3.

75 *Ibid,* s. 6.4.1.

76 *Ibid,* Appendix A – Definitions.

77 Canada Algorithmic Impact Assessment.

78 See Scassa, *Ibid*, and Jennifer Raso, "AI and Administrative Law" in Artificial Intelligence and the Law in Canada, eds. Teressa Scassa and Florian Martin-Bariteau, (Lexis-Nexis Canada) (2021).

79 Scassa at 28.

80 Directive (EU) 2019/2161 of the European Parliament and of the Council of of 27 November 2019, online: **https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L2161&from=FR**.

81 Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, online: **https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0771&from=en**.

82 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, online: **https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0770&from=FR**.

83 See generally, Law Commission of Ontario, *Regulating AI: Critical Issues and Choices* (2021) at 7.

84 Canada ADM Directive, s. 6.

85 Canada Algorithmic Impact Assessment.

86 Canada ADM Directive, s. 4.2.1.

87 *Ibid,* Canada ADM Directive, s.6.4.1.

88 *Ibid,* Canada ADM Directive, s. 6.4.1.

89 Canada Algorithmic Impact Assessment.

90 Canada ADM Directive, s. 6.2.1.

91 *Ibid,* s. 6.2.2.

92 *Ibid,* s. 6.2.2.

93 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, online: **https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31985L0374**.

94 In 2017, the Government of Canada appointed CIFAR to develop and lead the Pan-Canadian Artificial Intelligence (AI) Strategy, the world's first national AI strategy.

95 Canada's Digital Charte in Action: A plan by Canadians for Canadians (2019), online: **https://www.ic.gc.ca/eic/site/062.nsf/vwapj/Digitalcharter_Report_EN.pdf/$file/Digitalcharter_Report_EN.pdf**.

96 GPAI's 15 founding members are Australia, Canada, France, Germany, India, Italy, Japan, Mexico, New Zealand, the Republic of Korea, Singapore, Slovenia, the United Kingdom, the United States and the European Union. They were joined by Brazil, the Netherlands, Poland and Spain in December 2020.

97 OECD Principles on AI (2019), online: **https://www.oecd.org/going-digital/ai/principles/**.

98 The Global Partnership on Artificial Intelligence (GPAI), online: **https://gpai.ai/**.