Humanities & Social Sciences Communications

ARTICLE

https://doi.org/10.1057/s41599-025-05411-9 OPEN

# Insights from the Incheon Airport Case in South Korea: balancing public safety and individual rights with global scalability analysis

Haesung Lee[1], Eunsoo Kim[1] & Do Hyun Park[2]✉

This article examines the use of facial recognition technology (FRT) in policing by government agencies, exploring the tensions between public safety and individual rights. While FRT enhances law enforcement capabilities in crime prevention and security, it also raises significant concerns regarding privacy invasion and potential misuse. Based on the *Incheon Airport* case in South Korea, this analysis investigates whether the public interest derived from policing can justify violations of regulations under personal data protection and administrative laws while proposing necessary safeguards. In pursuit of a comprehensive data governance framework for FRT, we are emphasizing the need to establish a more specific and operable data governance structure, strengthen the Privacy by Design principle, and balance security imperatives with individual rights as key alternatives. By shedding light on the Korean case within international discourse, this study underscores the importance of tailoring regulatory frameworks to accommodate local legal traditions and societal values.

[1] Seoul National University, Seoul, Republic of Korea. [2] Gwangju Institute of Science and Technology, Gwangju, Republic of Korea. ✉email: gray@gist.ac.kr

## Introduction

Facial recognition technology (FRT) has emerged as a critical tool for government agencies worldwide, offering advanced capabilities for surveillance and identification. In certain situations, such as searching for missing children or elderly individuals, FRT has proven especially beneficial. Nonetheless, ethical controversies over FRT persist. For example, the Gender Shades study revealed significant racial and gender biases in leading FRT systems (Buolamwini and Gebru, 2018), highlighting the potential for discriminatory outcomes. These contrasting examples illustrate that while FRT may yield substantial societal benefits, it also demands oversight to prevent harm. Thus, striking a balance between harnessing its innovative advantages and mitigating its risks remains paramount, indicating that some sort of regulation would be inevitable.

In the context of artificial intelligence (AI) governance, various jurisdictions have adopted distinct criteria to categorize potentially problematic applications of such technology. For instance, with regard to FRTs that require regulation, while the European Union (EU) often refers to the concept of "high-risk" AI systems, South Korea (Korea) uses a "high-impact" framework to determine which innovative technologies require stricter scrutiny and discipline. Despite these conceptual differences, both approaches seem to underscore the need to protect fundamental rights. The core divergence lies in how each jurisdiction distinguishes between the contexts in which FRT substantially affects individual liberty and in which it does not, as well as how these differences are ultimately enforced.

In high-traffic and multicultural environments such as airports, FRT's appeal is particularly strengthened. Incheon International Airport in Korea (Incheon Airport)—one of the busiest transportation hubs in Asia[1]—illustrates the global relevance of FRT deployment, given its high passenger volume and multinational population. However, employing large-scale FRT for passenger management inevitably raises concerns about potential infringements on fundamental rights due to mass identification. Studying the *Incheon Airport* case can thus shed light on how legal safeguards and public interest intersect, revealing why the implications of FRT may differ depending on the jurisdiction. Even where technological capabilities and associated risks remain largely consistent across jurisdictions, differences in how fundamental rights are conceptualized, interpreted by courts, and valued by society can lead to markedly different regulatory approaches and public discourse surrounding FRT implementation.

In Korea, this tension between technological implementation and individual rights protection became particularly prominent when the Ministry of Justice of Korea decided to outsource the development of an AI system for FRT to private entities. Critics claimed that this initiative violated the Personal Information Protection Act (PIPA), sparking a debate over the extent to which public interests in national security and administrative efficiency can justify the collection of personal data without robust safeguards[2]. In response to these challenges, the authority has recently announced the "AI Privacy Risk Management Model for Safe AI Data Utilization" guideline to encourage self-regulation of AI enterprises (PIPC, 2024)[3]. This initiative arose from the recognition that the reach of AI has extended beyond technological innovation into everyday life, involving large-scale personal data processing that traditional regulatory approaches have struggled to govern. Consequently, privacy threats stand out as a representative risk of AI, prompting calls in Korea for a more robust risk-based approach to AI governance. This controversy thus highlights Korea's nuanced perspective on AI regulation, wherein fundamental rights and public safety considerations are balanced under a framework that diverges from EU standards in both substance and implementation.

On the other hand, Korea has stood at the forefront of digital governance, rapidly incorporating new technologies under relatively robust administrative and legal frameworks. This commitment also reflects the government's longstanding ICT-friendly policies, designed to foster major global players such as Naver and Kakao (Park et al., 2024). From this vantage point, the Incheon Airport incident can be regarded as an example of how Korea's traditional emphasis on promoting ICT industries has materialized in actual public-sector initiatives. The *Incheon Airport* case thereby offers an illustrative lens for global AI discussions: even governments that share commitments to national security and technological innovation may employ substantially different approaches to balancing these objectives with fundamental rights protections, leading to varied regulatory outcomes and enforcement practices. As such, Korea's regulatory strategies can serve as guidance for other countries—including EU member states and the United States—that are simultaneously crafting their own AI regulations while grappling with the questions of individual public safety and fundamental rights.

Methodologically, this study draws on a case-based analysis of *Incheon Airport* case, selected for its typicality in showing how governments adopt FRT in real-world, high-volume, and multicultural environment. We employ legal text analysis and comparative legal methods. Our data sources include legal documents (e.g., PIPA), media reports, government publications, international standards on FRT, privacy rights, and state obligations. By exploring the Korean regulatory framework of FRT and comparing it with legal regimes abroad, we aim to reveal how public safety considerations can influence the extent and nature of fundamental rights protections in the context of AI-based policing tools.

This article thus assesses the policy implications of FRT in law enforcement by examining whether and how public safety can justify infringements on fundamental rights and how Korea's legal system—particularly in a global hub like Incheon Airport—navigates these issues. By contextualizing the Korean experience within broader international discussions, this study aims to suggest future legal reforms and transnational policy-making, ensuring that AI-driven public safety measures should not undermine fundamental human rights.

## Facial recognition technology and its regulatory framework

FRT is a probabilistic technology used for automated personal authentication and verification based on facial features. Regardless of the hardware or software employed, an FRT system encompasses the following stages: first, facial images are extracted from various data sources and used as input data ("image capture"); next, the system detects the face in the captured images and identifies a template of the human face ("face detection"), focusing on distinctive features such as points or lines; finally, the template is compared with a database ("authentication or verification") (Karaboga et al., 2022). FRT serves two primary functions: *authentication*, which confirms the identity of a specific individual, and *verification*, which identifies an individual within a specific area, range, or database. Authentication entails using a pre-stored biometric template for one-to-one matching. Verification is a one-to-many process that identifies an individual after capturing their face and creating a biometric template (EDPB, 2023).

A study in 2019 revealed that over half of the world's democratic nations have integrated AI surveillance systems into their public-sector operations, with even more prevalent adoption in authoritarian regimes (Feldstein, 2019). Despite this widespread use, countries diverge considerably in how they regulate or

**Table 1 Use of FRT under Article 5 of EU AI Act.**

| | |
|---|---|
| • Prohibited use of FRT for untargeted scraping of facial images. | The placing on the market, the putting into service for this specific purpose, or use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage is prohibited. |
| • Prohibited use of FRT for 'real-time' and remote law enforcement systems. | The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement is prohibited. |
| • Exceptional use of FRT allowed for 'real-time' and remote law enforcement systems. | (i) for the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as searching for missing persons;<br>(ii) for the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;<br>(iii) for the localization or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation, prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years. |

oversee FRT. At one end of the spectrum, countries such as China and Russia either lack robust FRT-specific regulations or maintain opaque surveillance policies (Polyakova and Meserole, 2019). At the other end, actors like the EU and Korea have codified regulatory initiatives, although these differ in both intensity and content.

With the introduction of the AI Act, the EU has established a pioneering legislative framework to address the diverse risks that AI systems, particularly those deployed in surveillance, may pose to its citizens. The AI Act employs a risk-based approach that categorizes AI systems into four tiers—unacceptable, high, limited, and minimal risk. This framework is designed to ensure that AI systems posing an unacceptable or high risk, such as those used in FRT, receive stringent oversight, thereby preventing disproportionate intrusions on individual rights. By mandating specific controls, particularly regarding high-risk applications, the EU seeks to balance innovation with robust protections for fundamental rights[4].

In contrast, Korea's AI Framework Act, which was legislated by the National Assembly of Korea on December 26, 2024, adopts a "high-impact" perspective. Under this approach, "high-impact AI" is defined as AI systems that may have significant impacts on or pose risks to human life, physical integrity, or fundamental rights—spanning sectors such as energy, healthcare, public safety, and more. Although this concept parallels the EU's "high-risk AI," Korea's use of the more neutral term "impact" reflects a traditional policy focus on promoting ICT innovation and economic growth. In summary, although both paradigms seek to protect the public interest and prevent excessive restrictions on fundamental rights, they are rooted in different policy traditions, which may result in divergent regulatory outcomes when applied to FRT.

Under Korea's AI Framework Act, the only "high-impact AI" clause explicitly referencing FRT concerns the analysis and use of biometric information for criminal investigation and arrest. FRT may also fall under "other areas" designated by presidential decree as having a significant impact on the safety of human life and physical integrity or the protection of fundamental rights. However, in the current absence of subordinate legislation and guidelines, significant legal uncertainty remains. As a result, in practice, FRT regulation still hinges on the PIPA[5], which has been criticized by several agencies and civil society groups for inadequately safeguarding individual liberty (Lee, 2024). For example, the National Human Rights Commission of Korea has repeatedly cautioned against the unbridled use of FRT by highlighting the risks of unlawful mass surveillance and invasive data collection. On 12th January 2023, the Commission formally recommended legislative measures to ensure the responsible deployment of FRT while respecting fundamental rights (NHRCK, 2023).

Although it remains difficult to look beyond the fragmented regulatory system for FRT in Korea, the discussions on this topic have notably materialized within the EU. For instance, the EU introduced a risk-based approach to regulating FRT under the AI Act, which categorizes certain uses of FRT as prohibited (e.g., untargeted real-time surveillance) and the other FRT uses as high-risk subject to stringent compliance obligations. The in-depth analyses of FRT's legislative landscape and best practices can be found in the European Parliament's Regulating Facial Recognition in the EU (Madieg and Mildebrath, 2021) and the European Data Protection Board's Guidelines on Facial Recognition Technologies in the Area of Law Enforcement (EDPB, 2023). For instance, the recently enacted EU AI Act formalizes an unacceptable risk in Article 5 based on risk-based regulatory approach as Table 1.

Because FRT often processes vast amounts of personal data, it also falls under data protection regulations. In the EU, the General Data Protection Regulation (GDPR), which came into effect in 2018, governs personal data processing, including automated processing. While public entities may receive limited exemptions for criminal law enforcement (GDPR Art. 2(2)(d)), any processing of personal data for FRT beyond this scope must comply fully with GDPR principles—most notably "privacy by design and by default" (GDPR Art. 25). Moreover, the GDPR features robust enforcement mechanisms, including the administrative fines of up to four percent of an organization's global annual revenue (GDPR Art. 83), which reflects the "Brussels effect" by incentivizing global adherence to EU data protection standards (Bradford, 2020).

The Clearview AI controversy illustrates the EU's view on unlawful FRT practices. Clearview AI, a company specializing in FRT that scours publicly available sources for training data, collected facial images from various online platforms without user consent, prompting regulatory backlash in multiple jurisdictions. In May 2022, the UK's Information Commissioner's Office (ICO) imposed a £7,552,800 fine on Clearview for breaching GDPR (ICO, 2022). Such an enforcement underscores that even if a government entity justifies the use of FRT based on public safety or security imperatives, it must still observe stringent data protection standards and fundamental rights requirements.

Alongside the principle of 'Privacy by Design' (PbD), the data minimization principle—enshrined as a broader requirement under GDPR Article 5(1)(c)—stipulates that data collection be strictly limited to what is necessary for the intended purpose, thereby further reinforcing the goal of protecting personal data.

In line with the data minimization principle outlined in Article 3(1) of the PIPA, Korea has also begun to incorporate PbD principles into guidelines and enforcement decisions issued, which are less formalized than the EU. This concept is crucial in assessing when public safety can legitimately override privacy rights. By embedding PbD and data minimization principles from the outset, governments can effectively demonstrate that any restrictions on individual rights are strictly proportionate to what is necessary to achieve legitimate security goals.

To summarize, in the EU, "PbD" is explicitly encouraged (as reflected in the GDPR) to embed data protection safeguards, including data minimization, from the early stages of AI design and development. In contrast, while Korea's approach seeks to align with international standards, it is still evolving in terms of how these design principles should be practically operationalized, particularly in the context of biometric technologies like FRT. Moreover, Korea's "high-impact" framework, which seems to be more neutral in tone than the EU's "high-risk" regime, is marked by conceptual vagueness; this abstractness increases the likelihood that it will be interpreted in a pro-market fashion, much like its traditional ICT regulation[6]. This situation underscores the inherent challenge of balancing the promotion of technological innovation with the needs for robust oversight to protect fundamental rights.

This leads to the following question: when does public safety sufficiently outweigh individual rights? In the EU, the AI Act narrows that scope by strictly limiting real-time FRT usages to a few exceptional scenarios. Korea's approach hinges on the interpretation of "high-impact," a rather abstract concept, which may allow agencies to argue that security priorities justify the broader adoption of FRT. The *Incheon Airport* case (explored further in this study) illustrates how divergences in regulatory regimes manifest in practice, giving rise to ongoing controversies over privacy: while the authority recognized the security rationale for large-scale data collection, many voices in the public debate and legal communities have questioned whether those measures unduly threaten individual liberty. Examining this scenario is still instructive for future AI regulations, as it demonstrates the potential risks to individual rights when personal data is extensively processed by AI systems. Absent rigorous oversight, even ostensibly legitimate public safety measures can jeopardize fundamental rights.

## The Incheon Airport Case

**1. Background**. The Ministry of Justice of Korea, in collaboration with the Ministry of Science and ICT of Korea, had been building an AI system for identification and tracking to enable immigration control from 2019 to 2022. Facial images and personal information such as nationality, gender, and age of more than 170 million individuals, including Koreans and foreigners, which had been collected during the immigration process became accessible to private entities entrusted with establishing the system (KBS News, 2021). Figure 1 illustrates how personal information is collected, stored, processed, and eventually screened in the AI system training workflow.

In October 2021, several Korean media reported that the AI identification and tracking system might have violated the PIPA by granting private entities extensive access to personal data. After performing an investigation from December 2021 to April 2022, the authority found the system "generally legitimate" but noted several minor violations of the PIPA requirements (PIPC, 2021a).

**2. Legitimacy of facial image processing in the *Incheon Airport* Case**. In assessing the legality of FRT use, the first issue is whether the collection of facial images from the Incheon Airport passengers fell within the scope of the PIPA. The Personal Information Protection Commission of Korea (PIPC), the national authority responsible for overseeing personal data protection, concluded that while facial images are considered personal information, data derived from such images through technical methods, such as feature extraction, qualifies as biometric information. As such, it is classified as 'sensitive information' (Enforcement Decree of the PIPA Art. 18), which is a more sensitive category and is subject to stricter safeguards than general personal information. This interpretation is consistent with the standards set forth in the PIPC's Biometric Information Protection Guideline, issued in September 2021 (PIPC, 2021b), as illustrated in Figure 2. Under both the PIPA and the guideline, where facial images are deemed sensitive information, personal information controllers are prohibited from processing those data unless exceptional circumstances are applicable (PIPA Art. 23(1)).

Under the PIPA, processing of sensitive information is prohibited by default but allowed under two exceptional circumstances: (i) when personal information controllers obtain the consent of data subjects or (ii) when other statutes require or permit the processing of sensitive information. In the case of *Incheon Airport*, because data subjects' consent was not obtained, the PIPC had to determine whether the processing could be justified based on the second circumstance. The data processing in question primarily concerned immigration control, and upon review of the 'Immigration Act', the PIPC affirmed that it provides a legal basis for the processing of sensitive information. According to the PIPC, provisions of the Immigration Act related to the collection of biometric information from both nationals and foreigners during immigration inspections may serve as a legal basis for requesting or permitting the processing of sensitive information under Article 23(1)(2) of the PIPA.

The second issue is whether using the collected facial images to develop an AI system for immigration control constitutes processing within the scope of the purpose when the data is collected. The Immigration Act stipulates that the purpose of immigration affairs is to ensure safe border control (Art. 1) and that entry or departure inspections may be substituted with those using an informatization device (Arts. 3(2) and 6(3)). Based on these provisions, the PIPC concluded that the AI facial recognition system for advanced border control aligns with the purpose of the Immigration Act and that the use of facial images to train the AI system falls within the scope of the originally intended processing purpose at the time of data collection.

However, the legal status of entrusted private entities was still unclear. The PIPA delineates two conditions under which personal information can lawfully be transferred from a personal information controller to a third party: (i) when the controller provides personal information to a third party (Art. 17); or (ii) when the controller entrusts the processing of personal information to a third party (Art. 26). In the *Incheon Airport* case, the question is whether the Ministry of Justice of Korea's behavior fell under 'the provision of personal information' or 'entrusting the processing of personal information' to a third party.

The Supreme Court of Korea ruled that in order for a third party responsible for personal information processing under the PIPA to be a direct stakeholder under Article 17 rather than an entrusted party as per Article 26, the third party must have an 'independent interest' apart from the compensation for entrustment. In addition, the court specified that whether a specific behavior constitutes provision or entrustment to a third party is determined by the purpose and method of acquiring personal information, presence of compensation, actual management and supervision of the trustee, impact on the necessity of protecting the personal information of the data subject, and determining who is the de-facto user of such personal information (Supreme

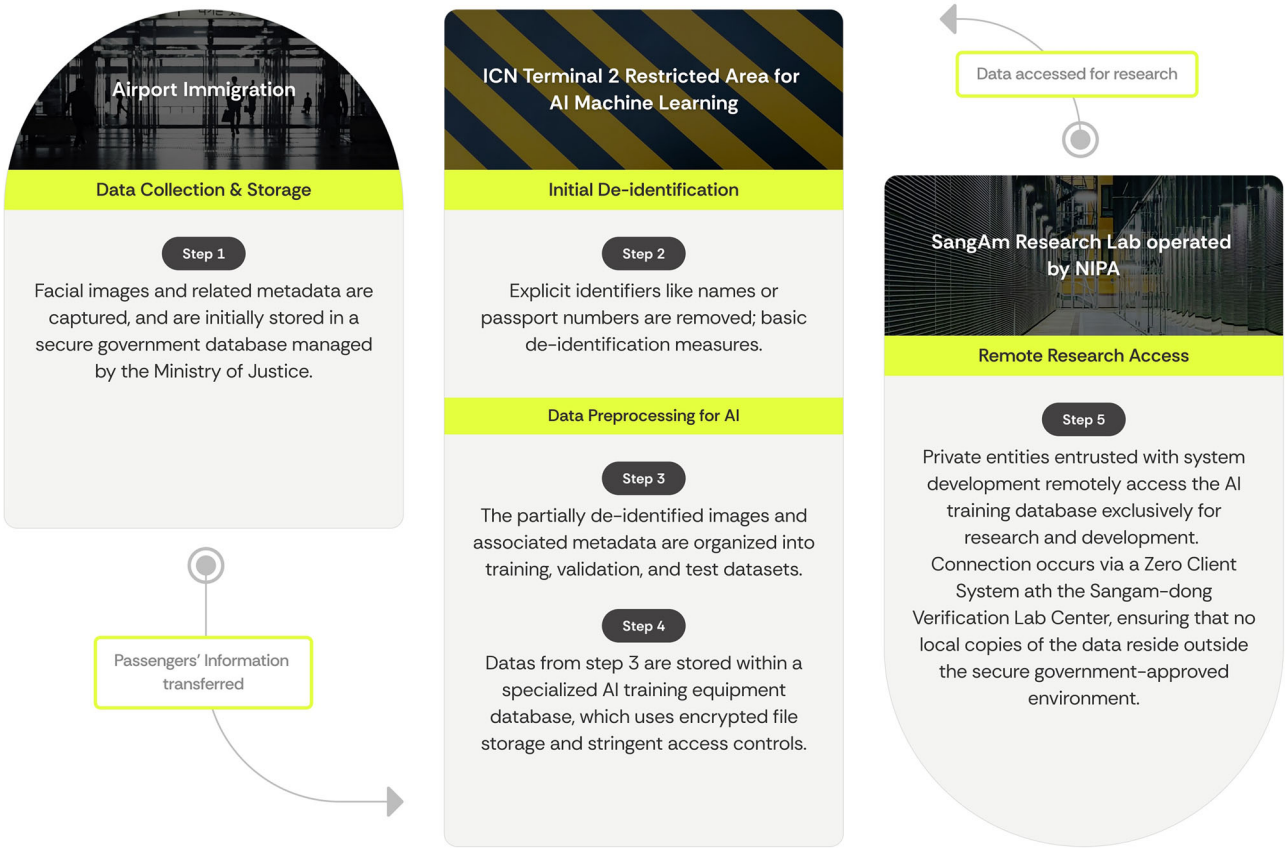


**Fig. 1** Information processing workflow for AI model in the Incheon Airport case.

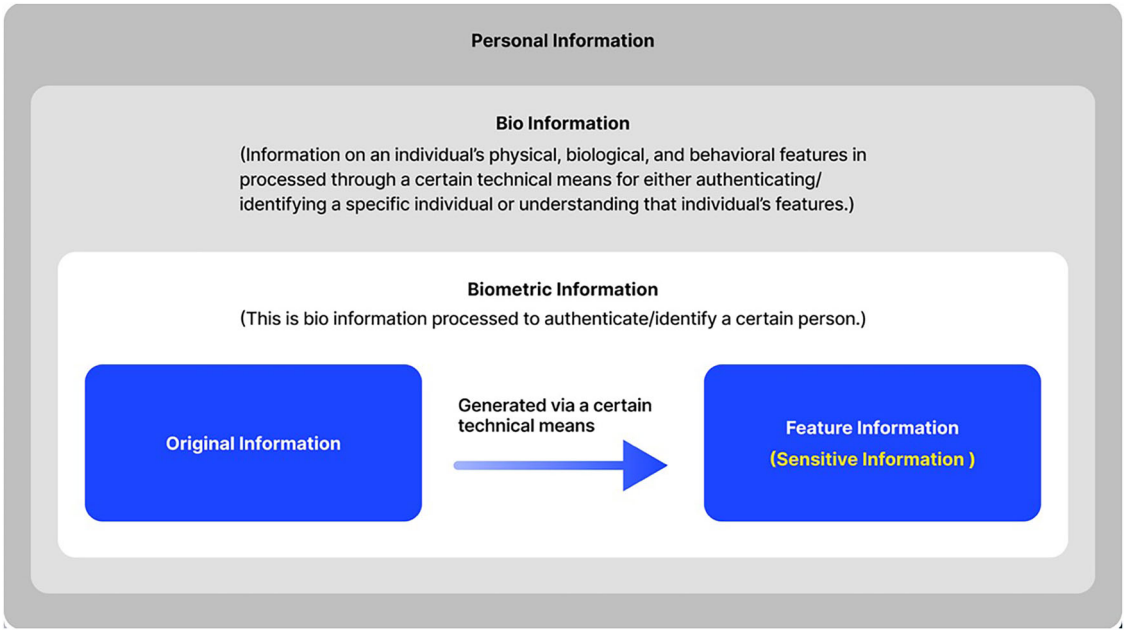


**Fig. 2** Diagram of the concepts related to biometric information.

Court of Korea, 2016). Based on this legal doctrine, the PIPC concluded that the outsourcing in this case should be regarded as entrustment, as there was no independent interest that aligned with the original purpose and scope of information collection.

Article 26(2) of the PIPA stipulates that when a personal information controller entrusts personal information processing, they must disclose the details of the entrusted affairs and the entity that processes the personal information so that a data subject can easily recognize them at any time. However, in this case, the Ministry of Justice of Korea, the entity that entrusted the collection of personal information, failed to fulfill this obligation. Consequently, the PIPC imposed a fine of 1 million KRW (approximately 700 USD) on the Ministry of Justice of Korea for violating the disclosure obligation of the PIPA.

**3. Regulatory gaps in the *Incheon Airport* Case**. As illustrated by the *Incheon Airport* case, the PIPA makes several limitations on safeguarding fundamental rights when processing personal information through FRT. Similar to the GDPR, Articles 3(1) and 3(4) of the PIPA explicitly delineate the principle of data minimization and a risk-based approach. However, these principles are not specifically stipulated, and the PIPA does not include a PbD requirement akin to Article 25 of the GDPR. Furthermore, the PIPA fails to adequately differentiate between "high-impact" AI applications and those that pose lesser risks. The absence of systematic criteria for evaluating potential harms could lead to a regulatory vacuum, thereby hindering effective data protection practices and undermining the balance between public safety and individual rights.

The regulatory gaps evident in the *Incheon Airport* case exemplify the divergent approaches to privacy regulation in Korea and the EU, reflecting underlying cultural and institutional differences that shape each jurisdiction's understanding of the relationship between individual rights and public interests. Korea's regulatory framework is deeply influenced by its state-led economic development model, which has prioritized national competitiveness and technological innovation since the 1960s. This legacy of developmental state has fostered a regulatory culture in which privacy protection is viewed through the lens of balancing individual rights against collective goals of economic development. The Korean approach maintains governmental flexibility to adapt AI regulations in response to technological advances and industrial demands, reflecting a belief that the state should play a leading role in coordinating competing interests to achieve socially optimal outcomes. The *Incheon Airport* case demonstrates how such a flexible regulatory approach can create regulatory gaps where emerging technologies like FRT systems are deployed for purposes of public safety and operational efficiency.

In contrast, the EU's rights-based approach to privacy regulation emerges from its post-World War II commitment to protecting individual dignity and democratic values as a response to historical experiences with totalitarian regimes. The EU treats privacy as a fundamental right enshrined in the Charter of Fundamental Rights, thereby shaping a regulatory philosophy in which personal data protection is positioned as constraints on economic activity, rather than as a value to be balanced alongside it. This rights-first approach manifests in the GDPR's emphasis on individual autonomy, explicit consent, and strict limitations on data processing, with severe penalties that are applicable without regard to potential economic benefits. This difference reflects distinct social contracts that Korea's approach regards rights as interests to be balanced against collective development goals, whereas the EU treats them as inherent limitations on state and corporate power. As a result, regulatory gaps like those observed in the *Incheon Airport* case are less likely to occur under the EU's regulatory frameworks.

The discussion above has focused on the regulatory gaps within Korea's legal framework for FRT, particularly from the perspective of the PIPA. However, while the AI Framework Act is not yet effective, the PIPA is not the sole law within the Korean legal system that can be applied to regulate FRT; other provisions of traditional or newly enacted administrative regulation can also play a role. Therefore, even if the PIPA presents inherent limitations, context-specific regulation for FRT may still be applied in accordance with general administrative regulatory principles and specific rules. The following chapter examines this issue in detail.

## Legal challenges of Policing with FRT in South Korea

Korea's administrative law framework shares its doctrinal foundations with continental European systems. However, in the context of fundamental rights, Korea exhibits significant divergence in practice – especially in how surveillance technologies such as FRT are deployed for policing. This section evaluates key legal challenges under Korean administrative law by examining how regulations governing FRT interact with and are constrained by constitutional principles, particularly statutory reservation and proportionality. This structure helps illuminate the gaps and tensions between technological enforcement practices and the protection of individual rights in the Korean legal context.

**1. Principle of statutory reservation**. According to Korean administrative law, "policing" refers to public agencies' administrative actions aimed at preventing risks to public safety, maintaining order, and resolving disturbances (Chung, 2024). These actions constitute administrative investigations (Lee et al., 2020) and are principally carried out by the National Police Agency under the Ministry of the Interior and Safety of Korea (Government Organization Act Art. 34(5)). When private entities perform policing functions on behalf of the state—as in the *Incheon Airport* case—their activities are likewise treated as administrative actions under the law.

Doctrine of legal basis Article 37(2) of the Constitution of Korea allows for restriction of individual liberty only by law for national security, public order, or public welfare. This principle is operationalized through statutes such as the General Act on Public Administration (Art. 8) and the Framework Act on Administrative Regulation (Art. 4), which require that administrative measures limiting individual rights be based on clear legislative authorization. The Constitutional Court reinforced this position, demanding heightened specificity in areas affecting fundamental rights (Constitutional Court of Korea, 1999).

Despite these safeguards, as illustrated by the *Incheon Airport* case, a particularly relevant issue arises concerning the so-called 'general authorization clause'—an abstract legal provision that grants broad discretionary powers without clearly defined conditions or scope. This concept has its roots in the past police administrative laws (Polizei- und ordnungsrechtliche Generalklausel) of Germany, and serves as the basis for permitting administrative actions without detailed, specific statutory provisions. However, the use of general authorization clause has provoked academic debates in Korea. While some scholars argue that such clauses do not satisfy the constitutional requirement of statutory specificity (Cho, 2018), others suggest the clause serves as a practical mechanism to overcome the inflexibility inherent in a formalistic interpretation of the rule of law (Lee S, 2018)[7]. This legal ambiguity continues to fuel controversy over the legitimacy of such practices in contexts where they may potentially violate fundamental rights, such as biometric surveillance.

Policing with FRT under general authorization clauses became controversial in Germany following the use of a FRT by Hamburg police during the violent protests at the G20 Summit in 2017. The police tracked suspects using facial recognition software Videmo 360 by analyzing facial images obtained through CCTV and the Internet (Montag et al., 2021), leading to concerns over the legality of the measure. The Hamburg Data Protection Authority (DPA) argued that it violated the principle of statutory reservation and ordered the deletion of the biometric database. In response, the Hamburg police contended the use of FRT was lawful under the general authorization clause.

Initially, the Hamburg Administrative Court (VG) overturned the Hamburg DPA's order. Upon appeal, the Hamburg Higher Administrative Court (OVG) concluded that the legal dispute was resolved because the database had already been deleted (VG Hamburg, 2019). Thus, the court did not explicitly rule on the role of the general authorization clause in this case, but given the

context, investigations are likely to be widely accepted in German law under the clause. In addition, since the case concerns the investigative process following police administration actions, it could be argued that the principle of statutory reservation may also apply to policing activities conducted under a general authorization clause.

However, this reasoning and conclusion would be problematic in Korea because it conflicts with the need to adhere to the strict principle of statutory reservation during the investigative process. In criminal proceedings, using FRT for investigation purposes without the consent of a suspect is regarded as a compulsory investigation, thereby invoking the principles of legality (Criminal Procedure Act Art. 199) and the warrant system (Constitution Arts. 12(1) and (3)). If an investigation is conducted in violation of due process (Constitution Art. 12(1)), the evidence obtained must, in principle, be considered inadmissible under the exclusionary rule for illegally obtained evidence (Criminal Procedure Act Art. 308-2). Considering these provisions, it would be difficult to claim that compliance with the statutory reservation principle can be upheld solely by the existence of a formal authorization clause, without examining the substantive legality of the investigation content and procedures.

The subsequent question is whether the principle of statutory reservation can be leniently applied and justified solely by the general authorization clause, given that police administrative actions are carried out prior to the investigation process. The key point of this issue should be the extent to which a policing activity restricts the citizens' fundamental rights, and in many cases, policing involving FRT is conducted without the voluntary cooperation of the individuals concerned. Therefore, the principle of statutory reservation should be strictly applied beyond the general authorization clause, even during administrative policing, which precedes the investigation stage.

Of course, it would be unreasonable and impractical to require strict adherence to the principle of statutory reservation in all cases of policing activities. Since the principle aims to protect fundamental rights, it is not necessary to extend the same standards to those that does not significantly restrict fundamental rights. To address this challenge, compliance with the principle of statutory reservation should be proportional to the degree of restriction on fundamental rights. For instance, in the case of a mandatory investigation without consent, it is reasonable to consider that compliance with the principle of statutory reservation requires a specific legal basis. On the contrary, for policing activities involving voluntary cooperation of individuals, it may be sufficient to attenuate the specificity of authorization and rely on a general authorization clause.

In accordance with this standard, policing activities involving the processing of personal information require more specific legal authorization, as they are likely to restrict the liberty to act and the right to self-determination of personal information. This is supported by the principles of the PIPA, which require that the purpose of personal information processing be specified and limited to that scope (PIPA Arts. 3(1) and 3(2); Kim, 2014b), and impose similar legal duties particularly on administrative authorities (PIPA Art. 5). These principles—purpose specification and limitation—are recognized under the principle of void for vagueness in the Constitution and provide meaningful insights when evaluating the specificity of general authorization clauses. In addition, this reasoning is further strengthened if the information processed during policing is classified as sensitive information beyond general personal information (Lee, 2023). Nevertheless, the current legal framework in Korea does not contain specific authorization provisions for the use of FRT in policing — let alone provisions addressing its use when it constitutes personal or sensitive information (Kim, 2014a).

**2. Principle of proportionality**. The PIPA obliges personal information controllers to manage personal information proportionately to the risks posed based on Article 3(4). In addition, Article 33 establishes an impact assessment system for this purpose, and subordinate standards mandate risk analysis to prevent data breaches. While these provisions suggest a robust framework for a risk-based approach, the actual application, as demonstrated by the *Incheon Airport* case, reveals inconsistencies in risk management. Particularly, it does not seem to adequately consider the differences in the risks associated with processing personal and sensitive information.

In the case of *Incheon Airport*, the PIPC avoided the dichotomy of categorizing all biometric information as either personal or sensitive information. The PIPC distinguished the generated feature information from the original facial images collected, classifying only the former as sensitive information, while the latter was treated as personal information (PIPC, 2021a). Therefore, at first glance, it appears that the risk-based approach has been effectively applied in the case of *Incheon Airport*.

By definition, the PIPA's distinction between personal and sensitive information should reflect the fact that data subjects are at a higher risk from a breach of sensitive information than of personal information. In this regard, the PIPA provides only two legal justifications for collecting and using sensitive information, while there are seven legitimate options for collecting and using personal information, as illustrated in Table 2. Thus, at first glance, the PIPA's regulations appear to effectively fulfill the intent of its risk-based approach; however, two main issues arise in this regard.

Under a risk-based approach, a specific category of personal information classified as 'sensitive' must be safeguarded by a more stringent protection mechanism (Tang, 2024). However, although not applicable in the *Incheon Airport* case, the intent of the PIPA to differentiate between personal and sensitive information through a risk-based approach could be effectively nullified, as Articles 15(1)(1) and 23(1)(1) can be readily fulfilled through a single consent. Even if FRT offers significant benefits, a proper risk-based regulatory system should assess the specific context of its use, carefully weighing the magnitude and nature of its countervailing risks and imposing more nuanced controls. In its current form, the PIPA does not seem to fully achieve this balance, as its reliance on broad legislative justifications may undermine the intended differentiated legal requirements and obligations between personal and sensitive information.

Furthermore, similar issues may arise with another exception regarding the permissibility of processing sensitive information: whether such processing is authorized by other applicable laws. Article 23(1)(2) does not clearly define what constitutes request or permission for the processing of sensitive information under another law, leaving uncertainty for justification in an overly abstract manner. In contrast, Articles 15(2) through 15(7), which describe the requirements of permitting the processing of personal data without consent, are more detailed. Consequently, there appears to be little distinction between the processing of personal and sensitive data when such processing without consent is authorized by other applicable laws. This, in turn, may result in a regulatory gap that fails to adequately reflect the differing levels of risks associated with personal and sensitive information.

In contrast, the GDPR, which has significantly influenced the recent amendment of the PIPA, not only stipulates that the processing of personal data for public interest (Art. 6(1)(e)) must incorporate comprehensive safeguards, but also requires that special categories of data (Art. 9(2)(g)) be processed only when necessary for substantial public interest—supported by additional controls under Article 9(4). Therefore, although both the GDPR

**Table 2 Types of lawful processing of personal and sensitive information under the PIPA.**

| Sensitive Information (Article 23(1)) | Personal Information (Article 15(1)) |
|---|---|
| | 1. Where consent is obtained from a data subject. |
| 2. Where other statutes or regulations require or permit the processing of sensitive information. | 2. Where special provisions exist in other statutes or it is unavoidable due to obligations under statutes or regulations.<br>3. Where it is unavoidable for a public institution's performance of work under its jurisdiction as prescribed by statutes or regulations, etc.<br>4. Where it is necessary to take measures at the request of a data subject in the course of performing a contract concluded with the data subject or concluding a contract.<br>5. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party.<br>6. Where it is necessary to attain the legitimate interests of a personal information controller, which such interest is manifestly superior to the rights of the data subject.<br>7. Where it is urgently necessary for the public safety and security, public health, etc. |

and PIPA aim to implement the risk-based approach, the PIPA's framework tends to exhibit a form of "downward harmonization" in protecting fundamental rights, compared to the GDPR's more rigorous approach of "upward harmonization." Reliance on broad legislative justifications provided by the general authorization clause—such as the Immigration Act—may inadvertently undermine the proportional safeguards for policing through FRT.

## Toward a comprehensive data governance framework for FRT

The *Incheon Airport* case underscores the profound tension between public safety and the protection of fundamental rights as technology advances. Korea's existing regulatory framework, including the PIPA and administrative law, is inherently vulnerable in light of the constitutional principles of statutory reservation and proportionality. Furthermore, the forthcoming AI Framework Act, with its ambiguous "high-impact" classification and a traditionally pro-market approach rooted in Korea's ICT policies, is likely to yield lax regulation as well. As a result, regulatory gaps in safeguarding fundamental rights may need to be addressed solely through self-regulatory guidelines, which must, at a minimum, incorporate the core principles of PbD and data minimization, in line with international standards. The followings are key takeaways to consider moving forward.

**1. Establishing more specific, operable data governance**. A robust data governance framework is essential for ensuring that FRT systems deliver public safety benefits while rigorously protecting individual privacy. To achieve this balance, concrete measures—grounded in the risk-based approach and data lifecycle management principles—should be implemented. First, mandatory data minimization should be enforced so that only the essential biometric data required for specific functions are collected and processed, reducing unnecessary disclosure. In addition, establishing clear data classification standards is critical; by categorizing data based on its sensitivity, regulators can implement differentiated controls tailored to each risk level.

Second, policy measures that strengthen data transparency and accountability are equally vital. For instance, public institutions could be required to disclose metadata about FRT databases—such as collection times, purposes, and retention periods—thereby providing stakeholders with critical insights into data practices. In parallel, technical safeguards such as robust encryption protocols and role-based access controls should be implemented to prevent unauthorized access. Additionally, clear data retention policies—including automated deletion schedules (e.g., six months after case resolution)—are essential to mitigate the risks of long-term data exposure and misuse.

Furthermore, to foster a truly privacy-centric approach, Korean policymakers should consider incorporating international standards such as ISO 27701 into procurement and operational guidelines. This would promote consistency in privacy practices and create a more transparent and accountable system for handling biometric data. In addition, establishing rigorous data lifecycle management practices—including explicit retention schedules, regular audits, and effective citizen grievance channels—would enhance the overall integrity of FRT systems. Given that existing statutory regulations remain insufficient, filling these gaps through self-regulatory guidelines would be required.

Finally, establishing public engagement mechanisms—such as dedicated citizen grievance channels on government websites—can empower individuals to report concerns and seek redress, thereby reinforcing public trust in the system. This is crucial because existing data governance structures are insufficient to effectively address individual complaints and provide redress following violations of fundamental rights. By integrating these specific and operable measures, a comprehensive data governance framework can be established—one that effectively balances innovation, public safety, and the protection of fundamental rights.

**2. Strengthening "Privacy by Design" Principle**. A key element in enhancing privacy is the systematic adoption of PbD principles across the entire lifecycle of FRT systems. PbD, as explicitly stipulated in the GDPR, mandates that data protection safeguards be integrated into systems from the outset. This includes not only default privacy settings but also the principle of data minimization—ensuring that only the necessary data is collected and processed. Such proactive measures are designed to ensure that privacy is not an afterthought, but a fundamental component of system design.

In contrast, while Korea's regulatory framework is theoretically aligned with international standards, its practical implementation of PbD—particularly in the area of biometric technologies like FRT—remains underdeveloped. Korean legal systems often fall short of fully operationalizing these principles. To fill this gap, Korea's forthcoming AI Framework Act would present a critical opportunity to mandate specific PbD requirements for FRT systems. Drawing from Article 25 of the GDPR, Korea could require FRT systems to extract only the essential facial features needed for their designated function – such as geometric facial landmarks rather than full facial images – thereby reducing the volume of personal data processed. This technical refinement should be coupled with impact assessments conducted before FRT deployment, similar to Article 35 of the GDPR's Data Protection Impact Assessment requirements.

In particular, ISO 31700, published in February 2023, can serve as a practical blueprint for adapting these principles to Korea's regulatory environment. This standard transforms Ann Cavoukian's original seven PbD principles into 30 comprehensive requirements divided between high-level guidance (ISO 31700-1) and concrete implementation examples (ISO 31700-2). For Korean FRT systems by state, ISO 31700 could be operationalized through several specific measures such as implementing automated data deletion schedules, incorporating real-time consent mechanisms for non-essential uses beyond public safety. Furthermore, it is worth considering their incorporation into the AI Framework Act's fundamental rights impact assessments for high-impact AI systems (Article 35). Embedding PbD requirements into such evaluations would not only align Korea with global best practices but also strengthen the normative coherence of its data governance in high-stakes domains such as biometric surveillance and FRT-based policing.

**3. Balancing security imperatives and individual rights**. It is clear that FRT can offer substantial benefits to public safety and security. It has been effectively employed to locate missing persons, identify suspects in criminal investigations, and prevent potential security threats. However, these advantages come with serious concerns over privacy invasion, threats to civil liberty, and mass surveillance. Unchecked deployment of FRT can lead to pervasive data collection and unwarranted intrusions into individual lives, thereby eroding fundamental rights such as privacy, data protection, and human dignity.

Importantly, while both Europe and Korea ostensibly aim to protect these fundamental rights through their regulatory approaches, the underlying legal frameworks and societal values differ significantly. In Europe, the regulations like the GDPR and the EU AI Act incorporate robust measures—such as explicit PbD principles and data minimization requirements—to ensure that any deployment of FRT is subject to strict and risk-based oversight. Conversely, Korea's framework, with its "high-impact" classification of AI systems, reflects a historically pro-market orientation that prioritizes ICT innovation and economic growth. This results in a regulatory approach where the protection of fundamental rights is often less clearly defined and rigorously enforced, despite both regions' stated commitments to safeguarding individual liberty.

These divergent legal and cultural contexts lead to differing outcomes in practice. In Europe, the well-articulated risk-based framework tends to impose stringent oversight on FRT applications, ensuring that any intrusion into personal privacy is proportionate to its public safety benefits. In contrast, Korea's more ambiguous "high-impact" categorization can leave significant regulatory gaps, potentially allowing extensive data collection under the guise of public interest. Consequently, even when both regions base their regulatory approaches on fundamental rights, the de-facto protection afforded to individuals may vary markedly. This discrepancy underscores the importance of tailoring regulatory strategies to local legal traditions and societal expectations, ensuring that the pursuit of technological advancement should not be performed at the expense of essential human rights.

## Concluding remarks

In conclusion, the *Incheon Airport* case represents a pivotal moment in the study of AI-integrated FRT since it offers a concrete example of the risks and challenges inherent in deploying such technologies. This case demonstrates how seemingly similar risk-based regulatory approaches can yield markedly different outcomes depending on the cultural, institutional, and historical contexts that shape their implementation. The regulatory gaps identified in Korea's handling of FRT deployment reveal the complicated interplay between technological innovation, privacy protection, and democratic accountability in contemporary AI governance.

The comparative analysis between Korea's developmental state approach and the EU's rights-based framework illuminates fundamental differences in regulatory philosophy that extend beyond technical specifications. While both Europe and Korea ostensibly seek to protect individual rights through stringent data protection and surveillance regulations, the *Incheon Airport* case reveals that Korea's "high-impact" framework—characterized by its abstract criteria and a pro-market orientation—may result in protections that differ from, and are potentially weaker than, the EU's more clearly delineated "high-risk" model. These differences underscore that the regulation of AI-driven technologies is not solely a technical or procedural issue; rather, it is deeply intertwined with the cultural, legal, and historical context of each jurisdiction.

The systematic adoption of PbD principles across FRT system lifecycles offers a pathway toward reconciling these tensions. As demonstrated through the operationalization of ISO 31700 standards and Article 25 of the GDPR requirements, the technical measures such as data minimization, automated deletion schedules, and mandatory privacy impact assessments can be adapted to different regulatory environments while maintaining core privacy protections. Korea's forthcoming AI Framework Act presents a critical opportunity to embed these concrete safeguards into its regulatory architecture, potentially addressing the gaps revealed by the *Incheon Airport* case.

The implications of Korea's regulatory history and experience provide valuable lessons to the other countries beyond national boundaries, particularly in light of the evolving international AI governance paradigm following the Trump administration's shift in the United States toward more market-friendly regulatory approaches. Korea's case offers valuable lessons for the emerging pro-market international framework: while regulatory flexibility can foster innovation and economic competitiveness, it requires robust institutional mechanisms to prevent the erosion of fundamental rights. The *Incheon Airport* case illustrates how market-oriented regulatory environments can enable rapid technological deployment while simultaneously generating privacy protection vulnerabilities that undermine public trust and democratic accountability.

Ultimately, the insights of this case emphasize that effective AI governance cannot solely rely on technical solutions or procedural frameworks. Instead, it requires a nuanced understanding of how regulatory approaches are shaped by cultural values, institutional legacies, and societal priorities. As global AI governance increasingly embraces market-driven approaches, policymakers should learn from Korea's experience to embed PbD principles and constitutional requirements into regulatory frameworks from the outset. The challenge lies not in choosing between innovation and rights protection, but in developing a governance mechanism that can accommodate both imperatives while maintaining democratic legitimacy and public trust. The *Incheon Airport* case thus serves as both a cautionary tale and a roadmap for navigating the complex terrain of AI governance in an interconnected world where technological deployment increasingly outpaces regulatory adaptation.

However, this study is subject to certain limitations, as it seeks to derive global legal and policy implications from a single case study in Korea. The selection of this methodology was, to some extent, unavoidable, given that FRT is a cutting-edge field and government-related privacy violation issues are rarely disclosed to the public. Nevertheless, future research should aim to broaden

the scope and depth of analysis by undertaking a systematic comparison with regulatory approaches adopted by other Asian countries with cultural similarities to Korea, as well as Western countries with distinct legal and institutional traditions. Through such comparative efforts, it is hoped that a more appropriate balance can be achieved between the benefits and risks associated with FRT.

## Data availability

No datasets were generated or analysed during the current study.

Received: 8 October 2024; Accepted: 20 June 2025;
Published online: 16 July 2025

## Notes

1 Incheon International Airport stands as a critical global hub, having maintained the number one ranking in the World Airport Service Awards for 12 consecutive years, while also ranking second in international cargo transportation and fifth in international passenger transport. As of October 2024, it serves 100 airlines with scheduled flights connecting 178 cities in 54 countries. With an impressive annual operational scale of approximately 358,000 flights, 70 million passengers, and 2.95 million tons of cargo processed, policy decisions implemented at Incheon are poised to have significant global ramifications, influencing air travel, international trade, and the overall connectivity of global transportation networks. Source: https://www.airport.kr/co_ko/576/subview.do (Accessed 24 Mar 2025)

2 In response to the Ministry of Justice's project, several civic societies filed a constitutional complaint. They argued that providing personal data—such as nationality, date of birth, and gender—of both Korean and foreign individuals to private companies without a legal basis infringes on their right to self-determination over personal information and violates their right to privacy and liberty.

3 The guideline aims to outline directions and principles for managing privacy risks in AI. Developed through discussions of the "Public-Private AI Privacy Policy Council," convened by the Personal Information Protection Commission of Korea, it is intended to be flexible enough for AI model and system developers and providers to adapt to their respective needs. Notably, its primary audience consists of companies and institutions seeking to establish, refine, or overhaul their internal privacy management frameworks as they adopt or apply AI technologies. Spanning the entire AI lifecycle—from pre-training and additional training to AI system development and provision—the model offers a comprehensive approach to risk management. Plans are also in place to create additional guidance tailored to specific groups, such as small-scale organizations and startups. This guideline will undergo continuous revision and improvement in response to evolving legal, institutional, and technological conditions.

4 For instance, the Act explicitly prohibits the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement—although this prohibition is tempered by broad exemptions—while mandating that high-risk systems comply with rigorous technological requirements, undergo fundamental rights impact assessments before deployment, and provide individuals with remedial rights such as the ability to obtain an explanation for decisions made by the system.

5 In Article 5 (Relationship with Other Laws) of the AI Framework Act (effective in 2026), it stipulates as (1) Except where otherwise specifically provided by other statutes, matters concerning AI, AI technology, AI industry, and AI society (as "AI, etc") shall be governed by the provisions of this Act. (2) Where enacting or amending other statutes concerning AI, etc., such legislation shall conform to the purpose of this Act.

6 Nonetheless, some critics caution that its broad, non-specific wording may inadvertently extend regulation to a wider range of AI systems. (Park, 2024)

7 The arguments supporting the general authorization clause for policing emphasize that requiring specific legal provisions for each policing activity would make it difficult for governments to fulfill their risk-prevention duties in a complex and rapidly changing modern society. They argue that while policing without a legal basis is impermissible, the principle of statutory reservation is still upheld if the related laws include general authorizations clauses, regardless of the specifics of the policing. Proponents often cite Article 2 of the Act on the Performance of Duties by Police Officers, which broadly defines police duties, as the basis for such general authorization.

## References

Bradford A (2020) The Brussels effect: How the European Union rules the world. Oxford University Press, New York

Buolamwini J, Gebru T (2018) Gender shades: intersectional accuracy disparities in commercial ender classification. In: Conference on fairness, accountability, and transparency, PMLR, pp 77–91

Cho H (2018) A study on inherent police power—using stray thoughts on legal grounds of general police power as writing material. Seoul Law J 59(4):1–39

Chung H (2024) Administrative law. 18th edn. Bubmunsa, Paju

Constitutional Court of Korea (1999) 98Hun-ba70, 27 May 1999

European Data Protection Board (2023) Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (Version 2.0). Available via EDPB https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf. Accessed 24 Mar 2025

Feldstein S (2019) The Global Expansion of AI Surveillance. Available via Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en&center=global. Accessed 24 Mar 2025

Information Commissioner's Office (2022) ICO fines facial recognition database company Clearview AI Inc more than £75m and orders UK data to be deleted. Available via ICO https://ico-newsroom.prgloo.com/news/ico-fines-facial-recognition-database-company-clearview-ai-inc-more-than-gbp-7-5m-and-orders-uk-data-to-be-deleted. Accessed 24 Mar 2025

Karaboga M, Frei N, Ebbers F, Rovelli S, Friedewald M, Runge G (2022) Automatisierte erkennung von stimme, sprache und gesicht: technische, rechtliche und gesellschaftliche Herausforderungen. vdf Hochschulverlag AG, Zürich

KBS News (2021) Government agency provides 170 million immigration photos to private companies. https://news.kbs.co.kr/news/pc/view/view.do?ncd=5306141. Accessed 24 Mar 2025

Kim D (2014a) Administrative law II. Parkyoungsa, Seoul

Kim I (2014b) Die Untersuchung über die Zweckbindung in Datenschutzgesetz. Study Am Constitut 25(3):109–134

Lee C (2024) Facial recognition technology and privacy. J. Korean So. Pri. Secur 23(1):89–114. https://doi.org/10.56603/jksps.2024.23.1.89

Lee C, Lee K, Lee J, Lee J (2020) Criminal investigation of administrative agencies: analysis of the current status and improvement measures. Available via Korean Institute of Criminology and Justice. https://www.kicj.re.kr/board.es?mid=a10101000000&bid=0001&list_no=10505&act=view. Accessed 24 Mar 2025

Lee M (2023) Legislative study on processing of facial recognition information for law enforcement purpose. Korean Minist Gov Legislat 702:109–146

Lee S (2018) The General Clause on the Police Law. Natl Public Law Rev 8(1):1–22

Madieg T, Mildebrath H (2021) Regulating facial recognition in the EU: in-depth analysis. Available via Publications Office of the European Union, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf. Accessed 24 Mar 2025

Montag L, Mcleod R, De Mets L, Gauld M, Rodger F, Pełka M (2021) The rise and rise of biometric mass surveillance in the EU: a legal analysis of biometric mass surveillance practices in Germany, the Netherlands, and Poland. Available via European Digital Rights (EDRi). https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf. Accessed 24 Mar 2025

National Human Rights Commission of Korea (2023) NHRCK emphasizes the importance of proactively addressing human rights risks posed by facial recognition technologies. Available via NHRCK, https://www.humanrights.go.kr/eng/board/read?boardManagementNo=7003&boardNo=7608785&searchCategory=&page=1&searchType=&searchWord=&menuLevel=2&menuNo=114. Accessed 24 Mar 2025

Park D, Cho E, Lim Y (2024) A tough balancing act – the evolving AI governance in Korea. East Asian Sci Technol Soc Int J 18(2):135–164

Park S (2024) Why Korea's AI framework actrequires amendment before implementation - A structural and textualanalysis. Info-Media Law 28(3):3–50

Personal Information Protection Commission of Korea (2021a) Decision of 27 April 2022, 2022-007-046. Available via PIPC, https://www.pipc.go.kr/np/default/agenda.do?op=view&mCode=E030010000&page=1&isPre=&mrtlCd=&idxId=2022-0161&schStr=&fromDt=&toDt=&insttDivCdNm=&insttNms=&processCdNm=#LINK. Accessed 24 Mar 2025

Personal Information Protection Commission of Korea (2021b) Biometric information protection guideline. Available via PIPC, https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=1761. Accessed 24 Mar 2025

Personal Information Protection Commission of Korea (2024) AI Privacy Risk Management Model for Safe AI Data Utilization. Available via PIPC, https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=11014. Accessed 24 Mar 2025

Polyakova A, Meserole C (2019) Exporting digital authoritarianism: the Russian and Chinese models. policy brief, democracy and disorder series (August 2019), pp 1–22

Supreme Court of Korea, 2016Do13263, 7 April 2017

Tang Y (2024) Privacy protection framework for open data: constructing and assessing an effective approach. Libr Inf Sci Res 46(3):101312

VG Hamburg, Urt. v. 23.10.2019, Az. 17 K 203/19

## Acknowledgements

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. RS-2022-NR070855).

## Author contributions

The authors contributed equally to this work. They jointly developed the research ideas through collaborative discussions and shared responsibilities in writing and reviewing the manuscript. In addition to these shared contributions: Haesung Lee conducted the literature survey, developed the methodology, and contributed to writing "Introduction", "Facial Recognition Technology and its Regulatory framework", and "Toward a Comprehensive Data Governance Framework for FRT" of the manuscript. Eunsoo Kim assisted with the conceptualization of the research, contributed to writing "The Incheon Airport Case" of the manuscript, and carried out proofreading. Do Hyun Park supervised the entire process, contributed to the conceptualization of the research, and wrote "Legal challenges of Policing with FRT in South Korea" of the manuscript.

## Competing interests

The authors declare no competing interests.

## Ethical approval

This article does not contain any studies with human participants performed by any of the authors.

## Inform consent

This article does not contain any studies with human participants performed by any of the authors

## Additional information

**Correspondence** and requests for materials should be addressed to Do Hyun Park.

**Reprints and permission information** is available at http://www.nature.com/reprints

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.