Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations

Kimon Kieslich
k.kieslich@uva.nl
University of Amsterdam
Amsterdam, Netherlands

Marco Lünich
marco.luenich@hhu.de
Heinrich Heine University Düsseldorf
Düsseldorf, Germany

ABSTRACT

AI is increasingly being used in the public sector, including public security. In this context, the use of AI-powered remote biometric identification (RBI) systems is a much-discussed technology. RBI systems are used to identify criminal activity in public spaces, but at the same time they are criticised for inheriting biases and violating fundamental human rights. As a result, the use of RBI poses risks to society. It is therefore important to ensure that such systems are developed in the public interest, which means that any technology that is deployed for public use needs to be scrutinised. While there is a broad consensus among business leaders, policymakers and scientists that AI must be developed in an ethical and trustworthy manner, scholars have argued that ethical guidelines do not guarantee ethical AI, but rather prevent stronger regulation of AI for the Common Good. As a possible counterweight, public opinion can have a decisive influence on policymakers (e.g. through voter demands) to establish boundaries and conditions under which AI systems should be used – if at all. However, we know little about the conditions that lead to regulatory demand for AI systems. In this study, we focus on the role of trust in AI as well as trust in law enforcement as potential factors that may lead to demands for regulation of AI technology. In addition, we explore the mediating effects of discrimination perceptions regarding RBI. We test the effects on four different use cases of RBI varying the temporal aspect (real-time vs. post hoc analysis) and purpose of use (persecution of criminals vs. safeguarding public events) in a survey among German citizens. We found that German citizens do not differentiate between the different modes of application in terms of their demand for RBI regulation. Furthermore, we show that perceptions of discrimination lead to a demand for stronger regulation, while trust in AI and trust in law enforcement lead to opposite effects in terms of demand for a ban on RBI systems.

CCS CONCEPTS

• **Human-centered computing → Empirical studies in HCI**; • **Social and professional topics → Governmental regulations**; • **Applied computing → Sociology**; **Law**.

KEYWORDS

Regulation, Trust, Discrimination Perception, Survey Research, Artificial Intelligence, Remote Biometric Identification

ACM Reference Format:
Kimon Kieslich and Marco Lünich. 2024. Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations. In *The 2024 ACM Conference on Fairness, Accountability, and Transparency (FAccT '24), June 03–06, 2024, Rio de Janeiro, Brazil.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3630106.3658548

FAccT '24, June 03–06, 2024, Rio de Janeiro, Brazil

ACM ISBN 979-8-4007-0450-5/24/06
https://doi.org/10.1145/3630106.3658548

1 INTRODUCTION

The European AI Act marks a key regulatory milestone in the regulation of AI. The AI Act guarantees that AI technologies must be classified into different risk classes [16]. It also includes a class of non-acceptable risk technologies. Systems in this class have too far-reaching negative risks for society and/or conflict with the EU's core ethical values. For example, social scoring systems should be banned, as well as, with some exceptions, *real-time* biometric remote identification (RBI) systems [17]. RBI systems analyse biometric data (e.g., faces, fingerprints) to identify individuals. The data is usually collected from video footage, such as surveillance cameras in public areas. Law enforcement agencies, in particular, are eager to use RBI to identify criminals or find missing persons [62]. However, the use of RBI is criticized for standing in conflict with fundamental rights, for instance, in being an unnecessary invasion of people's privacy and for discrimination of citizens [6, 46, 64].

In the European Parliament, the classification of real-time RBI as an unacceptable risk technology has led to some discussions with conservative parties arguing against a ban, as RBI would be useful for strengthening domestic security [14]. The regulation of RBI systems was also a heated discussion point in the final negotiations about the end-version of the EU AI Act. While these discussions take place in political institutions, the opinion of citizens on RBI are also relevant, as the European Parliament and European Council as democratic representative institutions need to heed the demands of citizens to a certain extent.

With the ever-growing influence of AI on society, how citizens want to be *governed* also warrants the interest of social scientists. However, it is not enough to show citizens' opinions on governance proposals, but also to explore what factors influence these demands. This is also of interest for the scholarly AI ethics community as factors may be identified that contribute to critical engagement with AI technology. Researchers already have explored a plethora of influential factors in relation to AI *opinions* and AI *use*. However, less attention has been paid to governance issues.

Therefore, in this study, we aim to contribute empirical evidence on what factors lead citizens to demand stronger regulatory approaches. In particular, we focus on the roles of discrimination perceptions of RBI technologies as well as trust in AI technology and law enforcement as a user of RBI technology. We do this with respect to the use of RBI in different usage contexts: 1) use with the purpose of identifying criminals vs. securing public events (such as the Olympics), and 2) use of RBI after a criminal activity vs. in real time. To gather empirical data, we used a factorial survey of *n=983* German citizens.

2 THE NEED FOR GOVERNANCE OF AI

The use of AI in the public sector is a particularly sensitive area of application, as it can have an impact on the lives of citizens without them having the choice of whether or not to engage with an AI system. There are numerous examples where AI systems have led to detrimental consequences for certain citizens [1]. For example, a tax fraud detection system used by the tax authorities in the Netherlands discriminated against people with certain demographic characteristics, such as gender, age and place of residence [11, 28], leading to the misclassification of thousands of people. These people were ultimately denied access to social services, which had a serious impact on their lives. In the UK, an automated grading system was used to determine students' final exam grades. As most students received significantly lower grades than before, this led to a public protest that resulted in the abolition of the system [33]. Also, in the education sector, an ADM system used for university admissions in France has been abandoned due to fairness issues arising from its use [65]. In the field of public security, there is a huge scientific and political discussion about the use of AI in the criminal justice sector, for example, for bail setting or predictive policing [3, 27].

All of these cases have in common that the AI system in question can be considered to have a high impact on the lives of citizens. However, the use of AI in the public sector is not profit-driven and should serve the public interest [69]. Accordingly, the use of AI must be justified to the public and it must be ensured that the use of AI technology does not cause social harm, i.e., that it meets ethical standards [69]. This approach is consistent with the normative goal of creating AI according to the idea of the Common Good [7, 20, 21], which aims to maximize ethical standards in AI that serve all affected individuals and not just a few stakeholders. However, ethical goals are often traded off against rapid implementation by vendors and developers, due to a strong focus on economic growth and a trial-and-error mentality [25]. This trend can be seen not only in the economic sector, but also in the political arena. The global AI race leads policymakers to prioritize funding and regulation for economic progress, which can lead to the neglect of ethical issues [10]. As a result, policymakers present AI as an inevitable technology that must be advanced quickly to keep pace with other nations [5, 31]. Following this approach, a lot of money is invested in the technology sector, while societal voices are largely ignored [23, 25].

Nevertheless, AI ethics guidelines have been published by several entities, suggesting ways to mitigate the ethical risks of AI systems [2, 19, 22, 26, 30, 51]. However, these guidelines lack a reinforcement mechanism [26, 34]. Stronger regulation could be such a mechanism, leading to the enforcement of ethical standards for AI. Several scholars in the field of AI ethics have already pointed to the need for a regulatory framework for AI [12, 40]. With the EU AI Act, such a framework has now been agreed upon and will be implemented in the EU member states. In principle, the EU AI Act distinguishes between four risk categories: unacceptable risk, high risk, limited risk, and minimal risk [6, 17]. While systems in the unacceptable risk category should be banned outright, systems in the other categories require different forms of regulation to limit the potential negative consequences.

3 REMOTE BIOMETRIC IDENTIFICATION AND THE AI ACT

In this study, we are particularly interested in RBI systems. Law enforcement agencies can use RBI as a predictive policing tool in the pursuit of criminals. The technology enables both real-time identification of people and post hoc analysis of collected video footage. Most RBI systems use facial recognition technology and compare faces to a database [46].

The motivation to deploy RBI systems in the first place is mostly driven by security concerns, largely influenced by the threat of terrorism affecting society on a large scale [8]. There is a widespread belief among policy makers and law enforcement agencies that the use of RBI systems will help in the fight against crime [62] and that the "increased use of technology [...] will render policing more efficient, whether this statement is eventually proven to be true or not." [64]. This changes the focus of law enforcement from prosecuting crimes that have already been committed to a strategy that attempts to prevent crime [64]. However, the use of RBI systems requires the collection of massive amounts of data that are needed to make predictions more reliable. In this sense, these systems are very privacy invasive [38], or, as Vogiatzoglou [64] describes it: "Data are gathered not for a specific criminal investigation but rather for an undetermined purpose, serving a mentality of 'nice-to-have' rather than 'must-have' intelligence. [. . .] Serving this mentality of 'nice-to-have', practices of mass surveillance have increasingly become the most popular means used by both law enforcement and intelligence services in the fight against serious crime."

Consequently, the large-scale application of RBI raises issues about the violation of fundamental rights of citizens, for instance, in terms of privacy, stereotyping, de-individualization and non-discrimination [6, 46, 64]. Furthermore, doubts exist concerning the accuracy, reliability, and security of those systems [46]. Acknowledging these risks, the EU AI Act makes several distinctions in the regulation of RBI. Regarding the *temporal* aspect, real-time data analysis should be *prohibited* with the three exceptions of searching for victims of crime and/or missing children, the prevention of serious crimes such as terrorist attacks, and the prosecution of criminal offenders [6, 46]. The post hoc analysis is *allowed* under legal obligations (e.g. usage has to be authorized by a judge) [6, 17]. The risk classification of RBI systems under the EU AI Act is, thus, dependent on the *temporal* aspect of data analysis (post hoc analysis vs. real-time) and the *purpose* of its usage. Real-time RBI systems should be banned with some exceptions, whereas post hoc analysis RBI systems are classified as high-risk systems. Those high-risk systems, according to the EU AI Act, "must implement a risk management system, use high-quality data sets, draw up technical documentation, enable record-keeping, ensure transparency and provide information to users, ensure human oversight and an appropriate level of robustness, accuracy and cybersecurity" [6]. Additionally, these systems need to be audited by third parties and registered into an EU database [6].

At the time of writing, the final draft of the EU AI Act has not yet been published, and there are reports of exceptions to the real-time use of RBI. In the run-up to the final discussion and vote on the EU AI Act, some political interest groups and parties have opted for more exemptions for the real-time use of RBI. In addition, some national governments also pushed for broader use of real-time RBI (e.g., the French government advocated the use of RBI at the 2024 Olympic Games) in the interest of national security [32]. Many scholars have criticized that the exceptions made for the use of real-time RBI open loopholes for widespread use of the technology [6, 46, 63].

4 PUBLIC OPINION ON AI GOVERNANCE

Given the enormous consequences of the use of RBI for society, the question of society's influence on the regulation of AI remains open. According to Rahwan [48], society needs to be involved in setting norms and regulations on how society wants to interact with AI. In his Society-in-the-Loop (SITL) approach, he opts to integrate public opinion on moral and ethical decisions into the regulatory framework. The call for greater public involvement is shared by several other scholars. For example, Züger and Asghari [69] argue for strengthening public deliberation on AI issues to include the voice of all members of society, and Crawford [12] opts for stronger counter-movements against techno-deterministic approaches. All in all, the AI for the Common Good and Public Interest community is united by the call for a stronger inclusion of societal voices to counterbalance hegemonic political and economic approaches [24, 53, 54, 67, 69]. Taking this call seriously means exploring public opinion on pressing issues related to AI and regulation. The potential use of RBI is arguably one such use case.

Public opinion can be a crucial factor in shaping technology development. In democratic societies, the public can express its political engagement in a variety of ways, such as protesting or, at the most basic level, voting. However, public opinion can only exert pressure if an issue is on the political agenda, i.e. if it is perceived as relevant by the public. The politicization of an issue is, therefore, a crucial factor in public influence. An issue can be perceived as politicized when the public debate is polarized, the issue is intensively reported on, and the issue resonates in society [13, 55]. However, recent surveys from the German context show that AI issues are not overly salient in the German population – in particular, AI ethics issues are not at all on the agenda for most German citizens [36]. Moreover, most German citizens do not consider AI issues overly relevant for their general voting decisions [45].

However, empirical studies focusing on *specific use cases* have shown that the public can be engaged with AI issues. For example, Marcinkowski and colleagues [44] showed that perceptions of unfairness lead to intentions to protest against university admissions systems, and Lünich and Kieslich [43] showed that distrust of AI systems leads to them being perceived as illegitimate. As mentioned above, several counter-movements against some AI applications have emerged [12]. Further, perceptions of trust in AI have been shown to be a critical factor in technology adoption [5, 57–59]. Additionally, Kieslich and colleagues [36] have shown that awareness of ethical issues of AI leads to higher political engagement.

But it is not only AI-related attitudes that influence political attitudes toward AI. Wenzelburger and colleagues [65] point out that contextual factors also play a role. In an empirical study on AI adoption in the public sector they showed that "the personal importance of the problem that an algorithm is supposed to deal with and the values at stake clearly matter for the extent to which citizens show general support of algorithms in policing" [65]. In addition, they also report that trust in the organisation using AI positively influences its acceptance, while the technological performance of the system has only marginal effects on technology acceptance [65].

In addition, several studies have been conducted that focus on the acceptance of facial recognition technology. Ritchie and colleagues empirically assessed public attitudes toward automatic facial recognition technology in the United Kingdom, Australia, and the United States [49]. They report that the context of use affects support for the use of facial recognition technology in the criminal justice system. Kostka and colleagues examined public opinion on the acceptability of the use of facial recognition technology in China, Germany, the United Kingdom, and the United States [39]. Their survey study distinguished four sets of influencing factors: political context and attitudes, history of surveillance, concerns about public issues, and individual preferences and characteristics. Their findings for the German context suggest that people who perceive facial recognition technology as a general invasion of privacy and a risk tend not to support the use of facial recognition technology. Moreover, German citizens concerned about terrorism and socially unacceptable public behavior also support the use of facial recognition technology. For all countries except Germany, effects were also found for trust in government and technology affinity. For example, people who trust the government and are open to technology also support the use of facial recognition technology. In addition, Trüdinger and Steckermeier showed that political trust leads to higher acceptance of surveillance policies in Germany [61].

However, there is still a lack of research on citizens' demand for concrete governance strategies on AI; in particular, to our knowledge, no other study has focused on the link between public opinion on AI and concrete regulatory measures regarding the EU AI Act. In this study, we focus on three different policy proposals: we distinguish between different regulatory mechanisms in 1) banning the technology due to its classification as an unacceptably risky system, and 2) registering the technology in a public database, as well as 3) the need for independent third-party review, as required in the high-risk category of the EU AI Act [6]. Furthermore, we contribute to the research literature by investigating different explanatory factors for regulatory demands: discrimination perceptions of RBI systems, trust in AI, and trust in law enforcement. We do this with respect to the use of RBI in different contexts: 1) use with the purpose of identifying criminals vs. securing public events, and 2) use of RBI after a criminal activity vs. in real time.

5 RESEARCH QUESTIONS

We first focus on whether the conditions of RBI deployment matter in terms of the regulation demands of the citizens. As outlined earlier, the EU AI Act makes several distinctions regarding the regulation of RBI. We manipulate two conditions of the use of RBI: the *temporal* aspect (post hoc analysis vs. real-time) and *purpose of use* (prosecuting criminals vs. securing public events). Thus, we pose the following research questions.

RQ1: Does the temporal context of data analysis (post hoc analysis vs. real-time) affect the approval of stronger regulatory interventions regarding RBI?

RQ2: Does the purpose of the use of RBI (prosecuting criminals vs. securing public events) affect the approval of stronger regulatory interventions regarding RBI?

Further, we explore the mediating role of discrimination perceptions as a distinct measure of awareness of AI ethics. We ask the question of whether discrimination perceptions are dependent on the context of the use of RBI. Accordingly, we ask:

RQ3: How do perceptions of discrimination mediate the relationship between the temporal context and the support for stronger regulatory interventions regarding RBI?

In the context of AI, trust is often recognized as a critical factor, for example, the EU's policy strategy is to develop a trustworthy approach to AI [15], and trust in AI was also identified as a critical factor for AI adoption [4, 43, 57–59]. In addition, trust in law enforcement, i.e. the agent using RBI systems, was identified as a contributing factor to the use of technology in law enforcement [39, 61]. Thus, we include trust in AI and trust in law enforcement as independent variables in our model. We are interested in the direct effect of the approval of stronger regulatory interventions as well as on the mediation effects of perceptions of discrimination. Hence, we ask:

RQ4a: Does trust in AI affect the approval of stronger regulatory interventions regarding RBI?

RQ4b: Does trust in law enforcement affect the approval of stronger regulatory interventions regarding RBI?

RQ5a: How do perceptions of discrimination mediate the relationship between trust in AI and the support for stronger regulatory interventions regarding RBI?

RQ5b: How do perceptions of discrimination mediate the relationship between trust in law enforcement and the support for stronger regulatory interventions regarding RBI?

In addition, we also include sociodemographic variables as controls, as several studies have shown that these influence technology acceptance or political engagement [9, 18, 29, 35, 36, 68]. Specifically, we pose the following research questions:

RQ6: Do other contextual factors affect the approval of stronger regulatory interventions regarding RBI?

RQ7: How do perceptions of discrimination mediate the relationship between the other contextual factors and the support for stronger regulatory interventions regarding RBI?

5.1 Procedure & Sample

To answer our research questions, we conducted an online survey among German citizens. The data was collected from June 19 to July 7, 2023. To recruit participants, we used the SoSci Panel, which is based on a convenience sample of German-speaking respondents. The SoSci Panel is a joint project of the Institute for Communication Science in Munich and the German Society for Communication Science (DGPuK). As such, it is thoroughly maintained, has strict quality criteria, and an internal peer-review process for studies conducted with the panel. However, the results are not representative of the German population.

As our study aims to explore political engagement and support for governance mechanisms, we decided to include only German citizens in the final sample. The inclusion of other political contexts (such as Swiss or Austrian), while interesting, would have added another layer of complexity to this study that we could not satisfactorily address.

The survey was designed as follows: First, participants had to answer some questions about their media use as well as their personal beliefs about social and political issues. The term AI was then introduced with the following definition: "*There is currently a lot of public talk about 'artificial intelligence' (AI). What is meant here are computer applications that automatically evaluate digital data. For AI, the evaluation of large volumes of data AI represents a learning process from which it continuously processes new information and thus recognizes ever more precise patterns over time. Based on this analysis, facts can be determined, and future developments can be predicted. Artificial intelligence systems can suggest courses of action or make decisions autonomously and or make decisions autonomously and execute them directly.*" Immediately afterwards, the participants had to indicate their trust in AI. We then introduced the use case of our study – Remote Biometric Identification. We manipulated the use of RBI systems in terms of two factors: 1) temporal component (post hoc analysis vs. real-time analysis) and 2) purpose of use (identifying criminals vs. securing public events). Participants were exposed to one of four possible scenarios. After the treatment check, participants answered questions about their concerns regarding the discriminatory impact of RBI. In addition, we asked our dependent variables about support for government action on RBI. Finally, we collected sociodemographic information and measured whether participants followed the EU AI Act debate. The survey was conducted in German.

All in all, 1003 respondents participated in the survey. However, 20 cases had to be excluded as these participants failed the treatment check. Thus, our final sample consists of 983 cases. 538 participants identify as female, 434 identify as male and 11 identify as non-binary. The average age of the respondents is 50 years (*SD*=18.25).

5.2 Measures

5.2.1 Dependent Variables: Support of Regulatory Interventions. We queried the support for regulatory interventions regarding AI with three self-developed items on a five-point Likert scale (1=do not support at all; 5=totally support; -1=don't know). All regulatory interventions are derived from current AI regulations that are either proposed by the EU AI Act or scholars in the field [16, 60]. The question and items read as follows: *At the political level, the* *regulation of AI-based remote biometric identification systems is currently being discussed. How much do you agree that policy should set the following rules?* Remote biometric identification should be banned; Law enforcement agencies should be required to commission independent testing companies (e.g. TÜV[1]) to test the dangers of the system before introducing remote biometric identification; Law enforcement agencies should be required to register remote biometric identification systems and their modes of operation in a public database. The three items will subsequently be addressed in short form as (1) ban, (2) audit, and (3) database registration.

5.2.2 Mediator: Discrimination Perception. Discrimination perception through RBI was measured via five items on a five-point Likert scale (1=do not support at all; 5=totally support; -1=don't know) that were adapted from Kieslich et al. [37]. The items that show good factorial validity and internal consistency (Cronbach's α = 0.88, Average Variance Extracted (AVE) = 0.60) read as follows: *If you now think about the consequences of using AI for remote biometric identification. To what extent do you agree or disagree with the following statements?* The use of RBI creates injustices. RBI systematically puts certain groups of people at a disadvantage. Existing inequalities are reinforced by the use of RBI. RBI creates new inequalities. The use of RBI leads to discrimination.

5.2.3 Independent Variables. **Use case of RBI.** As outlined above, respondents were confronted with one of four possible stimuli. We manipulated the *temporal* aspect (0 = post hoc analysis, 1 = real-time analysis) and the *purpose of use* (0 = public event, 1 = prosecution of criminals). The wording of the stimuli can be found in the Appendix.

Trust in AI. For trust in AI, respondents rated four statements on a five-point Likert scale (1=do not support at all; 5=totally support). The scale was adopted from Lünich and Kieslich [43] as well as Shin [58]. The items that show good factorial validity and internal consistency (Cronbach's α = 0.90, AVE = 0.69) read as follows: I trust that AI systems can make correct decisions; I trust the decisions made by AI systems; Decisions made by AI systems are trustworthy; I believe that decisions made by AI systems are reliable.

Trust in Police and Law Enforcement. Trust in police and law enforcement was measured with the same item wording and scale as the trust in AI except replacing the word "AI" with "police and law enforcement". Again, this scale was adopted from Lünich and Kieslich [43] and Shin [58]. The items that show good factorial validity and internal consistency (Cronbach's α = 0.96, AVE = 0.86) read as follows: *To what extent do you agree or disagree with the following statements?* I trust that German police and law enforcement authorities can make the right decisions; I trust the decisions made by German police and law enforcement authorities; Decisions made by German police and law enforcement authorities are trustworthy; I believe that the decisions made by German police and law enforcement authorities are reliable.

5.2.4 Controls. **Experienced Discrimination.** Experienced discrimination was measured on a five-point Likert scale (1=never; 2=seldom; 3=sometimes; 4=often; 5=very often). The item formulation was adopted from Schumann and colleagues [56], which is the German translation of the scale from Williams et al. [66]. The items that show good factorial validity and internal consistency (Cronbach's α = 0.88, AVE = 0.60) read as follows: *How often have any of the following things happened to you in your everyday life?* You were treated with less respect than other people; Someone acted as if you were not taken seriously; You were threatened or harassed.

Domestic Security Concerns. Domestic Security Concerns was measured with one item on a four-point Likert scale (1=not at all concerned; 2=a little concerned; 3=concerned; 4=very concerned) that was adopted from Wenzelburger et al. [65]. It reads: *Please indicate - intuitively - how worried you are about internal security in Germany.*

Other Controls. Additionally, we queried if the respondents have heard about the EU AI Act before (1=yes), as well as gender gender (1=female) and age (in years).

6 RESULTS

We conducted our data analysis using a structural regression model, employing the *lavaan* package in R [52]. The model encapsulated both the direct effects of the stimuli and other independent variables on the three dependent variables concerning support for regulatory interventions, and the indirect effects mediated through perceptions of resulting discrimination by RBI.

We subsequently present the results for each dependent variable separately when focusing on direct and indirect effects for enhanced clarity and comprehension. Table 1 below details the support for a ban on RBI, Table 2 presents findings on mandatory auditing of RBI systems, and Table 3 focuses on the necessity for registering all RBI systems in a public database. Given that our convenience sample size was not determined by a priori power analysis, we will subsequently concentrate on results where total standardized effects exceed .1 as the smallest effect size of interest. This approach will ensure a more focused examination of practically significant findings, emphasizing effects that are not only statistically significant but also of substantive importance in the context of our study. Overall, the structural regression model shows good fit ($\chi^2(224)$ = 605.03, p < 0.001; *RMSEA* = 0.042, *90% CI* [0.038, 0.046]; *TLI* = 0.963).

6.1 Banning RBI

Concerning the policy advocating for a complete ban on RBI (see Table 1), the findings for the total effects indicate no significant differences attributable to either the temporal condition (B = 0.010, *SE* = 0.094, *95% CI* (-0.174, 0.195), p = 0.913, β = 0.003) or the purpose of use (B = -0.035, *SE* = 0.094, *95% CI* (-0.219, 0.150), p = 0.712, β = -0.011).

Regarding the direct effects, on the one hand, the results reveal that both a higher trust in law enforcement (B = -0.236, *SE* = 0.054, *95% CI* (-0.341, -0.131), p < 0.001, β = -0.140) and a greater trust in AI among citizens (B = -0.215, *SE* = 0.059, *95% CI* (-0.330, -0.099), p < 0.001, β = -0.110) are linked to decreased support for a ban on RBI. Moreover, results suggest that regarding the support for a ban on RBI, discrimination perceptions had a strong positive effect (B = 0.543, *SE* = 0.041, *95% CI* (0.462, 0.624), p < 0.001, β =

[1]TÜV (short for Technischer Überwachungsverein [technical inspection association]) are German oversight organizations for technical safety checks. The TÜV is well-known in Germany as they are also conducting mandatory car inspections.

0.413). As a consequence, discrimination perceptions mediate these effects of trust in law enforcement (B = -0.190, *SE* = 0.028, *95% CI* (-0.244, -0.136), $p < 0.001$, $\beta = -0.113$) and trust in AI (B = -0.133, *SE* = 0.028, *95% CI* (-0.188, -0.077), $p < 0.001$, $\beta = -0.068$) on supporting a ban on RBI as suggested by the indirect effects, underscoring the influence of trust levels on attitudes towards RBI regulation. Moreover, when citizens had previously heard of the AI Act, there was a direct positive effect on support for a RBI ban (B = 0.269, *SE* = 0.106, *95% CI* (0.061, 0.477), $p = 0.011$, $\beta = 0.071$). This effect was mediated by discrimination perceptions (B = 0.165, *SE* = 0.050, *95% CI* (0.067, 0.263), $p < 0.001$, $\beta = 0.044$). Awareness of the AI Act came with heightened perceptions of discrimination, which in turn contributed to increased support for the ban.

6.2 Auditing RBI systems

Concerning the demand for mandatory audits of RBI systems (see Table 2), the findings for the total effects also indicate no significant differences attributable to either the temporal condition (B = -0.140, *SE* = 0.099, *95% CI* (-0.333, 0.054), $p = 0.157$, $\beta = -0.045$) or the purpose of use (B = 0.175, *SE* = 0.098, *95% CI* (-0.018, 0.368), $p = 0.075$, $\beta = 0.056$).

Moreover, neither trust in law enforcement (B = -0.032, *SE* = 0.059, *95% CI* (-0.147, 0.083), $p = 0.587$, $\beta = -0.019$) nor trust in AI had a significant total effect on the demand for mandatory audits of RBI systems (B = -0.069, *SE* = 0.066, *95% CI* (-0.198, 0.061), $p = 0.298$, $\beta = -0.036$).

When it comes to significant direct effects, respondents' age was the only factor showing a negative direct effect on support for mandatory RBI audits (B = -0.009, *SE* = 0.003, *95% CI* (-0.015, -0.003), $p = 0.002$, $\beta = -0.109$). Specifically, older respondents were less inclined to favour these audits. However, discrimination perceptions whose effect on the approval of mandatory auditing of RBI systems was less pronounced regarding audit demands than it was for a proposed ban (B = 0.162, *SE* = 0.047, *95% CI* (0.069, 0.254), $p < 0.001$, $\beta = 0.124$) did not mediate the effect of age on support for mandatory RBI audits (B = 0.000, *SE* = 0.000, *95% CI* (-0.001, 0.000), $p = 0.268$, $\beta = -0.005$).

6.3 Database registration of RBI systems

Concerning the demand for mandatory registration of RBI systems in a public database (see Table 3), the findings for the total effects also indicate no significant differences attributable to either the temporal condition (B = 0.050, *SE* = 0.130, *95% CI* (-0.205, 0.304), $p = 0.703$, $\beta = 0.012$) or the purpose of use (B = -0.156, *SE* = 0.129, *95% CI* (-0.409, 0.098), $p = 0.229$, $\beta = -0.038$).

Moreover, again, neither trust in law enforcement (B = -0.131, *SE* = 0.077, *95% CI* (-0.282, 0.020), $p = 0.089$, $\beta = -0.060$) nor trust in AI had a significant total effect on the demand for mandatory database registration of RBI systems (B = -0.050, *SE* = 0.087, *95% CI* (-0.220, 0.119), $p = 0.561$, $\beta = -0.020$).

Regarding the significant direct effects, respondents' gender was the only factor showing a direct effect on support for mandatory registration of RBI systems in a public database (B = -0.477, *SE* = 0.133, *95% CI* (-0.737, -0.217), $p < 0.001$, $\beta = -0.116$). Specifically, respondents who identified as female showed less inclination towards favouring the registration of databases. However, discrimination perceptions whose effect on the approval of mandatory public database registration of RBI systems was again less pronounced than it was for a proposed ban (B = 0.258, *SE* = 0.062, *95% CI* (0.137, 0.379), $p < 0.001$, $\beta = 0.151$) did not mediate the effect of gender on support for mandatory registration of RBI systems in a public database (B = 0.014, *SE* = 0.020, *95% CI* (-0.025, 0.053), $p = 0.469$, $\beta = 0.003$).

7 DISCUSSION

Our results yield important insights for the study of public opinion concerning the different contextual use conditions of RBI, trust in AI, trust in law enforcement, discrimination perceptions regarding AI technology, and their practical relevance for implementing regulations.

7.1 The Perceived Context-Independence of RBI Use

The absent effects of the experimental conditions – both as direct and mediated effects via discrimination perceptions – suggest that differences concerning the specific design and aim of RBI systems are rather irrelevant to citizens' demands for regulation. This is especially interesting in consideration of the different risk classifications of the temporal component in the EU AI Act [17]. While the EU AI Act defines real-time systems as unacceptably risky, its usage in post hoc analysis is merely defined as high-risk. This difference is, however, not mirrored in citizens' perceptions regarding regulatory demands.

However, it is unclear whether citizens are unable to distinguish between the risk levels or whether they perceive them as equally risky. This raises the question of whether citizens are overly concerned with how these surveillance systems are ultimately designed. This may suggest a restriction on the influence of public opinion in nuanced policy matters. For example, respondents may not fully grasp the privacy concerns associated with the real-time application of RBI. In such scenarios, RBI surveillance occurs indiscriminately, monitoring all citizens irrespective of any criminal activity. Conversely, in post hoc analysis, the utilization of RBI is typically predicated on the occurrence of a significant crime, warranting the examination of video footage after the event. Nonetheless, considering the limited public engagement with AI technology in general [36], it is plausible that many citizens are not adequately informed about the varying degrees of impact associated with these technologies.

Consequently, political decision-makers and interest groups have even more responsibility in recognizing the scope of different contexts of the use of RBI. Taking public interest orientation seriously also encompasses balancing the risks and benefits of AI systems, even if citizens may not be aware of it. Given these insights, advocacy groups championing marginalized communities or human rights should prioritize conveying the potential risks associated with distinct RBI systems. They ought to emphasize the privacy and discrimination concerns that can arise from employing RBI, particularly in real-time scenarios. Concurrently, law enforcement entities are likely to advocate for the conditional use of RBI in exceptional circumstances, such as child protection or counter-terrorism efforts. In the absence of a widespread public debate, these nuanced

	Estimate	Std. Error	z-value	p-value	95% Confidence Interval Lower	Upper	Std. All
Direct Effects							
Temporal Condition (0 = post hoc analysis, 1 = real-time analysis -> Ban	-0.006	0.087	-0.067	0.946	-0.176	0.164	-0.002
Purpose of Use (0 = Public Event, 1 = Prosecution of Criminals -> Ban	-0.011	0.087	-0.129	0.898	-0.181	0.159	-0.004
Trust in Law Enforcement -> Ban	-0.236	0.054	-4.400	<.001	-0.341	-0.131	-0.140
Trust in AI -> Ban	-0.215	0.059	-3.644	<.001	-0.330	-0.099	-0.110
Experienced Discrimination -> Ban	-0.181	0.082	-2.213	0.027	-0.341	-0.021	-0.077
'Heard of AI Act?' (1 = Yes) -> Ban	0.269	0.106	2.539	0.011	0.061	0.477	0.071
Domestic Security Concerns -> Ban	-0.051	0.055	-0.928	0.353	-0.159	0.057	-0.027
Gender (1 = female) -> Ban	-0.207	0.090	-2.316	0.021	-0.383	-0.032	-0.066
Age -> Ban	-0.003	0.003	-1.201	0.230	-0.008	0.002	-0.037
Mediator: Discrimination Perceptions -> Ban	0.543	0.041	13.097	<.001	0.462	0.624	0.413
Indirect Effects							
Temporal Condition (0 = post hoc analysis, 1 = real-time analysis -> Discrimination Perceptions -> Ban	0.016	0.040	0.405	0.686	-0.062	0.094	0.005
Purpose of Use (0 = Public Event, 1 = Prosecution of Criminals -> Discrimination Perceptions -> Ban	-0.024	0.040	-0.590	0.555	-0.102	0.055	-0.007
Trust in Law Enforcement -> Discrimination Perceptions -> Ban	-0.190	0.028	-6.871	<.001	-0.244	-0.136	-0.113
Trust in AI -> Discrimination Perceptions -> Ban	-0.133	0.028	-4.664	<.001	-0.188	-0.077	-0.068
Experienced Discrimination -> Discrimination Perceptions -> Ban	0.060	0.038	1.573	0.116	-0.015	0.134	0.025
'Heard of AI Act?' (1 = Yes) -> Discrimination Perceptions -> Ban	0.165	0.050	3.307	<.001	0.067	0.263	0.044
Domestic Security Concerns -> Discrimination Perceptions -> Ban	-0.092	0.026	-3.515	<.001	-0.143	-0.041	-0.049
Gender (1 = female) -> Discrimination Perceptions -> Ban	0.030	0.041	0.735	0.462	-0.050	0.111	0.010
Age -> Discrimination Perceptions -> Ban	-0.001	0.001	-1.166	0.243	-0.004	0.001	-0.017
Total Effects							
Temporal Condition (0 = post hoc analysis, 1 = real-time analysis -> Ban	0.010	0.094	0.110	0.913	-0.174	0.195	0.003
Purpose of Use (0 = Public Event, 1 = Prosecution of Criminals -> Ban	-0.035	0.094	-0.369	0.712	-0.219	0.150	-0.011
Trust in Law Enforcement -> Ban	-0.425	0.056	-7.599	<.001	-0.535	-0.316	-0.253
Trust in AI -> Ban	-0.347	0.063	-5.519	<.001	-0.471	-0.224	-0.178
Experienced Discrimination -> Ban	-0.121	0.088	-1.368	0.171	-0.294	0.052	-0.051
'Heard of AI Act?' (1 = Yes) -> Ban	0.434	0.115	3.791	<.001	0.210	0.659	0.115
Domestic Security Concerns -> Ban	-0.143	0.059	-2.407	0.016	-0.259	-0.027	-0.076
Gender (1 = female) -> Ban	-0.177	0.097	-1.821	0.069	-0.368	0.014	-0.056
Age -> Ban	-0.005	0.003	-1.601	0.109	-0.010	0.001	-0.053

Table 1: Mediation model on support of banning RBI

	Estimate	Std. Error	z-value	p-value	95% Confidence Interval Lower	Upper	Std. All
Direct Effects							
Temporal Condition (0 = post hoc analysis, 1 = real-time analysis -> Audit	-0.145	0.098	-1.474	0.140	-0.337	0.048	-0.046
Purpose of Use (0 = Public Event, 1 = Prosecution of Criminals -> Audit	0.182	0.098	1.861	0.063	-0.010	0.374	0.058
Trust in Law Enforcement -> Audit	0.025	0.061	0.408	0.683	-0.094	0.143	0.015
Trust in AI -> Audit	-0.029	0.067	-0.437	0.662	-0.160	0.101	-0.015
Experienced Discrimination -> Audit	-0.069	0.092	-0.746	0.456	-0.249	0.112	-0.030
'Heard of AI Act?' (1 = Yes) -> Audit	0.164	0.120	1.368	0.171	-0.071	0.399	0.044
Domestic Security Concerns -> Audit	0.083	0.062	1.329	0.184	-0.039	0.205	0.045
Gender (1 = female) -> Audit	-0.015	0.101	-0.146	0.884	-0.213	0.184	-0.005
Age -> Audit	-0.009	0.003	-3.086	0.002	-0.015	-0.003	-0.109
Mediator: Discrimination Perceptions -> Audit	0.162	0.047	3.436	<.001	0.069	0.254	0.124
Indirect Effects							
Temporal Condition (0 = post hoc analysis, 1 = real-time analysis -> Discrimination Perceptions -> Audit	0.005	0.012	0.402	0.688	-0.019	0.028	0.002
Purpose of Use (0 = Public Event, 1 = Prosecution of Criminals -> Discrimination Perceptions -> Audit	-0.007	0.012	-0.582	0.560	-0.031	0.017	-0.002
Trust in Law Enforcement -> Discrimination Perceptions -> Audit	-0.056	0.018	-3.155	0.002	-0.092	-0.021	-0.034
Trust in AI -> Discrimination Perceptions -> Audit	-0.039	0.014	-2.828	0.005	-0.067	-0.012	-0.020
Experienced Discrimination -> Discrimination Perceptions -> Audit	0.018	0.012	1.438	0.150	-0.006	0.042	0.008
'Heard of AI Act?' (1 = Yes) -> Discrimination Perceptions -> Audit	0.049	0.020	2.421	0.015	0.009	0.089	0.013
Domestic Security Concerns -> Discrimination Perceptions -> Audit	-0.027	0.011	-2.491	0.013	-0.049	-0.006	-0.015
Gender (1 = female) -> Discrimination Perceptions -> Audit	0.009	0.013	0.719	0.472	-0.016	0.034	0.003
Age -> Discrimination Perceptions -> Audit	0.000	0.000	-1.109	0.268	-0.001	0.000	-0.005
Total Effects							
Temporal Condition (0 = post hoc analysis, 1 = real-time analysis -> Audit	-0.140	0.099	-1.417	0.157	-0.333	0.054	-0.045
Purpose of Use (0 = Public Event, 1 = Prosecution of Criminals -> Audit	0.175	0.098	1.779	0.075	-0.018	0.368	0.056
Trust in Law Enforcement -> Audit	-0.032	0.059	-0.543	0.587	-0.147	0.083	-0.019
Trust in AI -> Audit	-0.069	0.066	-1.041	0.298	-0.198	0.061	-0.036
Experienced Discrimination -> Audit	-0.051	0.093	-0.550	0.582	-0.232	0.130	-0.022
'Heard of AI Act?' (1 = Yes) -> Audit	0.213	0.120	1.779	0.075	-0.022	0.448	0.057
Domestic Security Concerns -> Audit	0.056	0.062	0.893	0.372	-0.066	0.177	0.030
Gender (1 = female) -> Audit	-0.006	0.102	-0.057	0.955	-0.205	0.194	-0.002
Age -> Audit	-0.010	0.003	-3.211	0.001	-0.016	-0.004	-0.113

Table 2: Mediation model on support of stronger auditing of RBI

	Estimate	Std. Error	z-value	p-value	95% Confidence Interval Lower	Upper	Std. All
Direct Effects							
Temporal Condition (0 = post hoc analysis, 1 = real-time analysis -> Database Registration	0.042	0.129	0.326	0.745	-0.210	0.294	0.010
Purpose of Use (0 = Public Event, 1 = Terrorism -> Database Registration	-0.144	0.128	-1.125	0.260	-0.396	0.107	-0.035
Trust in Law Enforcement -> Database Registration	-0.041	0.079	-0.517	0.605	-0.197	0.115	-0.019
Trust in AI -> Database Registration	0.013	0.087	0.145	0.884	-0.159	0.184	0.005
Experienced Discrimination -> Database Registration	-0.035	0.121	-0.291	0.771	-0.272	0.202	-0.011
'Heard of AI Act?' (1 = Yes) -> Database Registration	0.086	0.157	0.545	0.586	-0.223	0.394	0.017
Domestic Security Concerns -> Database Registration	-0.102	0.082	-1.248	0.212	-0.262	0.058	-0.042
Gender (1 = female) -> Database Registration	-0.477	0.133	-3.592	<.001	-0.737	-0.217	-0.116
Age -> Database Registration	0.004	0.004	1.123	0.261	-0.003	0.012	0.039
Mediator: Discrimination Perceptions -> Database Registration	0.258	0.062	4.186	<.001	0.137	0.379	0.151
Indirect Effects							
Temporal Condition (0 = post hoc analysis, 1 = real-time analysis -> Discrimination Perceptions -> Database Registration	0.008	0.019	0.403	0.687	-0.030	0.045	0.002
Purpose of Use (0 = Public Event, 1 = Terrorism -> Discrimination Perceptions -> Database Registration	-0.011	0.019	-0.585	0.559	-0.049	0.026	-0.003
Trust in Law Enforcement -> Discrimination Perceptions -> Database Registration	-0.090	0.024	-3.702	<.001	-0.138	-0.042	-0.041
Trust in AI -> Discrimination Perceptions -> Database Registration	-0.063	0.020	-3.195	0.001	-0.102	-0.024	-0.025
Experienced Discrimination -> Discrimination Perceptions -> Database Registration	0.028	0.019	1.484	0.138	-0.009	0.066	0.009
'Heard of AI Act?' (1 = Yes) -> Discrimination Perceptions -> Database Registration	0.078	0.030	2.645	0.008	0.020	0.136	0.016
Domestic Security Concerns -> Discrimination Perceptions -> Database Registration	-0.044	0.016	-2.743	0.006	-0.075	-0.012	-0.018
Gender (1 = female) -> Discrimination Perceptions -> Database Registration	0.014	0.020	0.725	0.469	-0.025	0.053	0.003
Age -> Discrimination Perceptions -> Database Registration	-0.001	0.001	-1.127	0.260	-0.002	0.001	-0.006
Total Effects							
Temporal Condition (0 = post hoc analysis, 1 = real-time analysis -> Database Registration	0.050	0.130	0.382	0.703	-0.205	0.304	0.012
Purpose of Use (0 = Public Event, 1 = Terrorism -> Database Registration	-0.156	0.129	-1.202	0.229	-0.409	0.098	-0.038
Trust in Law Enforcement -> Database Registration	-0.131	0.077	-1.703	0.089	-0.282	0.020	-0.060
Trust in AI -> Database Registration	-0.050	0.087	-0.581	0.561	-0.220	0.119	-0.020
Experienced Discrimination -> Database Registration	-0.007	0.122	-0.056	0.956	-0.245	0.232	-0.002
'Heard of AI Act?' (1 = Yes) -> Database Registration	0.164	0.158	1.041	0.298	-0.145	0.473	0.033
Domestic Security Concerns -> Database Registration	-0.146	0.082	-1.782	0.075	-0.306	0.015	-0.060
Gender (1 = female) -> Database Registration	-0.462	0.134	-3.453	<.001	-0.725	-0.200	-0.112
Age -> Database Registration	0.004	0.004	0.943	0.346	-0.004	0.012	0.033

Table 3: Mediation model on support of registration of RBI in public database

yet critical discussions risk being monopolized by specific stakeholder factions, excluding broader citizen input. Consequently, the dynamics of power within these stakeholder groups are poised to predominantly influence the ultimate decisions regarding RBI usage, thereby reinforcing a top-down approach in AI governance.

7.2 Trust as a Double-Edged Sword in Regard to Strong Regulation

We found that trust plays a pivotal role in the support of banning RBI technology. Considering the total effects of trust in law enforcement and trust in AI on the dependent variables, we identified negative effects for the demands for a ban, while we found no significant total effects for the demand for registering RBIs in a public database and their mandatory audit by third parties. If people trust in the deployers and developers of the technology, they are less likely demanding a ban on RBI. Trust, as such, can be interpreted as a passing of responsibility towards other actors: either law enforcement, who applies the technology, or the technology (or developing) companies, that guarantee the functioning of the technology.

In addition, discrimination perceptions of RBI technology mediate the effect of the trust variables on a demand for a ban. Trust in law enforcement and trust in AI leads to lower perceptions of the discriminatory impact of AI. If people trust the technology or law enforcement, it also weakens discrimination perceptions, which, otherwise, have a high positive impact on citizens' demand for a ban. Thus, higher trust dampens this effect. Eventually, if the technology seems trustworthy and citizens believe in the actors that apply the technology, discrimination concerns diminish, and consequently, people are less likely to opt for a ban on RBI technology.

These findings are in line with previous research focusing on the link between trust in AI and AI adoption [4, 43, 57–59]. Trust leads citizens to use and accept AI technology. However, several scholars also noted the potential detrimental effects of overtrust, i.e. trusting even malfunctioning systems that may negatively affect the user and/or society [41, 50]. Ultimately, it also depends on the system's technical capabilities and societal effects if trusting AI systems leads to positive outcomes in the sense of the public interests. In the case of RBI systems, several scholars have warned regarding their potential for human rights violations and their actual performance [6, 46, 64]. On the other side, law enforcement stresses the benefits for security that these systems might entail [8, 62]. Thus, in the end, supporting regulatory governance policies is also a result of a trade-off of perceptions between the benefits and risks of the technology.

These findings yield important implications for stakeholders who communicate about AI. On the one hand, fueling distrust in AI may lead to more awareness regarding discriminatory impacts, which in turn influences the demand for strong regulations. On the other hand, the EU strives for the development of trustworthy AI systems [15]. That results in the question of how and if a way can be found to do both – strengthening critical evaluation and trust in (good) AI systems. Trust, as found in our study, is more a double-edged sword. Consequently, trust needs to be calibrated to ensure that citizens do not overtrust a risky technology, which may lead to detrimental consequences for society.

7.3 The Impact of Additional Factors

In addition to the effects of trust, we examined other factors that have been found to steer public opinion towards AI and the respondents' awareness of the AI Act itself. We found that having heard of the AI Act impacts the demand for a ban on RBI technology. As the AI Act focuses on risk classification – and RBI are deemed as either unacceptable or high risk – it is plausible that the use of RBI in the context of the AI Act is also perceived as risky and is connected to discrimination perceptions as some interest groups are actively highlighting exactly those harms. Therefore, individuals previously aware of the EU AI Act are also more likely to be informed about its ethical implications. Conversely, familiarity with the EU AI Act might indicate prior engagement with AI issues, indicating increased involvement in individual research, media coverage, or personal discussions related to the AI Act. This engagement in discussions about AI and its societal impact influences people's perceptions. While the exact causal relationship requires further investigation, this finding underscores the importance of involving citizens in dialogues about AI's applications and risks. Such involvement could significantly influence democratic decision-making processes.

Our study also showed that age negatively correlates with the perceived need for auditing. This trend could stem from older individuals' prior experiences, which may have led to a certain disillusionment with auditing practices in various societal domains. Additionally, our data indicates that male participants are more inclined to support the registration of RBI systems in a public database. Future research could explore the underlying reasons for these demographic differences by expanding on these findings. For instance, it would be insightful to examine how generational experiences and gender perspectives shape attitudes towards transparency and oversight in the realm of AI technologies. This exploration could provide valuable insights into tailoring communication and policy strategies to address different demographic groups' diverse concerns and viewpoints regarding AI governance.

7.4 The Role of Discrimination Perceptions

As outlined above, discrimination perceptions regarding RBI technology only mediate some effects. However, looking at the direct effects of citizens' discrimination perceptions on the demand for different types of regulation is also worthwhile.

While perceptions of RBI's discriminatory impacts are not directly affected by the contextual configurations of RBI systems, they are associated with support for regulatory measures. A general awareness of discrimination related to RBI systems impacts regulatory demands. This effect is more reflective of an overarching attitude towards RBI's discriminatory implications rather than its specific applications. This aligns with Kieslich et al.'s [36] findings, who highlight that ethical issue awareness intensifies political engagement with AI.

Notable disparities emerge when scrutinizing the impact of the three dependent variables. The most pronounced effects are observed in the context of supporting a complete ban on RBI systems. In contrast, while the impact of advocating for audits and registrations is significant, it is comparatively modest. Therefore, the perception of RBI as discriminatory propels citizens towards demanding more stringent regulations, specifically advocating for outright bans. Conversely, milder forms of regulation, such as mandatory database registration and auditing, although positively correlated with higher discrimination perceptions, elicit weaker reactions. As discrimination represents a serious concern in the context of human rights, it is plausible that people tend to opt for an outright ban rather than a mild form of regulation if they think that problematic discrimination is likely to happen when deploying RBI. This is also in line with the notion of unacceptable risk as classified by the EU AI Act. In this argumentation, some technologies are too risky to be implemented into society. It seems like if people perceive this risk, then they also opt for setting limits to the introduction of AI technologies.

This is a promising finding for the AI ethics community as it shows that awareness of discriminatory risks regarding RBI can, in fact, impact the support of regulatory approaches. However, in light of the findings above, this attitude is not nuanced in the sense that it is tied to the context of the use of RBI but rather reflects a general attitude towards RBI. Further, as elaborated above, trust in AI or in law enforcement can weaken discrimination perceptions. Thus, it remains an open question how discrimination perceptions can become more nuanced and reflective, leading to a deliberate and careful demand for regulation. Future research should try to fill this gap and illuminate the impact of additional predictors of regulatory demands. One potential factor frequently discussed in this regard could be strengthening AI literacy, especially regarding the social impacts of the technology [42, 47].

8 CONCLUSION

In this study, we tapped into German citizens' perceptions of the regulation of RBI systems. RBI systems are classified in the draft of the EU AI Act as an unacceptable risk or high risk depending on the temporal aspect and purpose of its application. However, as these classifications are drafted top-down by an expert commission, we explored the opinions of the populace and researched factors that lead to support regulatory measures regarding the use of RBI in different contexts – thus, bringing society in the loop [48]. We were especially interested in aspects of trust in law enforcement as well as in AI technology and discrimination perceptions of RBI systems. Our results from a factorial survey study showed that when it comes to regulation and discrimination perception, citizens do not distinguish between real-time and post hoc use and different purposes of RBI use. The fine-grained distinction made by the EU AI Act is not reflected in citizens' opinion – which questions the ability of citizens to engage in these detailed discussions about the deployment conditions of specific AI applications.

However, we found that general discrimination perceptions of the use of RBI impacts the demand for stronger regulation. If citizens show a high awareness of the discriminatory impact of RBI, they want these technologies to be banned – in terms of the EU AI Act classified as an unacceptable risk. This holds true, even if the technology is – according to the latest version of the AI Act – "only" deemed as high risk. Other counter-measures like stronger auditing or registration of RBI in a public database also finds support but are not as strongly positively influenced as the other dimensions. Interestingly, we also found that trust plays a significant role in smoothing regulatory demands. If citizens trust in law enforcement or in AI, they show less tendency to opt for a ban on RBI systems.

This study has shown the potential for public demands in terms of that awareness in the citizenry can lead to a demand for stronger regulation. At the same time, it also underscores the limitations of public opinion in regard to its inability to detect fine-grained distinctions between different use cases of a risky technology. Despite these limitations, the importance of incorporating citizens' perspectives in AI governance is emphasized, especially when AI is implemented in public domains. This inclusion ensures that the voices of the citizenry are considered in shaping policies for technologies that significantly impact society.

ETHICS STATEMENT

In conducting this research, we adhered to the highest standards of ethical integrity and responsibility. We ensured that all participants were fully informed about the nature and purpose of the research and provided their informed consent. Participant confidentiality and data privacy were rigorously maintained throughout the study. Ethical guidelines, including those pertaining to non-discrimination, fairness, and respect for individuals, were strictly followed. The research methods were designed to minimize potential harm or discomfort to participants. Any conflicts of interest were disclosed and managed appropriately. The questionnaire was reviewed by two academic scholar invited by the SoSci panel; both reviewers did not raise ethical concerns in regard to our study.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

DECLARATION OF GENERATIVE AI IN SCIENTIFIC WRITING

During the preparation of this work, the authors used ChatGPT in order to produce and adjust R and Markdown code for the statistical analysis and the reproducible manuscript. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

REFERENCES

[1] Algorithm Watch. 2020. Automating Society Report 2020. https://automatingsociety.algorithmwatch.org/

[2] Algorithm Watch. 2023. AI Ethics Guidelines Global Inventory. https://inventory.algorithmwatch.org/

[3] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner. 2016. Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. May 2016 (2016). https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

[4] Banu Aysolmaz, Rudolf Müller, and Darian Meacham. 2023. The public perceptions of algorithmic decision-making systems: results from a large-scale survey. *Telematics and Informatics* (2023), 101954. https://doi.org/10.1016/j.tele.2023.101954

[5] Jascha Bareis and Christian Katzenbach. 2022. Talking AI into Being: The Narratives and Imaginaries of National AI Strategies and Their Performative Politics. *Science, Technology, & Human Values* 47, 5 (2022), 016224392110300. https://doi.org/10.1177/01622439211030007

[6] Irena Barkane. 2022. Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance1. *Information Polity* 27, 2 (2022), 147–162. https://doi.org/10.3233/IP-211524

[7] Bettina Berendt. 2019. AI for the Common Good?! Pitfalls, challenges, and ethics pen-testing. *Paladyn, Journal of Behavioral Robotics* 10, 1 (2019), 44–65. https://doi.org/10.1515/pjbr-2019-0004

[8] Ian Brown and Douwe Korff. 2009. Terrorism and the proportionality of internet surveillance. *European Journal of Criminology* 6, 2 (2009), 119–134.

[9] Marco Carradore. 2021. People's Attitudes Towards the Use of Robots in the Social Services: A Multilevel Analysis Using Eurobarometer Data. *International Journal of Social Robotics* 38, 3 (2021), 218. https://doi.org/10.1007/s12369-021-00831-4

[10] Stephen Cave and Seán S. ÓhÉigeartaigh. 2018. An AI Race for Strategic Advantage. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, Jason Furman, Gary Marchant, Huw Price, and Francesca Rossi (Eds.). ACM, New York, NY, USA, 36–40. https://doi.org/10.1145/3278721.3278780

[11] Eva Constantaras, Gabriel Geiger, Justin Casimir Braun, Dhruv Mehrotra, and Htet Aung. 2023. Inside the Suspicion Machine. https://www.wired.com/story/welfare-state-algorithms/

[12] Kate Crawford. 2021. *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press, New Haven and London. https://doi.org/10.12987/9780300252392

[13] Pieter de Wilde. 2011. No Polity for Old Politics? A Framework for Analyzing the Politicization of European Integration. *Journal of European Integration* 33, 5 (2011), 559–575. https://doi.org/10.1080/07036337.2010.546849

[14] EPP Group. 2023. Every second counts to prevent terrorist attacks in Europe. We want law enforcement to use real-time remote biometric identification. Do not fear artificial intelligence but regulate risks and implement strict safeguards! #AI [Image attached] [Tweet]. https://twitter.com/EPPGroup/status/1668309797253398528

[15] European Commission. 2019. Ethics Guidelines for Trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[16] European Commission. 2021. Proposal for a regulation of the European parliament and of the council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=75788

[17] European Parliament. 2023. P9_TA(2023)0236. Artificial Intelligence Act: Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf

[18] Valentina Fietta, Francesca Zecchinato, Brigida Di Stasi, Mirko Polato, and Merylin Monaro. 2021. Dissociation Between Users' Explicit and Implicit Attitudes Toward Artificial Intelligence: An Experimental Study. *IEEE Transactions on Human-Machine Systems* (2021), 1–9. https://doi.org/10.1109/THMS.2021.3125280

[19] Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy, and Madhulika Srikumar. 2020. *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI.* https://doi.org/10.2139/ssrn.3518482

[20] Luciano Floridi, Josh Cowls, Monica Beltrametti, Raja Chatila, Patrice Chazerand, Virginia Dignum, Christoph Luetge, Robert Madelin, Ugo Pagallo, Francesca Rossi, Burkhard Schafer, Peggy Valcke, and Effy Vayena. 2018. AI4People-An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and machines* 28, 4 (2018), 689–707. https://doi.org/10.1007/s11023-018-9482-5

[21] Francesca Foffano, Teresa Scantamburlo, and Atia Cortés. 2022. Investing in AI for social good: an analysis of European national strategies. *AI & SOCIETY* (2022), 1–22. https://doi.org/10.1007/s00146-022-01445-8

[22] Aline Shakti Franzke. 2022. An exploratory qualitative analysis of AI ethics guidelines. *Journal of Information, Communication and Ethics in Society* ahead-of-print, ahead-of-print (2022). https://doi.org/10.1108/JICES-12-2020-0125

[23] Gemma Galdon-Clavell and Virginia Bertelli. 2023. How public money is shaping the future direction of AI: An analysis of the EU's investment in AI development. https://eticas.tech/wp-content/uploads/2023/03/28032023-EU-Investments-Report_ESAIF-and-Eticas.pdf

[24] Anne Gerdes. 2022. A participatory data-centric approach to AI Ethics by Design. *Applied Artificial Intelligence* 36, 1 (2022). https://doi.org/10.1080/08839514.2021.2009222

[25] Anne Gerdes. 2022. The tech industry hijacking of the AI ethics research agenda and why we should reclaim it. *Discover Artificial Intelligence* 2, 1 (2022). https://doi.org/10.1007/s44163-022-00043-3

[26] Thilo Hagendorff. 2020. The Ethics of AI Ethics: An Evaluation of Guidelines. *Minds and Machines* 30, 1 (2020), 99–120. https://doi.org/10.1007/s11023-020-09517-8

[27] Kathrin Hartmann and Georg Wenzelburger. 2021. Uncertainty, risk and the use of algorithms in policy decisions: a case study on criminal justice in the USA. *Policy Sciences* 54, 2 (2021), 269–287. https://doi.org/10.1007/s11077-020-09414-y

[28] Melissa Heikkilä. 2022. Dutch scandal serves as a warning for Europe over risks of using algorithms. https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/

[29] Yuko Ikkatai, Tilman Hartwig, Naohiro Takanashi, and Hiromi M. Yokoyama. 2022. Octagon Measurement: Public Attitudes toward AI Ethics. *International Journal of Human–Computer Interaction* 38, 17 (2022), 1589–1606. https://doi.org/10.1080/10447318.2021.2009669

[30] Anna Jobin, Marcello Ienca, and Effy Vayena. 2019. The global landscape of AI ethics guidelines. *Nature Machine Intelligence* 1, 9 (2019), 389–399. https://doi.org/10.1038/s42256-019-0088-2

[31] Christian Katzenbach. 2021. "AI will fix this" – The Technical, Discursive, and Political Turn to AI in Governing Communication. *Big Data & Society* 8, 2 (2021), 205395172110461. https://doi.org/10.1177/20539517211046182

[32] Laura Kayali. 2023. France sets EU precedent with 2024 Olympics surveillance arsenal. https://www.politico.eu/article/france-eu-precedent-2024-olympics-surveillance/

[33] Anthony Kelly. 2021. A tale of two algorithms: The appeal and repeal of calculated grades systems in England and Ireland in 2020. *British Educational Research Journal* 47, 3 (2021), 725–741. https://doi.org/10.1002/berj.3705

[34] Kimon Kieslich. 2022. Commentary: Societal Reactions to Hopes and Threats of Autonomous Agent Actions: Reflections about Public Opinion and Technology Implementations. *Human–Computer Interaction* 37, 3 (2022), 259–262. https://doi.org/10.1080/07370024.2021.1976642

[35] Kimon Kieslich, Birte Keller, and Christopher Starke. 2022. Artificial intelligence ethics by design. Evaluating public perception on the importance of ethical design principles of artificial intelligence. *Big Data & Society* 9, 1 (2022), 205395172210929. https://doi.org/10.1177/20539517221092956

[36] Kimon Kieslich, Marco Lünich, and Pero Došenović. 2023. Ever Heard of Ethical AI? Investigating the Salience of Ethical AI Issues among the German Population. *International Journal of Human–Computer Interaction* (2023), 1–14. https://doi.org/10.1080/10447318.2023.2178612

[37] Kimon Kieslich, Christopher Starke, Pero Dosenovic, Birte Keller, and Frank Marcinkowski. 2020. Artificial Intelligence and Discrimination. How does the German public think about the discrimination potential of artificial intelligence? https://www.cais.nrw/en/factsheet-2-ai-discrimination/

[38] Demetrius Klitou. 2014. *Privacy-Invading Technologies and Privacy by Design*. Vol. 25. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-026-8

[39] Genia Kostka, Léa Steinacker, and Miriam Meckel. 2023. Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly* 40, 1 (2023), 101761. https://doi.org/10.1016/j.giq.2022.101761

[40] Tobias D. Krafft, Katharina A. Zweig, and Pascal D. König. 2022. How to regulate algorithmic decision–making: A framework of regulatory requirements for different applications. *Regulation & Governance* 16, 1 (2022), 119–136. https://doi.org/10.1111/rego.12369

[41] Sebastian Krügel, Andreas Ostermaier, and Matthias Uhl. 2022. Zombies in the Loop? Humans Trust Untrustworthy AI-Advisors for Ethical Decisions. *Philosophy & Technology* 35, 1 (2022). https://doi.org/10.1007/s13347-022-00511-9

[42] Duri Long and Brian Magerko. 2020. What is AI Literacy? Competencies and Design Considerations. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Regina Bernhaupt, Florian 'Floyd' Mueller, David Verweij, Josh Andres, Joanna McGrenere, Andy Cockburn, Ignacio Avellino, Alix Goguey, Pernille Bjørn, Shengdong Zhao, Briane Paul Samson, and Rafal Kocielnik (Eds.). ACM, New York, NY, USA, 1–16. https://doi.org/10.1145/3313831.3376727

[43] Marco Lünich and Kimon Kieslich. 2022. Exploring the roles of trust and social group preference on the legitimacy of algorithmic decision-making vs. human decision-making for allocating COVID-19 vaccinations. *AI & SOCIETY* (2022), 1–19. https://doi.org/10.1007/s00146-022-01412-3

[44] Frank Marcinkowski, Kimon Kieslich, Christopher Starke, and Marco Lünich. 2020. Implications of AI (un-)fairness in higher education admissions. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, Mireille Hildebrandt, Carlos Castillo, Elisa Celis, Salvatore Ruggieri, Linnet Taylor, and Gabriela Zanfir-Fortuna (Eds.). ACM, New York, NY, USA, 122–130. https://doi.org/10.1145/3351095.3372867

[45] Meinungsmonitor Künstliche Intelligenz. 2023. Dashboard des Meinungsmonitor Künstliche Intelligenz. https://www.cais-research.de/forschung/memoki/memoki-bevoelkerungsbefragung/

[46] Rostam J. Neuwirth. 2023. Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA). *Computer Law & Security Review* 48 (2023), 105798.

[47] Anne Oeldorf-Hirsch and German Neubaum. 2023. What do we know about algorithmic literacy? The status quo and a research agenda for a growing field. *New Media & Society* (2023). https://doi.org/10.1177/14614448231182662

[48] Iyad Rahwan. 2018. Society-in-the-loop: programming the algorithmic social contract. *Ethics and Information Technology* 20, 1 (2018), 5–14. https://doi.org/10.1007/s10676-017-9430-8

[49] Kay L. Ritchie, Charlotte Cartledge, Bethany Growns, Yan, Yuqing Wang, Kun Guo, Robin S. S. Kramer, Gary Edmond, Kristy A. Martire, Mehera San Roque, and David White. 2021. Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world. *PLOS ONE* 16, 10 (2021), e0258241. https://doi.org/10.1371/journal.pone.0258241

[50] Paul Robinette, Wenchen Li, Robert Allen, Ayanna M. Howard, and Alan R. Wagner. 2016. Overtrust of robots in emergency evacuation scenarios. In *2016 11th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*. IEEE, 101–108. https://doi.org/10.1109/HRI.2016.7451740

[51] Cathy Roche, P. J. Wall, and Dave Lewis. 2022. Ethics and diversity in artificial intelligence policies, strategies and initiatives. *AI and ethics* (2022), 1–21. https://doi.org/10.1007/s43681-022-00218-9

[52] Yves Rosseel. 2012. lavaan : An R Package for Structural Equation Modeling. *Journal of Statistical Software* 48, 2 (2012). https://doi.org/10.18637/jss.v048.i02

[53] Catharina Rudschies, Ingrid Schneider, and Judith Simon. 2021. Value Pluralism in the AI Ethics Debate – Different Actors, Different Priorities. *The International Review of Information Ethics* 29 (2021). https://doi.org/10.29173/irie419

[54] Laura Sartori and Andreas Theodorou. 2022. A sociotechnical perspective for the future of AI: narratives, inequalities, and human control. *Ethics and Information Technology* 24, 1 (2022). https://doi.org/10.1007/s10676-022-09624-3

[55] E. E. Schattschneider. 1957. Intensity, Visibility, Direction and Scope. *American Political Science Review* 51, 4 (1957), 933–942. https://doi.org/10.2307/1952444

[56] Maria Schumann, Katja Kajikhina, Antonino Polizzi, Navina Sarma, Jens Hoebel, Marleen Bug, Susanne Bartig, Thomas Lampert, and Claudia Santos-Hövener. 2019. Konzepte für ein migrationssensibles Gesundheitsmonitoring. https://doi.org/10.25646/6071

[57] Donghee Shin. 2020. Expanding the Role of Trust in the Experience of Algorithmic Journalism: User Sensemaking of Algorithmic Heuristics in Korean Users. *Journalism Practice* (2020), 1–24. https://doi.org/10.1080/17512786.2020.1841018

[58] Donghee Shin. 2021. The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI. *International Journal of Human-Computer Studies* 146 (2021), 102551. https://doi.org/10.1016/j.ijhcs.2020.102551

[59] Donghee Shin. 2021. Why Does Explainability Matter in News Analytic Systems? Proposing Explainable Analytic Journalism. *Journalism Studies* 22, 8 (2021), 1047–1065. https://doi.org/10.1080/1461670X.2021.1916984

[60] Ben Shneiderman. 2022. *Human-centered AI*. Oxford University Press, Oxford.

[61] Eva-Maria Trüdinger and Leonie C. Steckermeier. 2017. Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly* 34, 3 (2017), 421–433. https://doi.org/10.1016/j.giq.2017.07.003

[62] Rosamunde van Brakel and Paul de Hert. 2011. Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Technol. Led Policing* 20 (2011), 165–192.

[63] Michael Veale and Frederik Zuiderveen Borgesius. 2021. Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International* 22, 4 (2021), 97–112. https://doi.org/10.9785/cri-2021-220402

[64] Plixavra Vogiatzoglou. 2019. Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity. *European Journal of Law and Technology* 10, 1 (2019).

[65] Georg Wenzelburger, Pascal D. König, Julia Felfeli, and Anja Achtziger. 2022. Algorithms in the public sector. Why context matters. *Public Administration* (2022). https://doi.org/10.1111/padm.12901

[66] D. R. Williams, Yu Yan, J. S. Jackson, and N. B. Anderson. 1997. Racial Differences in Physical and Mental Health: Socio-economic Status, Stress and Discrimination. *Journal of health psychology* 2, 3 (1997), 335–351. https://doi.org/10.1177/135910539700200305

[67] Karen Yeung, Andrew Howes, and Ganna Pogrebna. 2020. AI Governance by Human Rights–Centered Design, Deliberation, and Oversight. In *The Oxford Handbook of Ethics of AI*, Markus D. Dubber, Frank Pasquale, Sunit Das, Karen Yeung, Andrew Howes, and Ganna Pogrebna (Eds.). Oxford University Press, 75–106. https://doi.org/10.1093/oxfordhb/9780190067397.013.5

[68] Baobao Zhang and Allan Dafoe. 2019. Artificial Intelligence: American Attitudes and Trends. *SSRN Electronic Journal* (2019). https://doi.org/10.2139/ssrn.3312874

[69] Theresa Züger and Hadi Asghari. 2022. AI for the public. How public interest theory shifts the discourse on AI. *AI & SOCIETY* (2022). https://doi.org/10.1007/s00146-022-01480-5

APPENDIX

Vignette original (German) wording

Real-Time. **Der Einsatz von biometrischer Fernidentifikation zur 1) Echtzeit-Fahndung nach Schwerverbrecherinnen und Schwerverbrechern 2) Sicherung von Großveranstaltungen**

Ein derzeit von der Politik diskutiertes Thema ist der Einsatz von KI-basierten Systemen zur biometrischen Identifizierung von Personen, sogenannte Systeme zur **biometrischen Fernidentifikation**. Damit sind Computeranwendungen gemeint, die physische Merkmale von Personen (z. B. Gesichter) analysieren und damit konkreten Personen zuordnen können.

Biometrische Fernidentifikation kann von Strafverfolgungsbehörden **in Echtzeit** eingesetzt werden, um Personen zu identifizieren und zu verfolgen, die möglicherweise in kriminelle Aktivitäten verwickelt sind.

Sie funktioniert, indem Kameras oder andere Sensoren Bilder von Gesichtern, Fingerabdrücken oder anderen biometrischen Merkmalen einer Person aufnehmen und diese Bilder mit einer Datenbank bekannter Personen vergleichen.

Die Technologie verwendet Algorithmen und Künstliche Intelligenz, um die aufgenommenen Bilder zu analysieren und Übereinstimmungen mit der Datenbank zu finden. Dies ermöglicht es der Strafverfolgung, potenzielle Verdächtige schnell zu identifizieren und ihre Bewegungen zu verfolgen, selbst wenn sie sich in einem öffentlichen Bereich aufhalten oder versuchen, sich der Erkennung zu entziehen.

Ein relevantes Anwendungsgebiet von biometrischer Fernidentifikation ist der Einsatz zur 1) **Fahndung nach Schwerverbrecherinnen und Schwerverbrechern 2) Sicherung von Großveranstaltungen (z. B. Sportveranstaltungen)**.

Post hoc analysis. **Der Einsatz von biometrischer Fernidentifikation 1) zur Erkennung von Schwerverbrecherinnen und Schwerverbrechern 2) nach Zwischenfällen bei Großveranstaltungen**

Ein derzeit von der Politik diskutiertes Thema ist der Einsatz von KI-basierten Systemen zur biometrischen Identifizierung von Personen, sogenannte Systeme zur **biometrischen Fernidentifikation**. Damit sind Computeranwendungen gemeint, die physische Merkmale von Personen (z. B. Gesichter) analysieren und damit konkreten Personen zuordnen können.

Biometrische Fernidentifikation kann von Strafverfolgungsbehörden **im Nachgang von kriminellen Ereignissen** eingesetzt werden, um Personen zu identifizieren und zu verfolgen, die möglicherweise in diese verwickelt waren.

Sie funktioniert, indem Kameras oder andere Sensoren Bilder von Gesichtern, Fingerabdrücken oder anderen biometrischen Merkmalen einer Person aufnehmen und diese Bilder mit einer Datenbank bekannter Personen vergleichen.

Die Technologie verwendet Algorithmen und Künstliche Intelligenz, um die aufgenommenen Bilder zu analysieren und Übereinstimmungen mit der Datenbank zu finden. Dies ermöglicht es der Strafverfolgung, potenzielle Verdächtige schnell zu identifizieren und ihre Bewegungen zu verfolgen, selbst wenn sie sich in einem öffentlichen Bereich aufhielten oder versuchten, sich der Erkennung zu entziehen.

Ein relevantes Anwendungsgebiet von biometrischer Fernidentifikation ist der Einsatz zur **1) Erkennung von Schwerverbrecherinnen und Schwerverbrechern 2) Sicherung von Großveranstaltungen (z. B. Sportveranstaltungen).**

Vignette translated wording

Real-Time. **The use of remote biometric identification for 1) real-time searches for serious criminals 2) securing public events**.

A topic currently being discussed by politicians is the use of AI-based systems for the biometric identification of persons, so-called systems for **biometric remote identification**. This refers to computer applications that can analyse physical characteristics of persons (e.g. faces) and thus assign them to concrete persons.

Remote biometric identification can be used by law enforcement agencies **in real time** to identify and track individuals who may be involved in criminal activity.

It works by cameras or other sensors capturing images of a person's face, fingerprints or other biometric characteristics and comparing these images to a database of known individuals.

The technology uses algorithms and artificial intelligence to analyse the captured images and find matches with the database. This allows law enforcement to quickly identify potential suspects and track their movements, even if they are in a public area or trying to evade detection.

A relevant application of remote biometric identification is its use for 1) **searching for serious criminals 2) securing public events (e.g. sporting events)**.

Post hoc analysis. **The use of remote biometric identification 1) for the detection of serious criminals 2) after incidents at public events**.

A topic currently being discussed by politicians is the use of AI-based systems for the biometric identification of persons, so-called systems for **biometric remote identification**. This refers to computer applications that can analyse physical characteristics of persons (e.g. faces) and thus assign them to concrete persons.

Remote biometric identification can be used by law enforcement **in the aftermath of criminal events** to identify and track individuals who may have been involved.

It works by cameras or other sensors taking images of a person's face, fingerprints or other biometric characteristics and comparing these images with a database of known individuals.

The technology uses algorithms and artificial intelligence to analyse the captured images and find matches with the database. This allows law enforcement to quickly identify potential suspects and track their movements, even if they were in a public area or trying to evade detection.

A relevant application of remote biometric identification is its use for **1) recognition of serious criminals 2) securing public events (e.g. sporting events).**