Internet and E-Commerce Law in Canada

VOLUME 24, NUMBER 5 Cited as (2023), 24 I.E.C.L.C. SEPTEMBER 2023

# • QUÉBEC'S PRODUCT LIABILITY LAWS AND ARTIFICIAL INTELLIGENCE: A WHOLE NEW WORLD? •

Nicolas-Karl Perrault, Associate with the collaboration of Noah Boudreau,
Partner, Fasken Martineau DuMoulin LLP

Nicolas-Karl Perrault

Noah Boudreau

## LEGAL WARRANTIES OF QUALITY

**Pursuant** to the CCQ[1], the seller is bound to warrant the buyer that the property and its accessories are, at the time of the sale, free of latent defects which render it unfit for the use for which it was intended or which so diminish its usefulness that the buyer would not have bought it or paid so high a price if he/she had been aware of them. In a sale by a professional seller, a defect is presumed to have existed at the time of the sale if the property malfunctions or deteriorates prematurely in comparison with identical property or property of the same type.[2]

Considering the applicable presumptions, which often lighten the burden of proof on purchasers, and the generality of the terms used in the CCQ as to the scope of the warranty against latent defects, the application of these principles to incidents involving AI systems is likely to raise a number of contentious issues, particularly with respect to causation, the nature of the uses for which the AI system was intended, and what may be considered improper use by the purchaser which may exonerate the seller from liability in whole or in part.

While these issues are not unique to AI systems, the specific characteristics of AI systems, including their ability to learn and act autonomously and sometimes unpredictably, are likely to raise new evidentiary and legal issues. For instance, if purchasers attempting to claim damages for a latent defect related to the malfunction of an AI system wish to invoke the

• In This Issue •

LexisNexis®

INTERNET AND E-COMMERCE LAW IN CANADA

**Internet and E-Commerce Law in Canada** is published twelve times per year by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

**ISBN 0-433-43112-1 (print)** **ISSN 1494-4146**
**ISBN 0-433-44675-7 (PDF)**
**ISBN 0-433-44386-3 (print & PDF)**

Subscription rates: $335.00 per year (print or PDF)
$485.00 per year (print & PDF)

**General Editor**
Laura Flynn, J.D.
Content Development Associate
LexisNexis Canada Inc.
E-mail: laura.flynn@lexisnexis.ca

Please address all editorial inquiries to:

**LexisNexis Canada Inc.**
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: ieclc@lexisnexis.ca
Web site: www.lexisnexis.ca

EDITORIAL BOARD

**Note:** This newsletters solicits manuscripts for consideration by the Editors, who reserves the right to reject any manuscript or to publish it in revised form. The articles included in the *Internet and E-Commerce Law in Canada* reflect the views of the individual authors and do not necessarily reflect the views of the editorial board members. This newsletter is not intended to provide legal or other professional advice and readers should not act on the information contained in this newsletter without seeking specific independent advice on the particular matters with which they are concerned.

LexisNexis®

presumptions provided for by the CCQ, they will have to prove that the incident was caused by a malfunction of the AI and that that defect manifested itself prematurely. In all likelihood, meeting these criteria in relation to complex AI systems will require specific and detailed expert evidence. This will be especially true if the courts start applying product liability principles to software with built-in AI.

The legal warranty of quality is evaluated in relation to the use for which the property was intended. Unless the seller is aware of the buyer's particular intended use, the courts consider the "normal" use of the property. This will surely raise questions for goods incorporating complex AI systems that enable them to perform various tasks based on what is asked of them by users and the data provided to them. For example, what would be the "normal" use of a software application like ChatGPT? In general, it will be necessary to review the contractual documents, including the terms and conditions of purchase or service, to understand the applicable representations and limitations of the AI system's features, including its level of autonomy, terms of use, and appropriate maintenance requirements.

## PRESUMED KNOWLEDGE OF LATENT DEFECTS AND DEVELOPMENT RISKS

While sellers of AI systems will surely seek to limit their liability by including limitation of liability clauses and making the user responsible for supervising the system's actions and correcting its errors, the legal value of such limitations will likely be subject to challenges. Indeed, it must be recalled that under Quebec law, in no case can a professional seller limit its liability for defects of which they were aware or could not have been unaware.[3]

In accordance with the principles established by case law in the wake of *ABB Inc. v. Domtar Inc.*,[4] professional sellers are presumed to be aware of the defects in their products and their lack of knowledge generally constitutes a fault in itself.[5] The manufacturer may rebut the presumption only by showing that it was unaware of the defect and that its ignorance was justified.[6] In the case of products sold to consumers, merchants and manufacturers simply cannot claim ignorance of the defect as a defence in a latent defect action.[7]

To date, ignorance of a defect has very rarely been successfully asserted by manufacturers or specialized professional sellers. For AI systems used in a commercial context that are not intended for consumers, AI developers could potentially claim ignorance of a defect that is discovered after their system is released. However, since manufacturers are presumed to verify the quality of the products they put on the market, the courts will likely not easily side with manufacturers who invoke this defence.[8] A very specific exception is made for a development risk that no one could have known about when the product was put on the market. In view of the novelty and complexity of AI systems, the applicability of this exception is plausible, but it is a safe to assume that the courts will consider the steps taken by the defendant to test the system before and after it is release to market before exonerating an AI developer from liability for damages arising from product or system defects. This is particularly true since AI entrepreneurs have already expressed concern about deploying AI systems that have not been sufficiently tested to ensure that the risks associated with their use have been identified and can be controlled,[9] even though there is still no specific regulatory framework for AI system development and marketing activities.

## LIABILITY FOR THE AUTONOMOUS ACT OF A THING

We have discussed the obligations of developers and sellers of AI systems, but what of the liability of users? In the context of a claim against the seller of a property with a built-in AI system, the user's negligence in using or supervising the AI system may constitute a valid defence or a contributory fault that may result in shared liability.

In addition, the operator may also be liable for damages caused by a property with a built-in AI system if he/she acts as "custodian" of the property in question. Pursuant to the CCQ,[10] the custodian of a thing is bound to make reparation for injury resulting from the autonomous act of the thing, unless he/she proves that he/she is not at fault.

Liability for the autonomous act of the thing is subject to two specific conditions: the absence of direct human intervention in causing the injury, and the mobility or dynamism of the thing that caused the injury. Although almost all of the relevant case law concerns the autonomous act of physical things, the concept of "thing" covered by this article is broad and includes all movable, immovable, tangible and intangible property.[11] As with legal warranties of quality, it is therefore possible, if the reasoning of the court in the Fortnite decision cited previously was to be followed, that the liability regime for the autonomous act of a thing could find application not only to AI systems embedded in physical goods but also to AI systems embedded in software.

The concept of "custodian" of a thing that contains an AI system is also likely to raise interesting questions. According to the jurisprudence, the custodian is the person that, at the time the damage was caused, had a power of supervision, direction, command and control.[12] Custody of a thing is different from mere physical possession. The holder of a thing is not necessarily its custodian if he/she can exercise only limited control over it.[13] In the case of a physical thing that contains an AI system, it appears more obvious that the custodian of the thing will be the user if he or she has some control over the thing and the features of the AI system (e.g., self-driving car). However, in the event one considers the autonomous act of software, determining the identity of the custodian of the "thing" could prove to be far more complex and require an assessment of the totality of the circumstances, including the level of supervision, direction, command and control held by the various actors.

We note that the *Autonomous Bus and Minibus Pilot Project*[14] requires that the driver of an autonomous bus in motion "remain continuously attentive to events likely to affect road safety in order to be ready to intervene rapidly at any time in taking over control of the vehicle's automated system, immediately taking over the driving of the vehicle or adapting driving to the circumstances." This may suggest that users will generally not be able to avoid the obligations they would otherwise have by claiming an AI system malfunctioned if they failed to exercise due diligence or adequately monitor the AI's autonomous activities, particularly for AI systems used in risky and already highly regulated environments such as self-driving cars.

## CONCLUSION

At least for the meantime, it appears that the courts will have to rule on civil actions involving AI systems using the existing legal framework for civil liability in Québec. Indeed, and despite the expected enactment of the AIDA, until Québec's legislature passes new laws or amends existing laws to provide specific rules regarding the civil liability of developers, sellers, operators and users of AI systems, courts will be called upon to apply and adapt the current civil liability regime to claims involving AI systems.

While existing principles of product liability set out in the CCQ and the CPA should apply to disputes involving physical products with built-in AI systems without too much difficulty, the courts will likely be called upon to decide novel issues resulting from the unique characteristics of AI systems, including their ability to perform various tasks autonomously. Moreover, such disputes are likely to raise complex factual issues, including the causal link between the operation of an AI system and the damages and the level of care exercised by the user.

It is far more difficult to predict the legal framework that will apply in civil litigation involving AI systems embedded in software, particularly if such software were to be considered a "property" following the reasoning adopted by the Superior Court in the Fortnite decision. Until now disputes involving software have usually been governed by the general principles of Québec civil law in matters of contractual liability. However, the Fortnite decision is a sign that courts may be open to applying the principles of product liability, including legal warranties against latent defects, the manufacturer's liability for safety defects, and the custodian's liability for the autonomous act of a property, in ruling on such disputes. As those principles were generally developed for disputes involving physical goods, such an eventuality would raise a host of new legal issues which would have to be clarified by the courts or the legislature.

Government initiatives regarding the responsibilities of AI system developers will continue to be closely monitored, particularly for uses of AI systems that involve high risks due to their possible impact on the fundamental rights of third parties (privacy, discrimination, etc.) or the safety or health of users and the public. Close attention should also be paid to the developing case law regarding the characterization of software, including AI systems used in software, as "property" within the meaning of the CCQ. In this regard, we note that the defendants' application for leave to appeal the Fortnite decision was recently denied, which means that the class action will proceed to the merits. This decision could very well inspire similar litigation involving other video games or other types of popular digital services in the years to come. In fact, an application for permission to bring a class action was recently filed on January 24, 2023, against Meta, Facebook and Instagram alleging that they failed to warn Facebook and Instagram users of the risk of developing an addiction to those services.[15]

In the meantime, AI system developers and sellers can seek to minimize the risk of claims and litigation by clearly disclosing the system's features, its limitations, instructions of use, monitoring and maintenance, and the risks associated with its use and how to guard against them in their contractual documents and by including appropriate limitation of liability and indemnity clauses in such documents.

[***Noah Boudreau*** *is a Partner in the Litigation and Dispute Resolution group of Fasken Martineau DuMoulin LLP. Recognized in multiple Litigation Star lists, Noah is a seasoned litigator who acts regularly for internationally known corporations in the defence of significant private and class actions. His practice is also primarily focused on product liability, cybersecurity, consumer protection and transportation litigation matters.*

***Nicolas-Karl Perrault** is an Associate in the Litigation and Dispute Resolution group of Fasken Martineau DuMoulin LLP. Recognized on the "Ones-to-Watch" list, Nicolas-Karl's practice is mainly focused on cases involving product liability, disputes in the construction industry and consumer law. He also advises clients in the context of commercial contractual disputes, franchisee-franchisor relationships, disputes between shareholders and insurance coverage.*]

[1] Article 1726 CCQ.

[2] Article 1729 CCQ.

[3] Article 1728 CCQ.

[4] [2007] 3 S.C.R. 461, 2007 SCC 50 (S.C.C.).

[5] *Deguise* v. *Montminy*, [2014] J.Q. no 5604, 2014 QCCS 2672, paras. 1114–1116.

[6] *ABB Inc. v. Domtar Inc.*, [2007] 3 S.C.R. 461, 2007 SCC 50, para. 69 (S.C.C.); *CCI Thermal Technologies Inc.* v. *AXA XL (XL Catlin)*, [2023] J.Q. no 1043, 2023 QCCA 231, para. 44 (Q.C.C.A.).

[7] CPA, s. 53.

[8] *Imperial Tobacco Canada ltd* v. *Conseil québécois sur le tabac et la santé*, [2019] Q.J. No. 1387, [2019] J.Q. no 1387, para. 295 (Q.C.C.A.).

[9] "Musk, Bengio et un millier d'experts demandent une pause de six mois" (March 29, 2023), online at: https://www.lapresse.ca/affaires/techno/2023-03-29/intelligence-artificielle/yoshua-bengio-et-un-millier-de-personnalites-demandent-une-pause-de-six-mois.php.

[10] Article 1465 CCQ.

[11] *Québec (Ville de) v. Équipements Emu ltée*, [2015] J.Q. no 7623, 2015 QCCA 1344 (Q.C.C.A.).

[12] *Société d'assurances générales Northbridge v. 9180-2271 Québec inc. (Restaurant Pizzicato)*, [2014] J.Q. no 2735, 2014 QCCS 1304 (Qu. S.C.).

[13] *Pétroles Cadeko inc. c. 9166-0357 Québec inc.*, [2021] J.Q. no 10955, 2021 QCCS 3774 (Qu. S.C.).

[14] *Autonomous Bus and Minibus Pilot Project*, CQLR v. C-24.2, r. 37.01, s. 13.1.

[15] See the application for permission to institute a class action filed by Alexia Robert in the Superior Court of Québec (Court file number 500-06-01217-237).

# • SAFE BETS: FOSTERING RESPONSIBLE IGAMING •

Cam Cameron, Partner and Bryinne McCoy, Associate, Gowling WLG (Canada) LLP

**Cam Cameron**

**Bryinne McCoy**

The popularity of iGaming has soared in recent years, with online casinos and sports betting sites providing easy access to exciting wagering opportunities. However, it's important to acknowledge that gambling, in any form, carries inherent risks, including addiction and potential social and financial consequences.

## RESPONSIBLE GAMBLING STANDARDS IN ONTARIO

For those operating iGaming services in Ontario, maintaining a balance between promoting their business and ensuring responsible gambling can be challenging. While the environmental controls available to land-based casinos, such as face recognition, are not available in the online space, regulatory bodies have implemented standards to create similar protections and foster responsible iGaming environments.

The Alcohol and Gaming Commission of Ontario (AGCO), the regulatory authority for the iGaming industry in the province, has prescribed responsible gambling standards (the Standards) that iGaming operators must adhere to. These standards encompass various minimum requirements for responsible gambling (RG), including the obligation to ensure that players are "fit for play."

While the risk-based approach of such broad requirements offers operators flexibility in implementing compliant environments and practices, it also introduces ambiguity regarding compliance with each operator's specific practices.

## WHAT DOES "FIT FOR PLAY" MEAN IN AN ONLINE ENVIRONMENT?

The "fit for play" requirement entails that players confirm their readiness to engage in iGaming activities before participating on an iGaming site. While this requirement is relatively straightforward to enforce in physical establishments where staff can monitor players for signs of intoxication, monitoring online engagement poses inherent challenges.

Currently, iGaming sites typically ask players to confirm their fitness to play through a pop-up window and check-box. However, it remains uncertain whether this approach alone satisfies the Standards, as the phrase "fit for play" lacks a precise definition in the Standards or in case law. Operators must infer that it refers to a state of mental fitness that enables players to engage in iGaming without incurring significant negative consequences or health risks.

Being "fit for play" means participating in online gambling responsibly and in a controlled manner, without risking addiction, financial problems, or other adverse outcomes. It entails maintaining a healthy balance between the activity and other aspects of one's life, such as work, family, and social obligations.

Ensuring that players are "fit for play" poses challenges for iGaming operators. Practically speaking, operators must ultimately rely on players' self-assessment of their readiness, even though the RG obligations are imposed on the operator and non-compliance can result in significant risks, including fines. The AGCO takes breaches of the Standards seriously and has not hesitated to impose substantial fines.

Moreover, there are potential litigation risks for operators regarding RG matters, as Ontario courts have not provided clear guidance on whether gambling establishments owe a duty of care to their customers.

## WHAT IS THE VOLUNTARY SELF-EXCLUSION PROGRAM?

Another RG requirement outlined in the Standards is the implementation of a voluntary self-exclusion program. This program allows individuals concerned about or demonstrating signs of problematic or addictive gambling behavior to exclude themselves from a gaming site for a predetermined period or indefinitely.

However, effectively implementing such programs faces practical challenges, including identifying individuals with gambling problems who may not publicly exhibit symptoms. These challenges are magnified in the online environment, as individuals can create multiple accounts or register with different online gambling sites to bypass self-exclusion measures.

In an effort to address this issue, iGaming Ontario (iGO), which assists the AGCO in regulating the iGaming industry, intends to introduce a mandatory centralized self-exclusion program in the future, although it has not yet been implemented. Consequently, operators should explore additional measures to prevent individuals with gambling problems from engaging in online gambling.

While the above highlights some of the RG requirements defined in the Standards to cultivate a safe and responsible online gambling environment and mitigate the risks of fines or litigation, operators must adhere to all sections of the Standards without exception. Additionally, they should remain attentive to any other RG obligations identified by the AGCO and iGO.

### NAVIGATING COMPLEX REGULATORY CHANGES

To navigate the complex regulatory framework required by the AGCO and iGO, operators, and those looking to become operators, are advised to seek qualified legal counsel. Collaborating with experienced legal counsel will enable companies to stay ahead of regulatory changes and minimize exposure to fines, penalties, or the potential revocation of their operator's licence.

[***Cam Cameron*** *is a partner in the Business Law Department of Gowling WLG's Ottawa office, practicing in the Firm's Indigenous and Business Law Groups. Cam's general practice focuses on commercial contracts, including licensing, distribution, collaboration, and funding agreements. His particular specialties include Indigenous commercial matters and gaming law.*

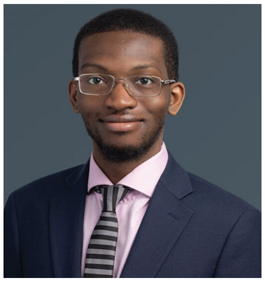
***Bryinne McCoy*** *is an associate lawyer in Gowling WLG's Ottawa office. She practices in the firm's Business Law Group and is licensed to practice law in Ontario and Newfoundland and Labrador. Bryinne's practice focuses on corporate commercial law, with an emphasis on contract and gaming law.*]

## • LEGAL RISKS ASSOCIATED WITH AUTOMATED HIRING TOOLS IN CANADA •

Ioana Pantis, Associate, Robbie Grant, Associate, and David Adjei,
Summer Law Student, McMillan LLP

**Ioana Pantis**

**Robbie Grant**


**David Adjei**

**On** July 5, 2023, New York's new law regulating automated employment decision tools ("Local Law 144") came into force. Among other things, Local Law 144 will require employers that use automated employment decision tools to conduct independent bias audits and notify employees and prospective hires of their use of such tools.[1]

We have received a number of questions about how automated hiring tools are regulated in Canada. This bulletin will provide an overview of the attractions and risks of using automated hiring tools, including a summary of two upcoming laws which will have a significant impact on the use of such tools (those being Québec's Act 25[2] and Bill C-27[3]).

### WHAT ARE AUTOMATED HIRING TOOLS, AND WHAT MAKES THEM ATTRACTIVE?

For the purposes of this bulletin, we use the term "automated hiring tools" to refer to any tools which assist in hiring decisions, whether or not a human reviewer is involved. There is a great range of automated hiring tools, with varying degrees of human intervention. For example,

- Targeted job advertisements may use algorithms to determine the best place to advertise job opportunities, which may influence the pool of applicants.
- Resume screening tools can eliminate resumes according to certain requirements or stipulations.
- Intelligent applicant tracking systems analyze application materials to estimate how a candidate might perform on the job based on keywords, past employee data, or algorithms.
- AI-powered video interviewing tools advertise the ability can assess candidates based on facial expression analysis.

There are two main incentives for adopting automated hiring tools: to increase efficiency and to reduce bias.

Particularly in industries with low barriers to entry, companies may receive hundreds or thousands of job applications—at times too many for the hiring team to review in detail. Some sources have suggested that the volume of job applications will increase as more applicants use free generative AI tools such as ChatGPT to assist in drafting cover letters or resumes.[4] Automated hiring tools can save costs and reduce reliance on arbitrary methods of prioritizing candidates (such as time of application, or first letter of applicant's name). Ideally, such tools can rank candidates in a manner that brings the best candidates to the top of the list.

Automated hiring tools also have the potential to reduce bias, and lead to better hiring outcomes, if properly managed. Studies have demonstrated that human hiring decisions are often influenced by unconscious bias.[5] Automated hiring tools may be able to reduce bias significantly (though, as discussed below, without proper management, they may create or reinforce bias as well).

## AUTOMATED HIRING TOOLS COME WITH RISKS

Along with their potential benefits, the use of automated hiring tools may give rise to legal risks. For example:

- Privacy laws may apply to the use of such technology insofar as the systems use personal information.
- Human rights laws may apply insofar as the use of these systems could lead to discrimination.
- Canada has laws related to automated decision tools coming into force in Québec on September 22, 2023, brought on by Québec's Act 25.
- Additional requirements for automated decision, prediction or recommendation tools are set out in the current draft of the Consumer Privacy Protection Act ("CPPA"), which forms a part of Bill C-27, currently under consideration in Parliament.[6]
- Finally, Canada's proposed Artificial Intelligence and Data Act (the "AIDA"), which also forms a part of Bill C-27, may apply to automated hiring tools, insofar as such tools meet the AIDA's definition of "AI System."[7]

## AUTOMATED HIRING TOOLS MAY TRIGGER OBLIGATIONS UNDER PRIVACY LAWS

In Canada, where privacy laws apply to the employment relationship, employers must ensure that their use of automated hiring tools complies with privacy laws.[8] In particular, employers must ensure they obtain valid consent where required, protect personal information with appropriate safeguards, and limit the collection, use and disclosure of personal information to appropriate purposes.

Canadian privacy laws generally require organizations to obtain consent in order to collect, use or disclose personal information. Analyzing an individual's application materials with an automated hiring tool would likely require consent. Furthermore, Québec's privacy regulator has previously ruled that the use of an algorithmic prediction system to generate a "score" for an individual constitutes a new collection of personal information, which would also require fresh consent.[9]

There are exceptions to these consent requirements under the Personal Information Protection and

Electronic Documents Act ("PIPEDA"), and substantially similar privacy laws in British Columbia and Alberta, for any collection, use or disclosure of personal information that is reasonable (under PIPEDA, "necessary") to establish, manage or terminate the employment relationship. Whether the use of automated hiring tools to assess a candidate would be reasonable or necessary in order to establish an employment relationship is not clear, and would likely depend on the context. However, the use of an individual's application materials to train an automated system for future use would likely fall short of these exceptions and require employee consent.

## AUTOMATED HIRING TOOLS MAY LEAD TO EXPOSURE UNDER HUMAN RIGHTS LAWS

One significant risk of using an automated hiring tool is the risk of bias and discrimination in the outcome. Bias can lead to worse hiring decisions, and liability under applicable human rights laws, which prohibit discrimination in employment based on certain protected grounds, such as race, ethnic origin, gender identity, age, etc.

Automated hiring tools are only as good as the dataset used to train them. If there is bias in the underlying training data, this bias may be amplified in the results. For example, a system trained on the application materials of past successful candidates may favour the demographic group that is most represented in the workplace. This bias may be difficult to detect, since an automated hiring tool may find other information that can be used as a proxy for demographic group. For example, a machine-learning based algorithm may prioritize certain candidates based on location (which could act as a proxy for membership in a certain cultural or racial demographic), or language choice (which may indirectly correlate with gender or cultural background).

Where the underlying decision-making formula is too complex or not readily discernable (as with black-box AI systems), it may only be possible to evaluate a system's biases with an audit performed by professionals. Employers that make adverse hiring and employment decisions based even in small part on protected grounds will be unlikely to avoid human rights liability by placing blame on an external automated hiring tool developer. It is therefore essential for employers to ensure their automated hiring tools are carefully and regularly assessed.

## FORTHCOMING TRANSPARENCY LAWS MAY APPLY TO AUTOMATED HIRING TOOLS

The problem of transparency will become more pressing as new privacy laws come into force, particularly transparency requirements under section 12.1 of Québec's Act respecting the protection of personal information in the private sector (the "Québec Act") (which comes into force on September 22, 2023), and sections 62 and 63 of the proposed CPPA, which is currently under consideration in Parliament.

### Section 12.1 of the Québec Act (September 22, 2023)

When section 12.1 of the Québec Act comes into force, Québec employers that use personal information to render a decision based exclusively on automated processing must inform prospective hires of this fact not later than the time the decision is communicated to them. Upon request, the employer must also inform the employee or applicant of:

- the personal information used to render the decision;
- the principle factors and parameters that were used to render the decision; and
- the right of the individual to have the personal information used to render the decision corrected.[10]

In addition, the employee or applicant must be given an opportunity to submit representations to a person in a position to review the decision.

Importantly, these requirements only apply to decisions rendered exclusively by automated processing. If a human being meaningfully participates in the decision-making process, the requirement will not apply.

One open question is whether this notice requirement will apply where an employer rejects a prospective employee's job application without notice to the applicant. Based strictly on the wording of the legislation, the requirement would never be triggered if the individual is never informed of the non-hire decision.

### Sections 62 and 63 of the Consumer Privacy Protection Act

As a starting point, the CPPA would only apply to a subset of employment relationships. Like PIPEDA (the legislation it would replace), the CPPA would only apply to applicants for work in a federally regulated workplace, or independent contractors in provinces without substantially similar privacy legislation.[11]

Under the current proposed draft CPPA, an "automated decision system" is defined as any technology that assists or replaces the judgment of human decision-makers through the use of a rules-based system, regression analysis, predictive analysis, machine learning, deep learning, a neural network or other technique.[12] If Bill C-27 is passed in its current form, section 62 of the CPPA would require organizations  to make readily available information about the organization's use of automated decision systems to make predictions, recommendations or decisions about individuals that could have a significant impact on them.[13]

Furthermore, if an organization uses an automated decision system to make a prediction, recommendation or decision about an individual that could have a significant impact on them, the organization must provide an explanation of the decision upon request by the individual.[14] The explanation must include:

- the type of personal information used to make the prediction, recommendation or decision;
- the source of the personal information; and
- the reasons or principal factors that led to the prediction, recommendation or decision.

The CPPA's requirements differ significantly from those outlined in section 12.1 of the Québec Act. First, the CPPA has a broader scope, as it covers automated hiring tools that either replace or assist human decision-makers and includes predictions and recommendations in addition to decisions. Thus, it applies to the use of automated hiring tools even when a human is "in-the-loop."

However, it is narrower than section 12.1 of the Québec Act because it only applies to the use of automated decision systems that will have a significant impact on individuals. While the term "significant impact" is not defined, it is difficult to conceive of a more significant impact than a decision regarding an individual's employment, so this narrower scope may not have much impact on the way the laws apply to automated hiring tools.

Furthermore, unlike section 12.1 of the Québec Act, which requires individual notifications by employers, the CPPA would require general public disclosure from employers, but place the responsibility on applicants or employees to request further information about an employer's use of automated decision systems as it pertains to them. The CPPA would also differ from 12.1 of the Québec Act in that it would not provide individuals with the right to have the decision (or prediction or recommendation) reviewed.

### AUTOMATED HIRING TOOLS COULD BE DEEMED "HIGH RISK" UNDER THE AIDA

If passed in its current form, the AIDA may impose significant obligations on employers using automated hiring tools, if those tools meet the definition of "AI System" under the AIDA.[15]

Innovation, Science and Economic Development Canada's companion policy to the AIDA specifically identified "screening systems impacting access to services or employment" as an area of interest to the government.[16] Given the severity of impact, imbalance of economic power of affected individuals, and inability to opt-out, AI systems used in the hiring process could well constitute "high impact" systems under AIDA, which would make such systems subject to a host of (yet unspecified) requirements related to human oversight, monitoring, transparency, fairness and equity, safety, accountability and/or validity and robustness.[17]

With that said, there are some unresolved questions about the application of the AIDA to employment relationships, given the division of powers between the federal and provincial governments, and the wording of the AIDA itself. Most requirements of the AIDA are confined the international or interprovincial trade and commerce. While the AIDA will likely apply to the commercial development and sale of employment-directed AI systems, it is not clear if it will extend to an employer's use of such systems in an employment setting.

## KEY TAKEAWAYS

Automated hiring tools present Canadian employers with advantages and risks. These tools offer increased efficiency and the potential to reduce bias in the hiring process. However, they may also give rise to privacy and human rights risks. It is crucial for employers to ensure compliance with privacy laws, obtain necessary consent, and mitigate the risk of discrimination with appropriate audits and legal reviews.

New transparency laws, such as section 12.1 of the Québec Act and sections 62 and 63 of the proposed CPPA, will impose additional requirements on employers using automated hiring tools. Furthermore, the forthcoming AIDA may impose additional obligations on the use of automated hiring tools. Consequences for failing to comply with the above laws could include litigation, regulator investigations, reputational impact, and administrative monetary penalties or fines. Employers should closely monitor legal developments and assess the potential impact of these tools on their hiring practices.

[***Ioana Pantis*** *is an accomplished employment lawyer with experience in all areas of management side-employment and human rights law. Her practice involves providing advice and representation to employer clients on a broad range of issues, including employment agreements, employment standards, termination advice and strategy, wrongful dismissal litigation, human rights, and accommodation.*

***Robbie Grant*** *is in the regulatory group, with a focus on privacy, data protection, and anti-spam law. His practice covers a wide range of privacy matters, including drafting and reviewing privacy policies, coordinating responding to data breaches, and advising on the privacy law dimensions of business practices and transactions. He also assists clients in preparing privacy impact assessments and responding to access to information requests.*

***David Adjei*** *is a summer law student at McMillan LLP and is pursuing his JD at Osgoode Hall Law School of York University. He is currently a representative for Osgoode Hall's International Law Society and is a student caseworker at Osgoode's Community & Legal Aid Services Program.*]

[1] Simone R.D. Francis and Zachary V. Zagger, "New York City Adopts Final Rules on Automated Decision-making Tools, AI in Hiring" (April 2023) National Law Review, online: https://www.natlawreview.com/article/new-york-city-adopts-final-rules-automated-decision-making-tools-ai-hiring.

[2] An Act to modernize legislative provisions as regards the protection of personal information, S.Q. 2021, c. 25.

[3] Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, short titled the Digital Charter Implementation Act.

[4] See for example, Morgan Smith, "ChatGPT can help you write a standout CV in seconds, job experts say: It's 'the ultimate resume-writing cheat code'" (March 22, 2023), CNBC, online: https://www.cnbc.com/2023/03/22/chatgpt-can-help-you-write-a-standout-resume-in-secondsheres-how.html.

[5] Truc Ngyuyen, "What's in a name? We talk to experts about racial bias in hiring and how to work to change it" (September 13, 2018), CBC, online: https://www.cbc.ca/life/culture/what-s-in-a-name-we-talk-to-experts-about-racial-bias-in-hiring-and-how-to-work-to-change-it-1.4822467.

[6] Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, short titled the Digital Charter Implementation Act at Part I, the Consumer Privacy Protection Act.

[7] See Robbie Grant, "ISED Releases Companion to Proposed AI Law: Timelines, Guidelines, and Enforcement" (April 17, 2023), online: https://mcmillan.ca/insights/publications/ised-releases-companion-to-proposed-ai-law-timelines-guidelines-and-enforcement/.

[8] Currently federally regulated employees, independent contractors, and employees in British Columbia, Alberta and Québec are subject to private sector privacy laws, although privacy concepts are applicable to the employment relationship in other provinces through privacy torts (for example, see Kristen Pennington, "Shedding "Light" on a New Privacy Tort" (March 2020), online: https://mcmillan.ca/insights/shedding-light-on-a-new-privacy-tort/ and Lyndsay A. Wasser "Seclusion Intrusion: A Common Law Tort for Invasion of Privacy" (January 2012), online: https://mcmillan.ca/insights/seclusion-intrusion-a-common-law-tort-for-invasion-of-privacy/.

[9] Enquête concernant le Centre de services scolaire du- Val- des- Cerfs (anciennement Commission scolaire du Val-des-Cerfs) Commission d'accès à l'information du Québec, Dossier: 1020040-S, online: https://decisions.cai.gouv.qc.ca/cai/ss/fr/item/520925/index.do.

[10] Québec Act, s. 12.1, as enacted by Act 25 (in force, September 22, 2023).

[11] Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, short titled the Digital Charter Implementation Act, Consumer Privacy Protection Act, s. 6.

[12] Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, short titled the Digital Charter Implementation Act, Consumer Privacy Protection Act, s. 2.

[13] Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, short titled the Digital Charter Implementation Act, Consumer Privacy Protection Act, s. 62.

[14] Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, short titled the Digital Charter Implementation Act, Consumer Privacy Protection Act, s. 63 (3).

[15] Currently, the definition of AI System is "a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions": Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, short titled the Digital Charter Implementation Act as of April 24, 2023, Part 3, s. 2, s.v., "artificial intelligence system".

[16] See Robbie Grant, "ISED Releases Companion to Proposed AI Law: Timelines, Guidelines, and Enforcement" (April 17, 2023), online: https://mcmillan.ca/insights/publications/ised-releases-companion-to-proposed-ai-law-timelines-guidelines-and-enforcement/.

[17] Innovation, Science and Economic Development Canada, "The Artificial Intelligence and Data Act (AIDA) – Companion document" (March 13, 2023), online: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document.