International Journal of Law, Ethics and Social Sciences

Article

Necessity and Institutional Design of Introducing a Qualified Right to Human Review of Significant Automated Decisions in Hong Kong, China: A Comparative Study Based on GDPR Article 22 and the PRC's Personal Information Protection Law

Jingyue Yu [1,*]

[1] the University of Hong Kong, Hong Kong, China
* Correspondence: Jingyue Yu, the University of Hong Kong, Hong Kong, China

Abstract: The rapid proliferation of automated decision-making (ADM) systems has raised significant concerns regarding algorithmic accountability, transparency, and the protection of individual rights. This article critically examines the necessity and institutional design of introducing a qualified right to human review for significant automated decisions within the legal context of Hong Kong, China. By conducting a comprehensive comparative study based on Article 22 of the European Union's General Data Protection Regulation (GDPR) and the People's Republic of China's Personal Information Protection Law (PIPL), this research identifies the respective strengths and weaknesses of these prominent regulatory frameworks. The analysis demonstrates that Hong Kong, China's current reliance on voluntary administrative guidelines and fragmented, sectoral-specific regulations is insufficient to address the complex challenges posed by advanced algorithmic systems. Consequently, this study argues that Hong Kong, China urgently requires the enactment of a robust statutory right to human review. To achieve this, the article proposes a five-pronged institutional design: first, redefining the legal scope of ADM subject to mandatory human review; second, establishing substantive and meaningful human intervention mechanisms; third, embedding a clear right to explanation as the foundational pillar for algorithmic transparency; fourth, formulating differentiated regulatory requirements tailored to the public and private sectors, coupled with independent oversight; and fifth, improving practical application, enforcement mechanisms, and accessible remedies. Ultimately, this framework aims to balance technological innovation with fundamental data privacy rights.

Keywords: automated decision-making; human review; data privacy; algorithmic accountability; right to explanation

Received: 05 April 2026
Revised: 11 May 2026
Accepted: 25 May 2026
Published: 01 June 2026

1. Introduction

An algorithm is a mechanism that enables machines to make decisions by filtering data and selecting features, capable of delivering solutions tailored to specific needs [1, 2]. However, algorithms are not always reliable, as they are prone to bias and errors. Such bias often originates from poor-quality training data, and the design of algorithmic models themselves can also negatively influence the decision-making process. Additionally, algorithms can be exploited to target users' vulnerabilities. Their processes and underlying rationales are frequently opaque to affected users, giving rise to the "black box" paradigm, as algorithms often lack transparency and interpretability. It is essential for legal frameworks to protect individuals' rights to review algorithmically generated decisions. No human being should be reduced to a mere object of the decision-making process; human dignity must be safeguarded by ensuring individuals have the right to contest decisions made by algorithms.

The GDPR and the PIPL grant individuals the right to challenge algorithmic decisions. However, each regulatory framework has its own strengths and weaknesses. This paper will examine how the EU and China have established a right to human review of significant automated decisions [3]. It will then propose how Hong Kong, China can introduce a qualified right to such review, ensuring it does not become a purely procedural safeguard.

2. EU's Approach

2.1. General Approach

Article 22 of the GDPR aims to prohibit algorithms in the machine learning field that wield non-transparent discretionary power from automated decision-making ("ADM"). This provision is designed to protect the public from "machine determinism" and uphold the principle of "informational self-determination," thereby preventing unfair and differential treatment of individuals by algorithms.

Article 22(1) sets out the general principle that "the data subject shall have the right not to be subject to a decision based solely on automated processing, which produces legal effects or similarly significantly affects the person concerned." This provision establishes a general prohibition that applies irrespective of whether the data controller takes any further action in relation to the personal data processing. Accordingly, data controllers are prohibited from carrying out ADM that produces legal effects or similarly significant consequences unless an exception applies. Article 22(2) provides for three exceptions: (a) for contract performance; (b) authorized by law; or (c) based on the data subject's explicit consent [4, 5]. Where an exception applies, Article 22(3) requires data controllers to implement appropriate measures to safeguard the data subject's rights and legitimate interests, including a human intervention mechanism.

2.2. Strengths

First, this provision adopts a rights-based approach, which grants individuals the core right to be protected from ADM through a comprehensive and systematic procedural framework. This advantage is further reinforced by transparency principles. Pursuant to the right to be informed, data controllers shall provide data subjects with information on how the ADM will operate, particularly where the ADM involves profiling [6, 7]. Such information shall include the existence of ADM falling within the scope of Article 22, meaningful information about the underlying logic, and the consequences of such processing. With Article 22 underpinned by these transparency obligations, data subjects will be aware of their right to consent to or opt out of ADM. This framework ensures the enforceability and accountability of Article 22.

Second, working guidelines mandate "meaningful human intervention of Article 22," as controllers cannot circumvent this provision by engaging in nominal or superficial human involvement. If such human involvement does not materially affect the outcome of the decision, the oversight of the ADM cannot be regarded as "meaningful human intervention." Such oversight must be exercised by an authorized and competent person to consider all relevant information to overturn the decision. This ensures that human oversight is always present in ADM processes [8].

2.3. Weaknesses

Firstly, the meaning of "solely automated decision-making" is unclear. Any degree of human involvement in the automated decision-making process can evade compliance with Article 22 requirements [9]. It remains uncertain what level of human involvement is necessary, and whether decisions ultimately made by humans but prepared using automated processing should be classified as automated decision-making. Automated decision-making in preparatory processes may not be regulated by Article 22, but it can still have a profound impact on individuals.

Second, while Article 22 clearly applies to automated decision-making that produces legal effects, its application to automated decision-making that produces "similarly

significant effects" is vague. Legal effects from automated decision-making include "affecting a data subject's legal rights, legal status, or contractual rights." However, the meaning of "similarly significant effects" remains ambiguous, even though it has been clarified that data subjects may still be entitled to protection even where no legal rights are altered [9, 10]. For example, practices such as behavioral advertising are generally excluded from Article 22 because they do not "significantly affect" data subjects, yet these practices, which permeate daily life, require regulatory intervention.

Third, rights to conduct human intervention are largely ineffective due to the absence of guidelines. When seeking to exercise their right to conduct human intervention, data subjects often do not know whom to contact, and submitting a view does not automatically trigger a review of the automated decision-making process. Even when a review is conducted, the inherent complexity of automated decision-making systems or unjustified reviewers hired by data controllers makes it difficult and unlikely for controllers to overturn automated decisions. Similarly, data subjects face barriers to contesting decisions, as there are no clear procedures to follow. Additionally, data subjects lack the technical expertise, information, and resources necessary to effectively challenge algorithmic decisions. As a result, the substantive protection afforded by Article 22 remains limited [11].

Lastly, Article 22 is not accompanied by mandatory regulatory mechanisms for automated decision-making, such as independent audits; the burden of proving that an automated decision-making system is harmful falls disproportionately on the public, rather than on system operators. Furthermore, there is no precedent or administrative enforcement to clarify the consequences of breaching Article 22, rendering the right largely unpredictable. Due to the lack of compliance incentives and guidance, data controllers and governments frequently disregard this provision. The public is also unaware of this right, and although a landmark case confirmed that automated credit scoring falls within Article 22, meaningful enforcement of Article 22 remains ineffective.

3. China's Approach

3.1. General Approach

The PIPL serves as the foundation of China's legislative framework addressing risks associated with AI [5, 12]. It governs automated decision-making (ADM) through Article 24, which outlines key principles, obligations for personal information handlers, individual rights, and specific rules for ADM that significantly impact individuals.

Article 24(1) stipulates that personal information handlers must adhere to the principles of transparency, fairness, and reasonableness throughout the decision-making process. Article 24(2) provides individuals with the right to refuse ADM used for information dissemination or commercial marketing, as well as the right to opt out of ADM targeting their personal characteristics. Unlike the GDPR's provision granting individuals the right not to be subject to ADM, Article 24(3) establishes two distinct rights: the right to request an explanation of the decision and the right to refuse decisions made solely by ADM that significantly affect their rights and interests [13]. Additionally, Article 73 defines ADM as decision-making conducted by computer programs that evaluate personal attributes, including behavior, preferences, and health.

3.2. Strengths

First, in terms of the structural governance of ADM in China, the country has adopted an algorithm filing system [14]. Under this system, ADM providers whose services have attributes of public opinion influence must disclose relevant information to the regulator within 10 working days of commencing operations, thereby enabling the regulator to gain a comprehensive understanding of the operation and potential impacts of the ADM systems. Furthermore, the algorithm filing system supports ongoing regulatory monitoring, as the information submitted also covers the ADM provider's risk control capabilities, allowing regulators to proactively assess and assign accountability.

Second, the right to refuse ADM under the PIPL is significantly stronger than its GDPR counterpart, as it is not subject to the three statutory exceptions that limit the scope of protection under the GDPR. Under the GDPR, the prohibition on solely automated decision-making does not apply to decisions necessary for the performance of a contract, authorized by law, or based on explicit consent. In contrast, under the PIPL, personal information handlers cannot rely on any exceptions to evade their obligations where a decision is made solely by ADM and has a significant impact. Even though the GDPR mandates that controllers adopt suitable measures to safeguard data subjects' rights and interests, including human intervention, where solely automated decision-making has a significant impact, the practical application of these requirements remains undefined [9]. The PIPL therefore places the onus of prohibition and compliance squarely on personal information handlers to protect the public, and handlers cannot invoke any exceptions to avoid human intervention for decisions made solely by ADM systems.

Third, compared with the GDPR, the rights and obligations under the PIPL are far more explicit and precise. Article 24(1) mandates that the principles of transparency, fairness, and reasonableness apply to all ADM activities, which provides basic principles and requirements to different services and upholds a clear guideline for ADM operation and application in China. The PIPL also explicitly enshrines the right to an explanation in Article 24(3), whereas this right is only mentioned in the non-binding recitals of the GDPR. The Chinese Government initiated "Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services 2021" ("2021 Provisions"), which requires ADM service providers not only to ensure the security of the internet, maintain market order, and protect individual rights, but also to provide additional protections for vulnerable groups. Moreover, Article 73 provides a statutory definition of ADM, which clarifies the scope of application of Article 24 for both personal information handlers and individuals. These clear statutory provisions and detailed rules reduce legal ambiguity and provide the public with a more predictable framework for understanding ADM regulation.

3.3. Weaknesses

First, similar to the shortcomings of GDPR Article 22, the application thresholds under the PIPL remain fundamentally vague. While regulators have sought to provide protection for different sub-types of the right to explanation in various scenarios, the operation of these rules remains uncertain. In addition, the PIPL does not clearly specify the extent and manner in which ADM systems should be disclosed or explained to the public, nor does it provide any objective criteria for determining what constitutes "significant effects" under Article 24. Although the 2021 provisions require internet service providers to comply with algorithmic transparency and explanation requirements, the enforcement of these provisions has been ineffective due to the absence of detailed implementing rules. The right to explanation under Article 24 is also poorly understood by the public, as it does not entitle individuals to access all technical information about ADM systems [15]. It is therefore necessary to first clarify the proper scope of the explanation obligation—namely, whether it is the decision itself or the underlying ADM process that must be explained—and then establish tailored methodologies for such explanation.

Second, the PIPL adopts a dual-track regulatory system, imposing different ADM obligations on the private sector and the government, which allows for sector-specific requirements. However, the effectiveness of ADM obligations imposed on the government is highly questionable, as there have been no reported cases of citizens successfully suing public authorities over algorithmic decisions in administrative proceedings. During the COVID-19 pandemic, when the health code system was used by public authorities to assess individual epidemiological risk and restrict movement, concerns arose regarding its application. For instance, the assignment of red health codes, which prevented travel to certain destinations and imposed mandatory movement restrictions and quarantine requirements, demonstrated that a tool originally designed for

public health purposes could be repurposed in ways that raised accountability concerns. This highlighted the PIPL's limitations in preventing government misuse of ADM in the public sector and underscored the need for stronger algorithmic accountability mechanisms applicable to government entities.

4. Hong Kong, China's Approach

4.1. Current Regulatory Landscape for ADM

Hong Kong, China currently adopts a dual-track regulatory model for data governance, whereby regulation is delivered through a combination of government guidance and self-regulation by sector-specific regulatory bodies. Regulation of artificial intelligence and ADM remains in its early stages. The primary legislative instrument that indirectly governs ADM is the Personal Data (Privacy) Ordinance ("PDPO"), which does not yet contain any provisions addressing the regulation of ADM systems. While the Privacy Commissioner for Personal Data ("PCPD") and the Digital Policy Office ("DPO") have issued a number of guidelines on AI and data protection, these frameworks are purely voluntary and non-binding. To address this regulatory gap, sector-specific regulators have published their own guidance. Notably, guidelines issued by regulators in the banking and finance, healthcare, and insurance sectors carry binding force, as they derive their authority from the respective sectoral ordinances, rather than the PDPO or any dedicated AI legislation [16].

ADM systems inevitably make errors, which can accumulate throughout the decision-making process, leading to harmful outcomes often caused by low-quality input data and underdeveloped algorithms [10]. Hong Kong, China 's non-binding guidelines to regulate ADM are insufficient to address the risks posed by these systems. A statutory framework is necessary to mitigate such harms and ensure accountability in ADM decision-making. Establishing a statutory basis for human review, supported by transparency principles, is essential to guarantee due process and prevent harm caused by solely automated decisions. Moreover, an effective legal right to human review of significant automated decisions should encompass both an obligation of "conduct," requiring ADM system operators to dedicate adequate efforts, and an obligation of "outcome," ensuring that human review effectively protects the public from harm caused by ADM systems.

4.2. Redefining the Scope of ADM Subject to Human Review

First, the most critical flaw of GDPR Article 22 is its "solely automated processing" threshold, which allows data controllers to easily bypass this protection by inserting a generic, nominal human review step to claim that a decision is not made purely by ADM. Hong Kong, China should adopt an approach where any decision in which ADM plays a determinative, material, or substantial role in the process or outcome is subject to human review, regardless of whether professional or nominal human supervision is present. Eliminating the "solely" requirement and adopting a "heavily influenced by ADM" standard reflects the practical reality that ADM not only makes final decisions on behalf of humans but can also exert a decisive influence on human decision-making, even when a human formally renders the final decision [17]. This reform should explicitly cover "quasi-automated decisions"—those made by humans who are heavily influenced by ADM outputs or affected by automation bias.

Second, while both the GDPR and the PIPL stipulate that ADM producing legal effects or similarly significant effects should be subject to human review, neither framework clearly defines what constitutes a "significant effect." Hong Kong, China can adopt the interpretation that "legal effects mean impacts on an individual's legal rights, legal status, or contractual rights." However, the determination of "significant effects" must be based on objective criteria; otherwise, the term will remain overly contextual or subjective. To address this, Hong Kong, China should issue regularly updated guidance clarifying the types of conduct that meet the "significant effect" threshold [18]. Such guidance should include, as a non-exhaustive list, automated decisions in the areas of

personal finance, employment, social welfare, and healthcare. The threshold may be adjusted in specific circumstances:

- Decisions that affect an individual's financial circumstances, such as credit history for further loan applications, shall constitute a "similarly significant effect."
- Decisions that place an individual at a serious disadvantage in employment shall meet the "significant effect" threshold.
- Decisions that could result in the loss of access to public social benefits or citizenship shall qualify as having significant effects.
- The "significant impact" threshold shall be lowered where the processing involves sensitive personal data, vulnerable data subjects, large-scale processing of personal information, or new technologies that amplify the scale of potential harm.

Third, Hong Kong, China should also learn from the EU AI Act and adopt a risk-based framework to ensure that regulatory requirements are proportionate to the potential harm posed by different ADM systems. This framework should align closely with the definition and threshold of "significant effect" to enhance public understanding of applicable compliance requirements and balance public interest protection with regulatory efficiency [19]. Furthermore, for effective governance, Hong Kong, China should explicitly provide a list of grounds to challenge algorithmic decisions. These grounds could include discrimination, inaccuracy, or unlawfulness. This structured approach would help regulators, human reviewers, and affected individuals understand how data protection and privacy principles apply to specific ADM processes.

4.3. Establishing Meaningful Human Intervention

For human oversight to be meaningful, intervention must enhance the quality, fairness, accountability, and reliability of algorithmic decisions while substantively monitoring automated decision-making processes [20]. Human reviewers must have the legal authority to overturn decisions and possess the technical expertise necessary to challenge outputs from automated decision-making (ADM) systems. A review that cannot alter the outcome or merely replicates the ADM process is not meaningful. Additionally, since ADM systems often produce opaque decisions, reviewers must have sufficient expertise to critically evaluate algorithmic outputs. Reviewers should act in good faith, aligned with the core purpose of human intervention. Furthermore, reviewers must receive appropriate training tailored to the specific ADM system and its operational tasks.

Human reviewers must be independent and have unrestricted access to ADM decisions and underlying data [21]. The optimal approach to ensuring reviewer independence is to separate reviewers entirely from the teams responsible for ADM development and operation. Organizations must provide an environment that shields reviewers from undue influence, enabling them to conduct impartial evaluations. For high-stakes decisions that may be overturned, multiple reviewers should be assigned to the case. A multi-reviewer panel helps limit individual discretion, facilitates mutual oversight, mitigates cognitive biases, and enhances overall accountability.

Human reviewers should conduct a thorough assessment using all relevant and related information. As ADM systems may fail to capture all pertinent contextual data from individuals, reviewers have the opportunity to collect and evaluate additional information during the review process. Meaningful intervention requires reviewers to adopt a fresh perspective to determine whether the algorithmic decision complies with legal standards. Reviewers should consider not only the data already factored into the ADM system but also any additional mitigating or aggravating circumstances. No relevant information should be arbitrarily disregarded, as this would render the review incomplete and unfair. Ideally, review panels should be multi-professional, including data analysts to identify false positives and discriminatory outcomes, and may seek assistance from independent external oversight bodies to rigorously scrutinize high-risk ADM decisions.

4.4. A Clear Right to Explanation as a Foundation for Transparency

First, a statutory right to explanation is essential in Hong Kong, China, as any challenge to an ADM-generated decision will be meaningless if the affected individual cannot understand the underlying logic and rationale of that decision. The GDPR does not explicitly enshrine a right to explanation in its operative provisions. This has led to ongoing debate over the very existence of such a right and has made it difficult for data subjects to request human intervention, as they are unable to access the specific reasons and logic behind their individual cases. Hong Kong, China should therefore directly establish a binding individual right to explanation. This right should not be limited to providing general information about the logic of ADM systems; it must require controllers to clearly disclose the specific factors and core reasons that influenced and determined their individual decisions. For example, where a loan application is rejected by an ADM system because of unsatisfactory income, the system must clearly state the applicable threshold and the specific factors it took into account.

Second, as neither the GDPR nor the PIPL provides clear details on the required scope and depth of explanations, Hong Kong, China should mandate that all explanations be transparent to the person concerned. The standard and method of explanation should be tailored to different ADM application scenarios to effectively help the public understand the reasoning and logic behind algorithmic decisions. Effective explanations should include, as a minimum: rules and standards applied by ADM systems, key factors and their respective weights in the decision-making process, technical explanations demonstrating how decisions were reached, and a clear outline of comprehensive and meaningful human intervention processes for challenging the decision.

Third, as neither the GDPR nor the PIPL specifies requirements for raising public awareness of the right to human review of ADM decisions, Hong Kong, China should require ADM operators to proactively inform affected individuals that a decision has been made by ADM systems and that they have the right to challenge it. The human intervention process can happen online to improve public accessibility. Additionally, the human review process must be subject to time limits. Where human intervention is denied, delayed, or not provided within the prescribed time limits, the relevant data or privacy protection authority shall automatically intervene to oversee the review process.

4.5. Differentiated Requirements for Public and Private Sectors with Independent Oversight

Under the PIPL, human intervention may be triggered in cases involving ADM, but the application of human intervention and the scope of the right to explanation differ between individual-government and individual-enterprise contexts. This dual-track approach balances national interests with private rights and provides tailored compliance frameworks for both government entities and the private sector. However, concerns have been raised about the misuse of ADM systems by governments for purposes outside the public interest. A higher standard of transparency is therefore required for the public sector. Specifically, when ADM is used for administrative and governmental purposes in social governance, the public's right to know and right to explanation must be robustly protected. Hong Kong, China should mandate that when the government uses ADM to make administrative decisions, it must inform the public in advance of its intended use of ADM and clearly explain the rationale and logic of each ADM-generated decision.

Second, both the PIPL and the GDPR face a common transparency challenge in the private sector: ADM decisions often involve legitimate trade secrets or intellectual property rights. In China, while individuals have the right to request explanations of ADM decisions from both government and private entities, such requests may be rejected if disclosure would infringe the trade secrets or intellectual property rights of the entity or third parties. To resolve this inherent tension, Hong Kong, China should establish an independent third-party professional body to adjudicate disputes where ADM operators invoke "trade secrets" or "intellectual property" as grounds to refuse disclosure requests. This approach would safeguard legitimate commercial interests while ensuring that individuals affected by ADM decisions have access to independent professional oversight to protect their rights. This body could be designated as the "ADM Ombudsperson" and

established as a dedicated unit within the PCPD. The ADM Ombudsperson would be staffed with cross-disciplinary experts in technology, law, and data protection to conduct impartial assessments of ADM decisions, investigate disputes, and resolve grievances arising from ADM use. The PCPD, as an independent statutory body responsible for overseeing compliance with the PDPO, could leverage its existing institutional authority, enforcement powers, and expertise in data protection regulation to incorporate this function.

Finally, to ensure the substantive effectiveness of human review, all ADM systems subject to human oversight requirements must undergo regular independent external audits. These audits should evaluate both the technical performance of ADM systems and the human factors involved in their operation. At a minimum, audits should assess the following aspects: the extent to which human intervention relies on ADM outputs, verifying the genuineness of human involvement in the decision-making process; whether the overall oversight framework, including sufficient time and information for reviewers and clear feedback channels from individuals and regulators, supports human review; whether reviewers receive ongoing training to maintain their critical thinking capabilities, and whether the organization employing the reviewers fosters a culture that encourages challenges to ADM decisions; and whether reviewers can make initial independent judgments before reviewing ADM outputs, mitigating automation bias and cognitive stereotyping.

4.6. Day-to-Day Application, Enforcement and Remedies

Hong Kong, China could draw on the experience of China, which has established an algorithm filing system for public safety purposes. This ex ante mechanism covers all levels of ADM systems and is tailored to the characteristics of each system, such as the number of individuals affected and the significance of the data processing involved. ADM system providers whose services have attributes of public opinion influence must submit full details of their systems to the government and conduct mandatory security assessments prior to market entry. This enables regulators to assess the risks of ADM systems. Furthermore, Hong Kong, China could also learn from the EU AI Act and establish a regulatory sandbox—a controlled environment where regulators and ADM operators can jointly test whether an ADM system may have unfair, unjust, or unlawful impacts on individuals. The regulatory sandbox can also be regarded as market approval prior to an ADM system's application.

In terms of remedies, both the GDPR and the PIPL impose administrative penalties on ADM operators and allow individuals to claim compensation for losses caused by unlawful ADM practices. However, neither regime provides clear and specific remedies for individuals where human intervention finds an ADM decision to be unjust, unfair, or unlawful. Hong Kong, China should therefore enact tailored remedies specifically for the qualified right to human review of significant automated decisions. For example, where human review determines that an ADM decision is unlawful, the law should grant affected individuals the right to reverse decisions and remove negative or false records from ADM systems. Where individuals have suffered damages, they should also be entitled to compensation, with compensation provisions modeled on those under the GDPR and the PIPL. The purpose of such tailored remedies is to make human review meaningful and effective, rather than a purely symbolic gesture.

As noted above, even where aggrieved individuals can claim compensation from ADM operators, proving infringement and quantifying losses remains extremely difficult [11, 22]. In particular, where the designer and operator of an ADM system are separate entities, it can be challenging to determine who bears liability for compensating affected individuals. In addition, ADM system outputs may not be fully controllable or predictable by designers or operators, and losses caused by ADM systems may stem from multiple factors. Critically, only the designers and operators possess knowledge of their technical specifications and limitations. Given this inherent information asymmetry, the burden of proof should be shifted to ADM operators and designers to demonstrate that their

decisions are fair, proportionate, and non-discriminatory. The PIPL has already adopted this approach: where an AI service infringes on users' personal information rights, the personal information handler must compensate for any losses unless it can prove it was not at fault.

Finally, individual enforcement of the right is inherently inefficient, as it only addresses harm on a case-by-case basis, while flawed ADM systems may affect millions of users. Hong Kong, China should therefore draw on Article 80 of the GDPR, which allows individuals to designate qualified non-profit organizations to initiate representative actions on their behalf to enforce data protection rights. Under Article 82 of the GDPR, infringers are liable to compensate all individuals who have suffered loss [23]. Under the PIPL, procuratorates and other authorized entities may file public interest lawsuits, as they are better positioned than individual victims to initiate civil proceedings due to their industry knowledge and expertise. This mechanism relieves individuals of the burden of understanding technical issues and gathering evidence for court proceedings, as legal entities are able to investigate and analyze potential and actual ADM issues, even where the system infrastructure and technical architecture are complex and incomprehensible to the general public.

5. Conclusion

Hong Kong, China 's reliance on non-binding guidelines and sector-specific regulation fails to provide adequate protection against harm caused by algorithmic ADM. Establishing a statutory qualified right to human intervention would help uphold social justice, human dignity, and public trust in AI systems. Drawing from international experiences, Hong Kong, China should adopt a "substantial influence" standard, mandate meaningful human intervention with clear authority and independence, and implement robust enforcement mechanisms and remedies. This approach ensures the right has substantive and meaningful effect while enhancing Hong Kong, China 's position as a leading international financial and innovation hub.

References

1. S. Dashti and S. Ranise, "Tool-assisted risk analysis for data protection impact assessment," in *IFIP International Summer School on Privacy and Identity Management*, Cham: Springer International Publishing, 2019, pp. 308-324.
2. I. Carnat, "Automation as Delegation of Power: Constitutional Constraints on AI Systems for the Administration of Justice," Available at SSRN 5690283, 2025.
3. D. Baldini and K. Francis, "AI Regulatory Sandboxes between the AI Act and the GDPR: the role of Data Protection as a Corporate Social Responsibility," in *CEUR Workshop Proceedings*, vol. 3731, Jan. 2024.
4. S. A. Birahim, "Contesting the algorithm: advancing a right to challenge AI decisions under the GDPR for algorithmic fairness," *Transforming Government: People, Process and Policy*, vol. 19, no. 4, pp. 895-913, 2025.
5. C. Castets-Renard, "Accountability of algorithms in the GDPR and beyond: a European legal framework on automated decision-making," *Fordham Intell. Prop. Media & Ent. LJ*, vol. 30, pp. 91, 2019.
6. L. Colonna, "Teachers in the loop? An analysis of automatic assessment systems under Article 22 GDPR," *International Data Privacy Law*, vol. 14, no. 1, pp. 3-18, 2024.
7. E. Bayamlıoğlu, "The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called 'right to explanation'," *Regulation & Governance*, vol. 16, no. 4, pp. 1058-1078, 2022.
8. Article 29 Data Protection Working Party, "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679," 2018.
9. N. N. Ridzuan, M. Masri, M. Anshari, N. L. Fitriyani, and M. Syafrudin, "AI in the financial sector: The line between innovation, regulation and ethical responsibility," *Information*, vol. 15, no. 8, pp. 432, 2024.
10. A. F. Zumbini, "Regulatory Framework, Procedural Requirements, and Infrastructural Aspects of Automated Administrative Decisions," *Italian J. Pub. L.*, vol. 18, pp. 352, 2026.
11. B. Goodman and S. Flaxman, "European Union regulations on algorithmic decision-making and a 'right to explanation'," *AI magazine*, vol. 38, no. 3, pp. 50-57, 2017.
12. M. Hawath, "Regulating Automated Decision-Making: An Analysis of Control over Processing and Additional Safeguards in Article 22 of the GDPR," *Eur. Data Prot. L. Rev.*, vol. 7, pp. 161, 2021.
13. R. Binns and M. Veale, "Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR," *International Data Privacy Law*, vol. 11, no. 4, pp. 319-332, 2021.

14. J. Hamuľák and A. Kluknavská, "Some Comments on the Unsuitability of the General Data Protection Regulation in the Field of Employment Relations in the Context of Automated Decision-Making," *European Studies–The Review of European Law, Economics and Politics*, vol. 10, no. 2, pp. 203-220, 2023.
15. H. L. Janssen, "An approach for a fundamental rights impact assessment to automated decision-making," *International Data Privacy Law*, vol. 10, no. 1, pp. 76-106, 2020.
16. T. Kirat, O. Tambou, V. Do, and A. Tsoukiàs, "Fairness and explainability in automatic decision-making systems. A challenge for computer science and law," *EURO journal on decision processes*, vol. 11, pp. 100036, 2023.
17. A. Roig, "Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR)," *European Journal of Law and Technology*, vol. 8, no. 3, 2017.
18. D. Sancho, "Automated Decision-Making and Article 22 GDPR: Towards a more substantial regime for solely automatic decision-making," Cambridge University Press, 2020.
19. B. P. Paal, "Article 22 GDPR: Credit Scoring Before the CJEU," *Global Privacy Law Review*, vol. 4, no. 3, pp. 127-137, 2023.
20. T. Davtyan, "An overview of global efforts towards AI regulation," *Bulletin of Yerevan University C: Jurisprudence*, vol. 15, no. 2 (41), pp. 158-174, 2024.
21. F. Thouvenin, A. Fruh, and S. Henseler, "Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right?," *Eur. Data Prot. L. Rev.*, vol. 8, pp. 183, 2022.
22. G. Malgieri and G. Comandé, "Why a right to legibility of automated decision-making exists in the general data protection regulation," *International data privacy Law*, vol. 7, no. 4, pp. 243-265, 2017.
23. S. Wachter, B. Mittelstadt, and L. Floridi, "Why a right to explanation of automated decision-making does not exist in the general data protection regulation," *International data privacy law*, vol. 7, no. 2, pp. 76-99, 2017.