**AI-driven Predictive Policing in Germany and Japan: Constitutional and Human Rights Challenges in Comparative Perspective**

*Dr. Ivo Gruev*

*Academy for European Human Rights Protection, University of Cologne*

*[ Note to the reader: Thank you for taking the time and patience to engage with this early draft, which remains a work in progress. I have written it specifically for the purposes of this symposium, adopting a somewhat unconventional—but I hope not unconvincing—comparative approach that examines Germany and Japan in relation to international human rights frameworks relevant to predictive policing.*

*The sections on Japan and the broader international legal framework (Parts III and IV) require further research and elaboration. I recognize the need for a more robust engagement with literature on Japan’s approach to predictive policing and AI governance, which is currently less developed in this draft. I would greatly appreciate constructive feedback on these areas, particularly regarding the conceptual framework and the comparative dimension. I also apologize in advance for any typos and formatting inconsistencies, as well as for the footnotes, which are not yet finalized.]*

Draft outline. Do not cite or circulate.

**Introduction**

Artificial intelligence (AI) has permeated many facets of modern society, including the realm of criminal justice. One particularly contentious application of AI that is gaining global popularity is predictive policing (PP). This method employs AI, big data analytics, and machine learning to forecast criminal activity and allocate police resources more efficiently.[[1]](#footnote-1) Advocates argue that predictive policing enhances crime prevention by offering a more data-driven and cost-effective approach to law enforcement. However, the deployment of AI in this domain raises significant constitutional and human rights concerns, particularly in relation to legal certainty, privacy, due process, and the risk of algorithmic bias undermining equality before the law.

The regulation and implementation of PP vary significantly across legal systems. Some jurisdictions have embraced AI-driven policing as an innovative law enforcement strategy, while others have imposed strict constitutional constraints on its use. Germany represents an example of the latter approach. In a landmark ruling in 2023, the German Federal Constitutional Court (*Bundesverfassungsgericht*, BVerfG) invalidated key provisions of predictive policing laws in Bavaria and Hesse. The Court held that the AI-generated risk assessments underlying these laws lacked legal certainty, disproportionately infringed upon privacy rights, and posed risks to equal treatment under Article 3 of the German Basic Law (*Grundgesetz*, GG). The ruling underscored the incompatibility of opaque algorithmic decision-making with fundamental rule-of-law principles, reinforcing the necessity of clear legal frameworks to regulate AI applications in criminal justice.[[2]](#footnote-2) This is not the end of the story in Germany, as a follow-up constitutional complaint has been filed, challenging the reformed legislation enacted in response to the BVerfG ruling on the grounds that it does not sufficiently address constitutional concerns.[[3]](#footnote-3)

At the regional level, while the European Court of Human Rights (ECtHR) has yet to issue a direct ruling on predictive policing, its jurisprudence on mass surveillance, data protection, and discriminatory policing offers valuable insights. In Gillan and Quinton v. UK (2010),[[4]](#footnote-4) the Court ruled against disproportionate stop-and-search powers, and in Big Brother Watch v. UK (2021),[[5]](#footnote-5) it found that mass surveillance systems lacking sufficient legal safeguards violated the right to privacy under Article 8 of the European Convention on Human Rights (ECHR). These precedents suggest that, if presented with a case on predictive policing, the ECtHR might follow a similar restrictive approach, emphasizing the importance of legal certainty, proportionality, and non-discrimination in AI-driven law enforcement measures.

Japan, by contrast, has taken a more permissive stance on predictive policing.[[6]](#footnote-6) Over the past decade, the Japanese government has actively promoted AI-based policing initiatives, particularly in densely populated urban areas such as Tokyo and Osaka. These systems generate crime risk predictions by analyzing vast datasets, including historical crime records, geographic patterns, and demographic information. Japanese AI-driven policing technologies have even been exported to other jurisdictions, such as Brazil, further demonstrating the country’s commitment to this approach. While Japan's regulatory framework for predictive policing continues to evolve, discussions about transparency, accountability, and human rights compliance remain ongoing. While Germany has imposed restrictions on predictive policing through constitutional court rulings, rather than legislative action, Japan, lacking comparable case law, approaches the oversight of AI-driven law enforcement through a different legal and institutional framework, making it an important counterpoint in a comparative legal analysis of predictive policing.

On the international level, the regulation of AI-driven predictive policing is still in its early stages. However, a significant development occurred on 11 February 2025, when Japan, alongside Canada, became the latest signatory of the newly adopted Council of Europe Framework Convention on Artificial Intelligence.[[7]](#footnote-7) This Convention represents a landmark effort to establish international human rights safeguards for AI applications, including their use in law enforcement. Given Japan’s participation in this emerging normative framework and Germany’s ongoing deliberations regarding AI regulation, their divergent approaches to predictive policing provide an important case study for assessing the constitutional and human rights implications of AI-driven law enforcement across different legal systems.

This article critically examines the use of predictive policing in Germany and Japan, focusing on the constitutional and human rights challenges that arise in each jurisdiction. The analysis is developed in four parts. Part I outlines the rise of predictive policing and its global appeal, providing an overview of key predictive policing models and technologies. Part II considers the German example, analyzing the BVerfG ruling and its implications for constitutional standards on legal certainty, privacy, and non-discrimination. Part III examines Japan’s approach to predictive policing, exploring its regulatory framework and human rights implications. Part IV situates these national experiences within the broader international legal landscape, with a particular focus on relevant ECtHR case law and the Council of Europe’s AI Convention. Finally, the concluding section offers comparative reflections on the constitutional and international human rights challenges posed by predictive policing, emphasizing the need for robust legal safeguards to ensure the compatibility of AI-driven law enforcement with fundamental rights.

**Part 1: Predictive Policing - An Outline**

**1. The Emergence of Predictive Policing**

The use of statistical techniques to enhance policing is not a novel concept.[[8]](#footnote-8) However, the rise of predictive policing (PP) is largely attributable to advances in artificial intelligence (AI) and big data analytics.[[9]](#footnote-9) These technological developments have enabled law enforcement agencies to process vast amounts of crime-related data to detect patterns and forecast criminal activity.[[10]](#footnote-10) At its core, PP is based on the assumption that certain environmental and social conditions create predictable patterns of criminal behavior, and that intervening in these patterns can prevent crime.[[11]](#footnote-11)

Governments and police forces worldwide have embraced PP as a means to enhance efficiency and optimize resource allocation. Given the constraints on law enforcement resources, predictive models are framed as tools to help authorities prioritize high-risk areas and individuals, allowing for proactive crime prevention. This justification has gained further traction in the context of growing concerns over terrorism, organized crime, and urban violence.[[12]](#footnote-12) However, while the efficiency-based rationale for PP is compelling, it also raises significant ethical and legal concerns, particularly regarding transparency, accountability, and judicial oversight.

**2. The Mechanics of Predictive Policing**

PP can be broadly categorized into three types: location-based, person-based, and event-based policing.[[13]](#footnote-13)

* **Location-Based Predictive Policing**

Location-based predictive policing focuses on identifying geographic areas where crimes are statistically more likely to occur. Technologies such as hotspot analysis and risk terrain modeling analyze crime patterns in relation to environmental and socio-economic factors, allowing law enforcement to concentrate resources in high-risk areas. One well-known example is PredPol (now Geolitica), a predictive software used in the United States and the United Kingdom to forecast burglary, assault, and theft trends.[[14]](#footnote-14)

* **Person-Based Predictive Policing**

Person-based predictive policing identifies individuals considered at high risk of committing crimes. These models utilize biometric surveillance, social network analysis, and AI-driven behavioral profiling to flag individuals based on factors such as past criminal records, associations with known offenders, or predictive risk scores. This approach is particularly controversial and most difficult to withstand heightened fundamental rights scrutiny, as it singles out individual names and faces, raising serious concerns about due process, fairness, and potential reinforcement of discriminatory policing practices.[[15]](#footnote-15)

The reliance on historical crime data in particular raises concerns about bias and discrimination, as such data often reflect existing disparities in law enforcement practices.[[16]](#footnote-16)

Critics argue that such systems often reflect pre-existing biases in policing data, leading to disproportionate targeting of marginalized communities.[[17]](#footnote-17) Nevertheless, person-based predictive policing has been implemented in cities such as London, Amsterdam, Chicago, Kansas City, and New York, underscoring the global appeal of these technologies despite their ethical and legal challenges.[[18]](#footnote-18)

* **Event-Based Predictive Policing**

**Event-based predictive policing** focuses on anticipating specific types of criminal activities based on temporal and situational factors.[[19]](#footnote-19) It targets specific types of criminal activities that are likely to occur. This model relies on real-time data analytics, monitoring large-scale events, financial transactions, or online activities to detect potential security threats. While this approach has been applied to terrorism prevention and financial fraud detection, it remains less developed than location- and person-based models in traditional policing contexts.

PP, especially of the location-based variety, has gained traction in various countries, including the United States, the United Kingdom, the Netherlands, Japan, and several European states.[[20]](#footnote-20)

Each of these models depends on vast datasets processed through machine learning algorithms. These algorithms analyze crime reports, surveillance data, and external sources, creating predictive models that purportedly enhance police decision-making.[[21]](#footnote-21) Machine learning algorithms, unlike traditional rule-based algorithms, evolve over time, refining their predictions as they process more data.[[22]](#footnote-22) However, this continuous adaptation introduces a major concern, which will be considered in more detail below: the risk of a self-fulfilling prophecy. Since police officers contribute data by recording incidents, these records shape future predictions, potentially reinforcing pre-existing human biases.[[23]](#footnote-23)

The following section canvasses some general concerns facing the application of PP from fundamental rights perspective.

**3. Fundamental Rights Challenges to Predictive Policing**

**The deployment of PP raises serious concerns about fundamental rights, particularly regarding non-discrimination, due process, transparency, and privacy.**[[24]](#footnote-24)The opacity of AI-driven decision-making further exacerbates these concerns, as many predictive models operate as "black boxes," making it difficult to assess their reliability and fairness. **These risks stem from the reliance on big data—drawn from historical crime records, public registries, and private sector sources—processed by machine learning algorithms that evolve without human oversight.**[[25]](#footnote-25)

**A major issue is the quality and potential biases in input data, often encapsulated in the phrase "garbage in, garbage out".**[[26]](#footnote-26) **Predictive models trained on crime data reflecting past policing practices risk perpetuating structural inequalities, disproportionately targeting marginalized communities.**[[27]](#footnote-27) **This creates a self-fulfilling prophecy, reinforcing the over-policing of certain groups rather than addressing underlying social causes of crime. Additionally, since machine learning continuously refines its rules based on data patterns, these biases may become embedded in ways that are difficult to detect and correct.**[[28]](#footnote-28)

**A further challenge lies in the opacity of predictive policing algorithms. Many of these systems operate as "black boxes," making it difficult to scrutinize how decisions are reached, particularly when proprietary software is involved.**[[29]](#footnote-29) **Even when transparency measures are in place, the complexity of machine learning models makes them difficult for law enforcement officers—and even experts—to fully understand, reducing opportunities for oversight and accountability.**[[30]](#footnote-30) **This opacity exacerbates automation bias, where officers defer to algorithmic recommendations without critical assessment, potentially leading to wrongful interventions and weakened procedural safeguards.**[[31]](#footnote-31)

**Predictive policing also raises significant privacy and surveillance concerns. The extensive collection and processing of personal data align with broader fears of mass surveillance, often compared to dystopian narratives such as Minority Report and 1984.**[[32]](#footnote-32) **Within the European Union, data protection laws—including the General Data Protection Regulation (GDPR) and the Law Enforcement Directive—set strict requirements for the processing of personal data.**[[33]](#footnote-33) **However, concerns persist about compliance, oversight, and the extent to which predictive policing technologies adhere to these legal frameworks. Without adequate safeguards, there is a risk that predictive policing will not only infringe on privacy rights but also undermine public trust in law enforcement institutions. The German approach, as shaped by the Constitutional Court—examined in the next section—underscores the necessity of robust legal safeguards without which the implementation of predictive policing poses significant risks to fundamental rights and the rule of law.**

**Part II Predictive Policing in Germany**

1. **Overview**

Predictive policing has become a subject of considerable debate in Germany since its introduction in 2014. Various federal states have experimented with different technological solutions to anticipate criminal activity, particularly focusing on property crimes like residential burglary.[[34]](#footnote-34) The primary aim of predictive policing in Germany thus far has been to identify high-risk locations rather than to profile individuals, distinguishing it from some approaches used in other countries. The applications are thus largely based on geospatial analysis, which seeks to identify crime-prone areas by analyzing historical crime data and applying criminological theories. The dominant theoretical underpinning of these systems is the "near-repeat" phenomenon, which suggests that certain crimes, such as burglary, tend to occur in clusters: once a burglary has been committed in a particular location, there is a statistically higher probability that a similar crime will take place nearby within a short timeframe.

This principle has guided the development and deployment of various predictive policing tools across different federal states. The most well-known software, Precobs (Pre Crime Observation System), was developed by the Institute for Pattern-Based Prediction Techniques and piloted in Bavaria, Baden-Württemberg, and North Rhine-Westphalia. These systems analyzed historical crime data to predict high-risk areas, allowing police to concentrate patrols accordingly. Different regional varieties of such applications, such as KrimPro in Berlin, and SKALA in North Rhine-Westphalia adopt similar approaches that rely on crime data and the near-repeat phenomenon to generate spatial crime forecasts. Some, such as KrimPro, integrate socio-economic data to refine predictions, while others, like PreMAP in Lower Saxony, were eventually abandoned due to inefficiency and a lack of sufficient data for reliable forecasts.

Beyond these geospatial prediction models, Germany has also experimented with predictive systems that assess individual risk factors. *RADAR-iTE* (*Regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des akuten Risikos – islamistischer Terrorismus*), developed by the Federal Criminal Police Office (*Bundeskriminalamt*), is used to evaluate the potential threat posed by individuals suspected of harboring Islamist extremist views.

​Finally, Germany has also adopted large-scale data analysis tools such as *HessenData*, which employs Palantir’s *Gotham* software to aggregate and analyze vast amounts of information from multiple sources, including police databases, surveillance footage, and communication records. While *HessenData* does not generate direct crime predictions, it facilitates advanced data mining and pattern recognition, allowing law enforcement to identify potential threats more efficiently. However, this system has been criticized for its broad data collection practices, which some legal scholars argue amount to mass surveillance, leading to a constitutional complaint before the federal constitutional court challenging the legislation authorizing the use of this system.

1. **The 2023 Federal Constitutional Court Judgment on Automated Data Analysis in Hesse and Hamburg**

In a landmark ruling, the German Federal Constitutional Court declared that provisions in the security laws of Hesse and Hamburg allowing for automated data analysis by police authorities were unconstitutional.[[35]](#footnote-35) These provisions, which authorized the processing of stored personal data through advanced analytical methods, were found to violate the right to informational self-determination under Article 2(1) in conjunction with Article 1(1) of the German Basic Law (*Grundgesetz,* GG). The Court ruled that these laws lacked sufficient legal safeguards and failed to meet the required constitutional threshold of an identifiable danger (*konkretisierte Gefahr*) necessary to justify such intrusive measures.

The case concerned § 25a(1) of the Hesse Security and Public Order Act (*Hessisches Gesetz über die öffentliche Sicherheit und Ordnung* – HSOG) and § 49(1) of the Hamburg Act on Data Processing by the Police (*Hamburgisches Gesetz über die Datenverarbeitung der Polizei* – HmbPolDVG), which provided a legal framework for linking and analyzing previously unconnected data sources in police databases through automated means. These provisions granted law enforcement authorities in both states extensive powers to process personal data for two primary purposes: preventing serious criminal acts as defined in § 100a(2) of the Code of Criminal Procedure (*Strafprozessordnung* – StPO) and averting dangers to certain legal interests, including public safety and security. By enabling the establishment of links between individuals, groups, organizations, objects, and locations, these provisions allowed police to filter out irrelevant information, detect patterns, and generate new intelligence. In Hesse, the HessenDATA platform had already been used extensively under these powers, with thousands of applications per year. In contrast, Hamburg had not yet put § 49(1) into practice.

The Court found that these provisions amounted to a severe interference with the right to informational self-determination. The interference, it held, arose not only from the continued use of previously collected data but also from the new intelligence that could be derived from automated data analysis. The ruling emphasized that such analytical methods could reveal far-reaching personal details about individuals, generating insights beyond what conventional investigative techniques would uncover. The Court acknowledged that automated data analysis could serve the legitimate goal of improving crime prevention in light of increasing digitalization and data complexity. However, it found that the challenged provisions failed to comply with constitutional requirements, particularly the principle of proportionality.

A key element of the ruling was the Court’s assessment that the legal provisions did not meet the required threshold of an identifiable danger. Under German constitutional law, predictive policing and data-driven law enforcement must be grounded in a concrete and specific threat. The provisions in question, however, permitted data analysis without the existence of a tangible or imminent risk, allowing law enforcement agencies to proactively generate new leads and potential suspects based on algorithmic analysis alone. The Court criticized this approach, arguing that it fundamentally altered the traditional investigative process by shifting police work toward speculative surveillance rather than responding to actual threats. The lack of a concrete danger threshold effectively granted authorities the power to conduct large-scale data mining without sufficient justification, making it possible for innocent individuals to be subjected to police scrutiny without any direct link to a crime.

Another major constitutional flaw identified by the Court was the absence of adequate safeguards to limit the use of collected data to its original purpose. While data gathered for specific investigations may sometimes be repurposed for crime prevention, strict legal safeguards are required to prevent misuse. The provisions in Hesse and Hamburg, however, failed to include meaningful restrictions regarding the types of data that could be analyzed, effectively allowing for indiscriminate processing of personal information, including that of third parties with no connection to criminal activity. Furthermore, the Court noted that the laws imposed no clear restrictions on the methods of analysis, meaning that highly intrusive techniques, such as self-learning artificial intelligence (AI) and predictive algorithms, could potentially be employed without oversight.

The ruling also highlighted the broader implications of these provisions for privacy and mass surveillance. By enabling police authorities to process vast amounts of data at the click of a button, the laws effectively allowed for the creation of comprehensive digital profiles of individuals, groups, and social networks. This, the Court held, amounted to an unconstitutional risk of excessive state control over personal data. The ability to instantly cross-reference police databases, analyze personal relationships, and generate suspect profiles without individualized suspicion fundamentally changed the nature of law enforcement, blurring the line between investigation and preventive surveillance.

Based on these findings, the Court ruled that § 25a(1) of the Hesse Act would remain in force temporarily, but only under strict limitations until 30 September 2023, to allow the state legislature time to revise the law and bring it into compliance with constitutional standards. In contrast, § 49(1) of the Hamburg Act was declared void (nichtig) with immediate effect. Since the provision had not yet been applied in practice, there was no justification for allowing it to remain in force.

In its ruling, the Court also imposed specific restrictions on the continued use of hessenDATA in Hesse until the law is revised. Police may only conduct automated data analysis when specific, well-founded suspicion exists that a particularly serious criminal act within the meaning of § 100b(2) StPO has already been committed. Additionally, any analysis must be linked to specific circumstances indicating that similar crimes are likely to occur in the future, posing a direct risk to life, physical integrity, or national security. The Court further required that police provide a written justification in each case, explaining the necessity of the data analysis and ensuring that particularly sensitive information—such as data obtained from home surveillance, telecommunications interception, or undercover operations—is excluded.

The ruling has far-reaching implications for the future of predictive policing and automated data analysis in Germany. It reinforces the requirement that predictive policing methods must be grounded in an identifiable danger rather than vague suspicions or general crime prevention goals. Future legislative efforts to expand predictive policing powers will need to incorporate stricter safeguards and oversight mechanisms to ensure compliance with constitutional standards. The judgment also highlights the need for greater transparency in how police use automated data analysis, requiring legislators to provide clearer definitions regarding what types of data can be processed, under what circumstances, and using which analytical methods.

The ruling is particularly significant in the context of increasing reliance on AI and big data in law enforcement. By rejecting overly broad data analysis powers, the Court signals that Germany will not permit unchecked algorithmic decision-making in policing without clear legal safeguards. This decision also sets a precedent that could lead to constitutional challenges against similar data processing laws in other German states. Given the growing role of digital surveillance and predictive policing, the ruling establishes an important legal framework for balancing technological advancements with fundamental rights.

Ultimately, the Federal Constitutional Court’s decision is a reaffirmation of the principle that state surveillance and data processing must be subject to strict legal constraints. While acknowledging the importance of digital tools for modern law enforcement, the ruling underscores that such technologies cannot override fundamental rights to privacy, proportionality, and accountability. As German legislators move forward with revising the legal framework for predictive policing, they will need to craft more precise, legally sound policies that ensure both security and the protection of constitutional freedoms.

*[Further analysis of comparative significance to be added.]*

**Part III: Predictive Policing in Japan**

*[Note to the reader: The section on Japan is still in the very early stages of drafting and requires further research and development. I would greatly appreciate any feedback or suggestions for improvement, as well as recommendations for relevant literature.]*

Predictive policing, mostly of the location-based variety, has gained increasing traction in Japan.[[36]](#footnote-36) The loss of experienced law enforcement personnel due to the retirement of the baby-boomer generation, coupled with declining recruitment rates and budget constraints, has encouraged the integration of AI-based predictive systems. Technologies such as Risk Terrain Modeling (RTM), which rely on environmental factors rather than past crime data, have been tested in Japan with promising results. Additionally, AI-based facial and gait recognition systems, such as those developed by Hitachi, have been trialed for public safety, particularly in high-profile events like the Tokyo 2020 Olympics.

In 2024, Singular Perturbations Inc., a startup focused on crime reduction, developed an innovative AI-driven technology, Crime Nabi, designed to predict the occurrence of crimes with purportedly high accuracy. The system not only forecasts when and where crimes are likely to happen but also generates optimized patrol routes recommendations. This system has recently been exported to Brazil, a country facing severe public security challenges, where its high prediction accuracy and user-friendly design are poised to transform policing operations and impact society at large.[[37]](#footnote-37)

However, Japan presents a unique case due to its exceptionally low crime rate compared to other developed nations, making conventional predictive models less effective. Predictive models like KDE, ProMap, and SEPP, which depend on historical crime data, struggle to function effectively in Japan due to a lack of crime concentration and interaction effects. RTM has been suggested as a more viable alternative since it does not require extensive crime data. Nonetheless, the effectiveness of such models remains uncertain, given that crime patterns in Japan are often highly dispersed and less predictable than in high-crime Western cities.

**1. Legal Regulation and Transparency Issues**

Japan’s approach to AI-based predictive policing is shaped by a patchwork of legal and ethical guidelines rather than a comprehensive regulatory framework. The Ministry of Internal Affairs and Communications has issued AI Principles (2017), emphasizing autonomy, transparency, data integrity, risk management, and human-centricity. However, these principles remain broad and lack specific enforcement mechanisms tailored to law enforcement applications.

A key concern is the opacity of predictive policing algorithms. Unlike some Western jurisdictions where crime data is publicly available, Japan’s restrictive data-sharing policies make it difficult for independent researchers and civil society to scrutinize the effectiveness and fairness of predictive models. This lack of transparency raises concerns about potential biases embedded in the algorithms and their implications for due process and accountability. Moreover, Japan does not have an explicit legal framework governing the use of predictive policing, leaving law enforcement agencies significant discretion in deploying these technologies.

Recognizing the need for a more robust regulatory framework, Japan is considering the Basic Act on the Advancement of Responsible AI. If enacted, this legislation would impose obligations on AI developers and operators, introducing penalties for non-compliance and marking a significant shift towards stringent AI regulation. Existing laws, such as the Act on the Protection of Personal Information, also impact AI systems, particularly concerning data privacy and the handling of personal data.

**2. Constitutional and Human Rights Challenges**

* **Privacy and Data Protection**

One of the most pressing human rights concerns is the potential infringement on the right to privacy. AI-based systems like Hitachi’s facial and gait recognition technology can track individuals based on multiple biometric identifiers, even without clear facial images. While Japan has data protection laws, including the Act on the Protection of Personal Information (APPI), these regulations were not specifically designed to address the complexities of AI-driven surveillance. The lack of stringent oversight mechanisms increases the risk of unauthorized data collection and retention, leading to potential abuses.

* **Due Process and Presumption of Innocence**

Predictive policing introduces the risk of law enforcement treating individuals as potential criminals based on probabilistic assessments rather than concrete evidence. This raises fundamental concerns under Article 31 of the Japanese Constitution, which guarantees due process rights. If predictive policing tools influence decisions about policing strategies and resource allocation, there is a risk that certain individuals or communities may be unfairly targeted based on algorithmic predictions rather than actual criminal behavior.

* **Risk of Discrimination and Bias**

Although Japan does not have pronounced socio-economic divisions akin to those in the United States or Europe, predictive policing models may still reinforce biases. AI-based policing systems rely on data patterns that may inadvertently target marginalized groups, including foreign workers and single-person households—two demographics that are increasing in Japan. The AI Principles emphasize fairness and non-discrimination, yet the current lack of regulatory oversight means that biases in predictive algorithms may go unchecked.

* **Overreach of Police Powers**

The increasing reliance on AI-based policing tools risks expanding law enforcement powers without adequate legal safeguards. Without proper oversight, predictive policing could shift law enforcement’s focus from responding to crimes to preemptively surveilling individuals based on statistical probabilities. This could lead to a system where law enforcement exerts control over citizens in ways that are incompatible with constitutional guarantees of individual liberty and freedom from arbitrary state intervention.

* **Possible Recommendations**

Several measures could be taken to ensure compliance with constitutional principles and human rights protections:

Strengthening Legal Frameworks: specific legislation governing predictive policing, including clear guidelines on data usage, accountability measures, and limitations on AI-based surveillance.

Enhancing Transparency and Public Oversight: Crime data and algorithmic decision-making processes to be made more accessible to independent researchers and oversight bodies to prevent potential biases and ensure due process.

Implementing Robust Privacy Protections: Stricter data protection laws, particularly regarding biometric data collection, storage, and usage, to prevent privacy infringements.

Ensuring Human Oversight in Decision-Making: AI-based predictions should serve as supplementary tools rather than determinants of law enforcement action. Human decision-makers must remain ultimately responsible for policing decisions.

**Part IV: The ECHR and Council of Europe Framework**

The constitutional constraints on predictive policing are reinforced by broader human rights principles enshrined in both the European Convention on Human Rights (ECHR) and the Council of Europe’s newly adopted AI Convention. While Germany, as a member state of the Council of Europe, is bound by the ECHR, it has not yet signed the AI Convention. In contrast, Japan is not a party to the ECHR but is, since 11 February 2025, among the most recent signatories of the AI Convention.

The interaction between these two legal frameworks is particularly relevant given the complementary nature of their human rights protections. The ECHR provides well-established jurisprudence on privacy, due process, and non-discrimination, which could serve as a foundational reference for assessing predictive policing under the AI Convention. Conversely, the AI Convention introduces specific, legally binding principles tailored to the governance of artificial intelligence, including safeguards against algorithmic bias, requirements for transparency, and mandates for human oversight. These principles are likely to influence future interpretations of human rights protections under the ECHR, particularly in cases involving AI-driven policing technologies.

For Germany, the ECHR already imposes significant human rights constraints on the deployment of predictive policing technologies, particularly through the case law of the European Court of Human Rights (ECtHR) on surveillance, privacy, and discrimination. While the country has yet to adopt the AI Convention, the Convention’s standards may still shape domestic debates on AI regulation, either through its eventual ratification or by influencing European human rights discourse more broadly. Japan, on the other hand, is not subject to the ECHR’s legal framework but has voluntarily committed to the AI Convention’s regulatory framework. This raises critical questions about how Japan will reconcile its AI-driven predictive policing practices with the stringent transparency, oversight, and anti-discrimination obligations set out in the Convention.

A comparative analysis of Germany and Japan is therefore instructive in understanding how these two distinct human rights instruments impose limitations on predictive policing. The interplay between the ECHR’s established human rights protections and the AI Convention’s emerging governance principles provides a valuable framework for evaluating the legal boundaries of AI-driven law enforcement.

1. **The European Court of Human Rights**

Although the ECtHR has not explicitly ruled on predictive policing, the Court's case law on surveillance practices and data protection is highly relevant in this context. In *Big Brother Watch v. UK* (2021), the Court emphasized that mass surveillance, including the use of technologies that monitor individuals' movements or behaviors, requires robust legal safeguards to prevent misuse and ensure accountability. The principles established in this case could be directly applicable to predictive policing, particularly when assessing whether AI-driven systems infringe upon privacy rights under Article 8 ECHR (right to respect for private and family life).

Predictive policing, by its nature, often involves the collection and analysis of vast quantities of data, including personal information, to forecast potential criminal activities. This could lead to significant concerns about privacy if the data collected is used arbitrarily or disproportionately. The ECtHR’s decision in *Big Brother Watch* suggests that, without proper regulation and oversight, such practices could violate individuals' rights under Article 8. Furthermore, predictive algorithms that disproportionately target certain groups based on race, socio-economic status, or other protected characteristics could raise serious concerns under Article 14 ECHR, which guarantees protection against discrimination.

The ECtHR's ruling in *Gillan and Quinton v. UK* (2010) further complicates the legal landscape for predictive policing. In that case, the Court found that stop-and-search practices, which were conducted without adequate oversight, violated the right to liberty and security under Article 5 ECHR. AI-driven profiling, which often forms the basis of predictive policing models, could similarly lead to arbitrary or discriminatory actions against individuals without sufficient legal safeguards. The lack of oversight and accountability in such systems could, therefore, constitute a violation of both privacy and liberty rights under the ECHR.

1. **The 2024 Council of Europe AI Convention**

In addition to the ECtHR's jurisprudence, the 2024 Framework Convention on Artificial Intelligence, which Japan has ratified, provides an important international legal framework for regulating AI technologies, including predictive policing. This Convention establishes several key principles that are particularly relevant for the deployment of AI in law enforcement.

The Convention mandates that AI systems, especially those used in high-stakes areas like policing, must adhere to principles of transparency, accountability, and non-discrimination. Specifically, it prohibits AI systems that pose unacceptable risks, including those that may result in algorithmic discrimination. Predictive policing technologies that disproportionately target certain demographic groups based on flawed data or biased algorithms could therefore be deemed non-compliant with these provisions. Additionally, the Convention requires that AI-based decision-making be subject to human oversight, ensuring that automated systems do not operate in a manner that infringes upon fundamental rights.

One of the Convention’s most significant provisions is its focus on anti-discrimination safeguards. The risk of racial or socio-economic profiling in predictive policing is a concern that has been widely discussed, and the Convention provides legal frameworks to address such risks. By requiring transparency and human review of AI-driven decisions, the Convention aims to prevent the systemic discrimination that can arise from the use of biased data or algorithms in law enforcement.

Japan’s ratification of the AI Convention raises important questions about whether its adoption of predictive policing systems, including those exported to countries like Brazil, aligns with the human rights principles enshrined in the Convention. While the technology itself may offer significant improvements in crime prevention and law enforcement efficiency, its deployment must comply with the Convention's requirements for transparency, oversight, and non-discrimination. These legal principles could form the basis for future legal challenges, both domestically and internationally, should the predictive policing systems fail to meet the high standards set by the Convention.

**Conclusion: Comparative analysis** [work in progress]

1. Meijer, A., and Wessels, M., “Predictive Policing: Review of Benefits and Drawbacks.”  2019 *International Journal of Public Administration* 42 (12): 1031–39 (2019). [↑](#footnote-ref-1)
2. BVerfG, 1 BvR 1547/19, 2023. [↑](#footnote-ref-2)
3. <https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-vb-big-data-analyse> . [↑](#footnote-ref-3)
4. Gillan and Quinton v. the United Kingdom, no. 4158/05, ECHR 12 January 2010. [↑](#footnote-ref-4)
5. Big Brother Watch and Others v. the United Kingdom, nos. 58170/13, 62322/14, and 24960/15, ECHR 25 May 2021. [↑](#footnote-ref-5)
6. Ohyama, T., Amemiya, M. Applying Crime Prediction Techniques to Japan: A Comparison Between Risk Terrain Modeling and Other Methods. *Eur J Crim Policy Res* 24, 469–487 (2018). [↑](#footnote-ref-6)
7. <https://rm.coe.int/1680afae3c>; <https://www.coe.int/en/web/portal/-/canada-and-japan-sign-council-of-europe-s-first-ever-global-treaty-on-ai>. [↑](#footnote-ref-7)
8. Elizabeth E Joh, ‘Feeding the Machine: Policing, Crime Data, & Algorithms’ (2017) 26 Wm Mary Bill Rts J 287. [↑](#footnote-ref-8)
9. The literature in this field is rapidly expanding, particularly in the United States, where predictive policing models have been in use for the longest period: Buchholtz, G. (2020). Artificial intelligence and legal tech: Challenges to the rule of law. In *Regulating artificial intelligence* (pp. 175–198). Cham: Springer; Degeling, M., & Berendt, B. (2018). What is wrong about robocops as consultants? A technology-centric critique of predictive policing. *AI & Society,* *33*(3), 347–356; Egbert, S, & Krasmann, S. (2019). Predictive policing: Not yet, but soon preemptive? *Policing and Society*; erguson, A. G. (2015). Big data and predictive reasonable suspicion. *University of Pennsylvania Law Review,* *163*(2), 327–410; Ferguson, A. G. (2017a). Policing predictive policing. *Washington University Law Review,* *94*(5), 1115–1194; Nissan, E. (2017). Digital technologies and artificial intelligence’s present and foreseeable impact on lawyering, judging, policing and law enforcement. *AI & Society,* *32*(3), 441–464; Sheehey, B. (2019). Algorithmic paranoia: The temporal governmentality of predictive policing. *Ethics and Information Technology,* *21*(1), 49–58. [↑](#footnote-ref-9)
10. Saunders, J., Hunt, P., & Hollywood, J. S. (2016). Predictions put into practice: A quasi-experimental evaluation of Chicago’s predictive policing pilot. *Journal of Experimental Criminology,* *12*(3), 347–371; Kreutzer, R. T., & Sirrenberg, M. (2020). Fields of application of artificial intelligence—Security sector and military sector. *Understanding artificial intelligence* (pp. 225–233). Cham: Springer; Kulkarni, P., & Akhilesh, K. B. (2020). Big data analytics as an enabler in smart governance for the future smart cities. In *Smart technologies* (pp. 53–65). Singapore: Springer. [↑](#footnote-ref-10)
11. Uchida, C. (2014). Predictive policing. In G. Bruinsma & D. Weisburd (Eds.), *Encyclopedia of criminology and criminal justice* (pp. 3871–3880). New York: Springer; Moses, L. B., & Chan, J. (2018). Algorithmic prediction in policing: Assumptions, evaluation, and accountability. *Policing and Society,* *28*(7), 806–822. [↑](#footnote-ref-11)
12. Ferguson, A. G. (2017b). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York: New York University Press; Egbert and Krasmann 2019. [↑](#footnote-ref-12)
13. <https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf> ; Oosterloo, S., & van Schie, G. (2018). The politics and biases of the ‘crime anticipation system’ of the Dutch police. In *Proceedings of the international workshop on bias in information, algorithms, and systems* (BIAS 2018); Couchman, H. (2019). *Policing by machine: Predictive policing and the threat to our rights*. Retrieved July 10, 2019, from <https://reurl.cc/RdM1Er>. [↑](#footnote-ref-13)
14. Hardyns, W., & Rummens, A. (2018). Predictive policing as a new tool for law enforcement? Recent developments and challenges. *European Journal of Criminal Policy Research,* *24*, 201–218. [↑](#footnote-ref-14)
15. Ferguson 2017b. [↑](#footnote-ref-15)
16. Prince, A., Schwarcz, D. (2019). Proxy discrimination in the age of artificial intelligence and big data. *Iowa Law Review, 105*, 1257–1318; Richardson, R., Schultz, J., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *New York University Law Review,* *94*, 192–233. [↑](#footnote-ref-16)
17. Amnesty International UK 2018; Oosterloo & van Schie 2018; Couchman 2019. [↑](#footnote-ref-17)
18. Human Rights Watch. (2017). China: Police ‘big data’ systems violate privacy, target dissent. Retrieved June 25, 2019, from <https://reurl.cc/A1Z8ld>; Human Rights Watch. (2019). *World report 2019*. Retrieved June 25, 2019, from <https://reurl.cc/6g641d>. [↑](#footnote-ref-18)
19. Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. Rand Corporation. Retrieved Jan 16, 2020, from <https://reurl.cc/QpQ3k0>. [↑](#footnote-ref-19)
20. Amnesty International UK 2018; Hardyns and Rummens 2018. [↑](#footnote-ref-20)
21. Jo 2017. [↑](#footnote-ref-21)
22. Michal S Gal, ‘Algorithmic Challenges to Autonomous Choice’ (2018) 25(1) Michigan Telecommunications and Technology Law Review 59, 65; Peter Flach, *Machine Learning: The Art and Science of Algorithms that Make Sense of Data* (Cambridge University Press 2012) 3. [↑](#footnote-ref-22)
23. Mittelstadt et al, ‘The Ethics of Algorithms: Mapping the Debate’ (2016) July–December Big Data & Society 1, 5;  Lindsey Barrett, ‘Reasonably Suspicious Algorithms: Predictive Policing at the United States Border’ (2017) 41(3) NYU Review of Law & Social Change 327, 340–41. [↑](#footnote-ref-23)
24. (Couchman 2019; Richardson et al. 2019. [↑](#footnote-ref-24)
25. **Joh 2017, 287;** Beth Pearsall, ‘Predictive Policing: The Future of Law Enforcement?’ (2010) 266 NIJ Journal 16. [↑](#footnote-ref-25)
26. **Mittelstadt et al. 2017, 5.** [↑](#footnote-ref-26)
27. Barrett 2017, **340–41** [↑](#footnote-ref-27)
28. Frank Pasquale, *The Black Box Society* (Harvard University Press 2015) 3. [↑](#footnote-ref-28)
29. Barrett 2017, 344. [↑](#footnote-ref-29)
30. Kroll et al, ‘Accountable Algorithms’ (2017) 165(3) University of Pennsylvania Law Review 633, 638. [↑](#footnote-ref-30)
31. Danielle Keats Citron, ‘Technological Due Process’ (2008) 85(6) Washington University Law Review 1249, 1271–72; Ferguson 2017a, 1178. [↑](#footnote-ref-31)
32. Barrett 2017, 327. [↑](#footnote-ref-32)
33. **Regulation 2016/679; Directive 2016/680.** [↑](#footnote-ref-33)
34. For an oiverview, see <https://kops.uni-konstanz.de/server/api/core/bitstreams/10477c12-a4b9-46b2-b9d0-5b58cbd127bf/content> and <https://penal.org/sites/default/files/files/A-02-23.pdf> [↑](#footnote-ref-34)
35. BVerfG, 1 BvR 1547/19, 16 February 2023, available at <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html> . [↑](#footnote-ref-35)
36. Ohyama, T., Amemiya, M. Applying Crime Prediction Techniques to Japan: A Comparison Between Risk Terrain Modeling and Other Methods. *Eur J Crim Policy Res* **24**, 469–487 (2018). [↑](#footnote-ref-36)
37. <https://www.japan.go.jp/kizuna/2024/06/japans_ai-based_crime_prediction.html> . [↑](#footnote-ref-37)