

European New School of Digital Studies
Chair for Law and Ethics of the Digital Society

Thesis submitted to obtain the Master's degree in the Master of Digital Entrepreneurship at
European University Viadrina Frankfurt (Oder)

Same words, new world:

Controlling remote biometric surveillance in an age of illiberalism

An evaluation of the AI Act's control mechanisms for the use of real-time remote biometric identification systems in public places by law enforcement and recommendations for their implementation in Germany, focusing on the risk of a strategic interpretative expansion of legal bases

First Supervisor:	Philipp Hacker
Second Supervisor:	Agnieszka Vetulani-Cęgiel
Submitted by:	Pauline Kussmann
Word count:	30.152
Submitted on:	15.08.2025

‘When I use a word,’ Humpty Dumpty said in rather a scornful tone, ‘it means just what I choose it to mean — neither more nor less.’

‘The question is,’ said Alice, ‘whether you can make words mean so many different things.’

‘The question is,’ said Humpty Dumpty, ‘which is to be master — that’s all.’

— Lewis Carroll, 1871 in *Through the Looking Glass and What Alice Found There*

Table of Contents

I. Introduction.....	5
II. An Introduction to Remote Biometric Identification.....	7
1. Definition.....	7
2. What it is not.....	8
3. Technical basics.....	9
4. “Live” and “public” RBIS.....	10
5. Common risks.....	10
III. Legal Analysis.....	13
1. Theorizing the problem: A strategic interpretative expansion of legal bases.....	13
a) The problem: Vagueness and interpretability of law.....	13
b) The background: The rise of illiberalism and autocratic legalism.....	14
c) The mechanism: Strategic interpretative expansion of legal bases.....	16
d) The solution: Liberal constitutionalism.....	19
e) A first evaluation criterion: The need for mechanisms to control against a liberal constitutionalist baseline.....	20
2. Analysis of the AI Act’s provisions.....	22
a) AI Act’s provisions on live and public RBIS.....	22
i) What these regulations don’t cover.....	23
ii) A guiding example.....	25
b) AI Act’s Controlling authorities for live and public RBIS.....	26
i) Data Protection Authorities.....	26
ii) Market Surveillance Authorities.....	27
iii) Fundamental Rights Protection Authorities.....	28
c) AI Act’s control mechanisms for law enforcement’s use of live and public RBIS.....	28
i) case-by-case control.....	28
ii) in-case control.....	29
iii) systemic control.....	30
3. Interplay of AI Act and German legal bases.....	32
a) Law enforcement’s use of RBIS in Germany before the AI Act.....	32
b) Potential implementation of live and public RBIS in Germany.....	34
i) German authorities that would control law enforcement’s use of live and public RBIS.....	36
(1) Fundamental Rights Protection Authorities.....	36
(2) Data Protection Authorities.....	36
(3) Market Surveillance Authorities.....	37
ii) German laws that would regulate law enforcement’s use of live and public RBIS.....	39
IV. Legal evaluation.....	41
1. Evaluation of the AI Act’s control mechanisms’ sufficiency and identification of controlling criteria.....	41
a) Authorization.....	42
b) Notification.....	45
c) Disclosure of documentation.....	45
e) Fundamental Rights Impact Assessment.....	47
f) Annual reports.....	50
g) Risk Management System.....	51
2. Evaluation of sufficiency of control mechanisms besides the AI Act and identification of further controlling criteria.....	52
a) Data Protection Impact Assessment.....	52
b) Overall Surveillance Account.....	54
3. Conclusion.....	56

V. Recommendations.....	59
1. Comprehensive RBIS Control Framework.....	59
a) National competent authorities.....	61
b) Tasks.....	62
i) Operationalization.....	62
ii) Initial Assessment.....	63
iii) Continuous Testing and Evaluation.....	63
iv) Consequences for RBIS uses that pose a risk to or infringe upon fundamental rights. .	64
v) Reporting.....	64
vi) Training.....	65
vii) Cooperation with law enforcement.....	65
2. Additional recommendations.....	66
VI. Discussion.....	67
Bibliography.....	69

I. Introduction

Imagine the following scenario: A political protest in a public place. A hidden camera films the protest. The filmed data is connected to a huge police database, and a software that automatically compares the images taken with all other images in the database. Today, the software is tasked with finding out the identity of one of the protesters without raising his attention to it. Only a second after the filming, the software spits out a result, having found the protester's full name, home address, and ID number. For the duration of the protest, he remains unaware of any of this happening. But the next day, without any warning, police storms his home.

What sounds like Orwellian science fiction is the result of the provisions on “remote biometric identification systems” (hereafter RBIS) of the AI Act.¹ With them, for the first time, a Europe-wide legal basis is created for law enforcement's use of these systems. While the Act lists them as “prohibited” (Art 5(2)), it stipulates a broad range of exceptions, thereby ultimately providing a framework for their use.² This did not pass unchallenged: The topic of RBIS was among the most controversial issues in the negotiations surrounding the Act, with data protection authorities as well as civil society actors warning of its harmful consequences,³ and the European Parliament even voting against it.⁴ This is because RBIS are considered to be exceptionally risky, not only for the rights of any affected individual, but for democratic societies as a whole⁵ - for instance, for the exercise of freedom of expression, assembly and association, as well as for the freedom of movement.⁶

While such broad societal risks are frequently postulated, the majority of academic research on RBIS is limited to risks concerning the *technology itself*, such as the accuracy of its results, or

1 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) 2024 (AI Act).

2 Alice Giannini and Sarah Tas, ‘AI Act and the Prohibition of Real-Time Biometric Identification’ (*Verfassungsblog*, 10 December 2024) <<https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/>> accessed 23 June 2025.

3 Deutscher Anwaltverein, ‘PM 06/23: Biometrische Fernidentifizierung verbieten – in Echtzeit und nachträglich!’ (*Deutscher Anwaltverein*, 16 February 2023) <<https://anwaltverein.de/de/newsroom/pm-06-23-biometrische-fernidentifizierung-verbieten-in-echtzeit-und-nachtraeglich>> accessed 16 April 2025; Sebastian Meineck, Chris Köver and Daniel Leisegang, ‘Grundrechte in Gefahr: Die sieben quälendsten Fragen zur KI-Verordnung’ *netzpolitik.org* (26 January 2024) <<https://netzpolitik.org/2024/grundrechte-in-gefahr-die-sieben-quaelendsten-fragen-zur-ki-verordnung/>> accessed 16 April 2025; Amnesty International and AlgorithmWatch, ‘Offener Brief an Die Bundesminister Marco Buschmann Und Robert Habeck’ 2 <https://algorithmwatch.org/de/wp-content/uploads/2023/09/Offener-Brief_28.09.23.pdf> accessed 16 April 2025.

4 European Parliament, ‘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)’ (European Parliament) Amendments P9_TA(2023)0236.

5 Johanna Hahn, *Automatisierte Gesichtserkennung in Der Strafverfolgung* (Nomos Verlagsgesellschaft mbH & Co KG 2025) 30 ff.

6 As postulated by Germany's former Federal Data Protection Commissioner, see Meineck, Köver and Leisegang (n 3).

biases in its code that might lead to the discrimination of certain groups of people. Risks like these arise from the design, development, and implementation of the technology. The assumption is – and this is also visible in the finalized AI Act – that they can be mitigated through technical and procedural compliance. However, the argument of this thesis is that even when an RBIS is applied in full compliance with the AI Act’s provisions, it might substantially infringe upon fundamental rights *when the context wherein it is used, changes*.

The thesis will be concerned with a “strategic interpretative expansion of legal bases” as a specific form of such a context change. The term refers to the phenomenon of interpreting legal bases increasingly broadly, thereby expanding their range of application. Applied to the legal bases of RBIS, this might lead to an increasing number of people under surveillance, causing substantial infringements upon their fundamental rights, and risks to the democratic foundations of the society wherein this happens.

The word “strategic” is important here, since such an expansion doesn’t occur by happenstance. It is part of the repertoire of autocratic legalists who use legal means and methods to further their illiberal agenda.⁷ In Germany, the right-wing party *Alternative für Deutschland* (AfD), at times with the help of autocratic conservatives, has been testing a variety of legal and administrative avenues for hollowing out the state’s democratic core.⁸ The strategic interpretative expansion is one such avenue, and it will be explored in this thesis – specifically, whether the AI Act’s control mechanisms over RBIS use⁹ sufficiently protect against its negative consequences. The aim is to recommend improvements in this regard for an implementation in Germany, should the government decide to legalize it in future. This is particularly relevant at present, since Germany, like other EU member states, needs to finalize an AI Act implementation bill before 2nd August 2025.¹⁰

Hence, the research question is: “In how far do the AI Act’s control mechanisms over law enforcement’s use of live and public remote biometric identification systems safeguard against risks for and infringements upon fundamental rights caused by a strategic interpretative expansion of legal bases in Germany, and how can German law be improved in this regard?”.

The thesis will be structured as follows: After this introduction (Chapter I), Chapter II explains “remote biometric identification systems” by providing a definition, outlining the technology, and describing common risks associated with it. Chapter III starts with conceptualizing the risk of a strategic interpretative expansion of legal bases (1(a)-(c)), and provides the theoretical framework of “liberal constitutionalism” for an evaluation of the sufficiency of current legal provisions ((d)-

7 Kim L. Scheppele, ‘Autocratic Legalism’ (2018) 85/2 The University of Chicago Law Review 545.

8 See various practices in Arne Semsrott, *Machtübernahme - Was passiert, wenn Rechtsextremisten regieren* (Droemer Knaur 2024).

9 Specifically, RBIS use by law enforcement in real-time and in public places

10 At the point of submission of the thesis in mid-August 2025, this has not happened.

(e)). This is followed by an analysis of the AI Act's provisions for controlling law enforcement's use of RBIS (2). To illustrate the analysis, the opening scenario of this thesis will be expanded as an example case under (a)(ii), describing a scenario where RBIS' legal bases are broadened to target climate activists of the "Letzte Generation". Section 3 describes the interplay of the AI Act's provisions with legal bases in Germany. Then, Chapter IV evaluates the sufficiency of the Act's control mechanisms with regard to risks arising through a strategic interpretative expansion (1). For the sake of completeness, two additional control mechanisms will be evaluated that aren't part of the AI Act, but might nevertheless be relevant in this regard (2). Based on the evaluation, Chapter V recommends additional control mechanisms to be implemented in Germany. Lastly, Chapter VI discusses implications as well as limitations of the findings, and a potential transferability to other realms of surveillance control.

II. An Introduction to Remote Biometric Identification

1. Definition

Article 3(41) AI Act (AIA) explains RBIS as an AI system used to identify people – without their involvement – by comparing their biometric data against a reference database. "Remote" refers to the fact that the identification typically happens at a distance great enough for the system to scan multiple people in its field of view.¹¹ This allows for an identification without the individual being aware of it. Therefore, providers advertise these systems as 'seamless' and 'without the need for end-user collaboration'.¹² There is no clear-cut definition of what counts as "remote", and hence, what exactly counts as an RBIS remains ambiguous.¹³

"Biometric" data is defined in Article 3(34) as data of the unique physical, physiological, or behavioral characteristics of a person.¹⁴ This includes gait, speech, and, most importantly at the moment, facial features.¹⁵ Biometric data is considered "personal data" and falls under "special categories of personal data" because firstly, it allows for individual identification, and secondly, it is unchangeable and tied to an individual for life. Therefore, its processing for identification is

11 EDRI, 'Remote Biometric Identification: A Technical & Legal Guide' (*European Digital Rights (EDRI)*, 23 January 2023) <<https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/>> accessed 23 June 2025.

12 *ibid.*

13 Hahn (n 5) 23.

14 The same definition is given in Art 4(14) GDPR and adopted in section 46(12) BDSG.

15 Johanna Hahn, 'Ein Anfang, Mehr Nicht' (*Verfassungsblog*, 11 December 2024) <<https://verfassungsblog.de/ein-anfang-mehr-nicht/>> accessed 15 April 2025.

forbidden (see General Data Protection Regulation (GDPR)¹⁶ Art 9(1), with specific exceptions in Article 9(2)). As the GDPR does not apply to law enforcement, this ban also does not apply to them. Instead, the Law Enforcement Directive (LED)¹⁷ applies, stipulating that the processing of biometric data by law enforcement is only allowed “where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject” for the protection of vital interests of either the individual itself or another person (Art 10).

Lastly, “identification” refers to the system’s ability to discover the specific identity of a previously unidentified individual, for instance, to determine the identity of an unknown crime suspect.¹⁸ The process of identification happens “1:n” – matching one person against the records of many people (n) saved in a database.¹⁹ When used by law enforcement, this database might contain records of known criminals, missing persons, or anyone who has previously undergone identification procedures (such as crime suspects, but also people seeking asylum). The database used is important, since the possibilities of a successful identification depend on its size and content.²⁰ Due to the increasing number of recorded images, the probability of identifying someone in them is also steadily increasing.²¹

2. What it is not

Two distinctions have to be made to avoid conceptual confusion: firstly, between biometric “identification” and “recognition”. “Identification” aims to answer the question: “Who is this person?”. “Recognition” entails comparing data to find matches, without necessarily leading to an individual identification.²² It only refers to the recognition of certain traits and the verification of their consistency. As such, it aims to answer questions like: “Is this the same person as before?” or “What attributes does this person have?”. An example is the system used by law enforcement during

16 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) 2016 (GDPR).

17 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Law Enforcement Directive) 2016 (LED).

18 Gerrit Hornung and Stephan Schindler, ‘Das biometrische Auge der Polizei’ (2017) 5 ZD 203, 203, 207.

19 Some argue that RBI is in fact “many-to-many” matching, so “n:n”, because every individual present gets scanned, even though only one person is being searched for (see EDRI (n 11)). Hence, the question: “Is this person X?” might in practice be answered with: “No, this is person Y”.

20 Stephan Schindler, *Biometrische Videoüberwachung* (1st edn, Nomos Verlagsgesellschaft mbH & Co KG 2021) 191.

21 BKA, ‘Gesichtserkennung’ (*Bundeskriminalamt*) <<https://perma.cc/NZ3K-B555>> accessed 19 April 2025.

22 Hahn (n 5) 23.

the G20 protests in Hamburg, where recognition was used to create movement profiles of protesters, without comparing them against a database for individual identification.²³ So while “identification” always involves recognizing someone, recognition does not automatically entail identification. The second important distinction is “identification” versus “verification”. While identification is “1:n”, verification is “1:1”.²⁴ With “verification”, the subject in question is already known; its identity only needs to be verified. It answers the question: “Is this really the same person?”. An example is a passport control at the airport, where law enforcement takes an individual’s fingerprints to compare them in real-time against the fingerprint data in its passport. Verification is considered less infringing upon individual freedoms, since only a single database is controlled.²⁵ Also, its error rate is lower, since it usually happens in a situation where the subject is cooperating, for instance by directly facing a camera.²⁶

3. Technical basics

Modern RBIS are based on machine learning (therefore “AI”): The system learns by itself through trial and error, and subsequently improves.²⁷ It starts by creating a mathematical model, for instance, a model of each face for facial identification. This model is called “embedding” (or “template”) and consists of multiple vectors representing facial characteristics.²⁸ This modeling is performed in deep convolutional neural networks trained on millions of photos.²⁹ The networks learn to identify distinctive markers from the training data, for instance, which biometric features are important for identifying a face. Since this process is mathematically highly complex, it is not possible to reconstruct how a network created a specific embedding.³⁰ The created embedding is then compared to the models of reference pictures to get a “match”. If the similarity of two embeddings passes a certain threshold, the face will be identified as the matching one. The number of matches depends on the threshold set: If the threshold is increased, the matches decrease, and along with it the

23 *ibid* 27–28.

24 *ibid* 40.

25 *ibid* 41.

26 Stan Z Li and Anil K Jain (eds), *Handbook of Face Recognition* (Second Edition, Springer 2011) 1,3; Massimo Tistarelli and Christophe Champod (eds), *Handbook of Biometrics for Forensic Science* (Springer International Publishing 2017) 1,5.

27 Stuart Russell and Peter Norvig, *Artificial Intelligence, Global Edition* (4th edn, Pearson Education 2021) 670 ff.

28 Florian Schroff, Dmitry Kalenichenko and James Philbin, ‘FaceNet: A Unified Embedding for Face Recognition and Clustering’, *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (IEEE 2015) 815,821 <<https://ieeexplore.ieee.org/document/7298682>> accessed 18 June 2025.

29 Martin Knoche, Stefan Hörmann and Gerhard Rigoll, ‘Susceptibility to Image Resolution in Face Recognition and Training Strategies to Enhance Robustness’ (2022) 8 *Leibniz Transactions on Embedded Systems* 01:1, 1,6.

30 Hahn (n 5) 50.

number of false positives.³¹ The significant development of neural networks in recent years, along with an enormous increase in the availability of training data, has led to an increased performance and use of RBIS.³²

4. “Live” and “public” RBIS

This thesis will be focused on RBI practiced “in real time” and “in public places” (hereafter “live and public”). “Live” refers to the identification occurring immediately, delivering results more or less at the moment of data collection.³³ “Public” means that the data is collected in public places, whereby data of anyone present might be collected in the process. These places could be train stations, parks, streets, sports venues, or any other place the public can enter.³⁴ Using RBIS “live and public” is considered especially risky and is hence subject to stricter regulation in the AIA, because firstly, since the data is collected in public, biometric identifiers of many uninvolved bystanders are scanned as well.³⁵ Secondly, public places are also the location where people gather for protesting. Hence, biometric identifiers of people are collected at a place where their political opinion can be inferred, thereby potentially restricting their freedom of assembly (Art 8 Basic Law).³⁶ Thirdly, practicing RBI “live” means that there is no time gap between recording and identifying, leaving the suspect with no time to evade identification and its consequences, for instance, a subsequent conviction. As such, RBIS significantly strengthen law enforcement’s overall power, with the potential to cause vast consequences when left uncontrolled.³⁷

5. Common risks

³¹ *ibid.*

³² On the historical development of RBIS, see Woodrow Wilson Bledsoe, *A Facial Recognition Project Report* (King Hurley Research Group 1093); ‘Face Recognition Technology (FERET) | NIST’ <<https://perma.cc/3EWX-WC9B>> accessed 18 June 2025; John D Woodward, ‘Super Bowl Surveillance: Facing Up to Biometrics’ [2001] RAND 9; Kelly Gates, ‘Identifying the 9/11 “Faces of Terror”: The Promise and Problem of Facial Recognition Technology’ (2006) 20 Cultural Studies 417; Magdalena Tomaszewska-Michalak, ‘Biometric Technology 20 Years After 9/11 – Opportunities and Threats’ (2022) 63 Studia Politologiczne; ‘ACLU NEWS Newspaper of the American Civil Liberties Union of Northern California Volume LXVI, No. 1’ (2001) <<https://www.aclunc.org/sites/default/files/Winter%202001%20ACLU%20News.pdf>> accessed 18 June 2025.

³³ Andreas P Müller, ‘Orwell’sche Gleichgültigkeit und Europäische Demokratie’ (*Verfassungsblog*, 23 January 2024) <<https://verfassungsblog.de/orwellsche-gleichgultigkeit-und-europaische-demokratie/>> accessed 7 July 2025.

³⁴ EDRI (n 11).

³⁵ Hornung and Schindler (n 18) 208.

³⁶ Hahn (n 5) 144; Grundgesetz für die Bundesrepublik Deutschland 1949 (GG).

³⁷ Hahn (n 5) 76; Joe Purshouse and Liz Campbell, ‘Automated Facial Recognition and Policing: A Bridge Too Far?’ (2022) 42 Legal Studies 209.

Legal scholar Hahn identifies the confluence of five factors to make RBIS especially risky: next to *biometrics*, these are *secrecy*, *spread*, *accuracy*, and its *networking capability*.³⁸ According to her, no other criminal procedural measure in Germany combines all these factors and has such a danger potential.³⁹ I will add *bias* (related to accuracy), *function creep* (related to *networking capability*) and a *chilling effect* as additional commonly identified risks.

Secrecy is a risk factor inherent to all surveillance processes: Since it usually happens covertly, the subject under surveillance is ideally unaware of it. Even if the subject were to gain awareness of it, there are limited possibilities of finding out details about it, since in an ongoing investigation, information about surveillance measures is usually not disclosed to the subject. Lacking this information, the subject's capabilities of defending itself against it are very limited.⁴⁰

Secondly, *spread* refers to the "mass effect": To identify a subject, especially in public places, many uninvolved bystanders are also filmed and their biometric data is evaluated (see II.4). Critics therefore argue that RBIS do not target the accused, but primarily bystanders.⁴¹

The factors of spread and secrecy lead to a *chilling effect*, meaning that people practice self-censorship out of fear of being recorded. This is already mentioned in the Census Ruling of 1983, wherein the German Constitutional Court (*Bundesverfassungsgericht*, BVerfG) states that data collection and integration might cause psychological pressure that impacts individual behavior.⁴²

The risks of chilling effects have also been recognized by the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR).⁴³ Because RBIS is seen as particularly potent, the risk of potential chilling effect is seen as especially high.⁴⁴

The *accuracy* of RBIS' results remains low, with the most popular systems achieving around 90% accuracy.⁴⁵ While this might sound like a high mark, 10% of false positives of a system used by law enforcement might have serious adverse consequences for many innocent people. Additionally, a false positive of an RBIS can lead to a situation where the wrongfully identified subject is not *at all* connected to the crime in question - as was recently the case in the US, with the suspect living multiple states away from the conducted offense.⁴⁶ Importantly, accuracy varies depending on

38 Hahn (n 5) 31.

39 *ibid* 36.

40 *ibid* 33.

41 *ibid* 32.

42 *Census Act Decision* [1983] Bundesverfassungsgericht 1 BvR 209/83, BVerfGE 65, 1 13(145).

43 Laurent Pech, 'The Concept of Chilling Effect - Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU' [2021] Open Society - European Policy Institute 2.

44 Müller (n 33).

45 Monika Simmler and Giulia Canova, 'Facial Recognition Technology in Law Enforcement: Regulating Data Analysis of Another Kind' (2025) 56 Computer Law & Security Review 106092, 3.

46 Kashmir Hill and Ryan Mac, "'Thousands of Dollars for Something I Didn't Do'" *The New York Times* (31 March 2023) <<https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html>> accessed 18 June 2025.

gender, age, skin colour, and other markers.⁴⁷ A test conducted by the NIST showed that for 1:n matching, accuracy was especially low for African American females.⁴⁸ This leads to a *bias* against these groups, since with a lower accuracy, the number of false positives among their group grows, putting them at risk of increased scrutiny by law enforcement,⁴⁹ and in the worst case leading to wrongful convictions.

Hahn names the *networking capability* as another risk, referring to RBIS' technical capability to conduct their searches across various databases.⁵⁰ Since the technique of embedding enables a comparison against all file-compatible images, for instance, all passport photos, linking these databases together is *de facto* already possible, and is only prevented by law. This risk relates to the concept of *function creep*. The term refers to "the expansion of a system or technology beyond its original purpose".⁵¹ With regard to RBIS, this could be a creep of RBIS' function to include other reference databases (see *networking capability*), or a change of its code to enable additional functions like emotion recognition.

The risk factors of *secrecy*, *spread*, and a resulting *chilling effect* are inherent to many surveillance instruments and have been dealt with in the fields of law, political theory, sociology, and psychology.⁵² The risks of *accuracy*, *bias* and *function creep* (including a *networking capability*) are relevant for many technologies, and are known risks in the field of technology development. In recent years, they have increasingly been researched with regard to RBIS.⁵³ These risks associated with the *technology itself* are the risks most commonly identified and researched. However, risks of RBIS can also arise from its *legal application within a certain political context*. This thesis argues that even when all the described risks are mitigated through technical or procedural compliance, the legal application of RBIS can lead to serious infringements upon fundamental rights, affecting individuals, and in the long run, society itself. This will be elaborated in the next section.

47 Purshouse and Campbell (n 37) 10.

48 Patrick Grother, Mei Ngan and Kayee Hanaoka, 'Face Recognition Vendor Test Part 3: Demographic Effects' (National Institute of Standards and Technology 2019) NIST IR 8280 66.

49 Purshouse and Campbell (n 37) 11.

50 Hahn (n 5) 34.

51 Bert-Jaap Koops, 'The Concept of Function Creep' (2021) 13 Law, Innovation and Technology 29, 1.

52 See e.g., Hahn (n 5) 30 ff; Kiran Kappeler, Noemi Festic and Michael Latzer, 'Qualitative Evidence on Chilling Effects—How Users' Imaginaries of Dataveillance Lead to Inhibited Digital Behavior', *AoIR Selected Papers of Internet Research* (2022); Pech (n 43); Jonathon W Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (btj, 2016); 'The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda'; Julian Staben, 'Der Abschreckungseffekt auf die Grundrechtsausübung', *Strukturen eines verfassungsrechtlichen Arguments* (Mohr Siebeck GmbH & Co KG 2016).

53 See e.g., Hahn (n 5) 32 ff; Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification'; Grother, Ngan and Hanaoka (n 48); Koops (n 51); Purshouse and Campbell (n 37); Simmler and Canova (n 45).

III. Legal Analysis

1. Theorizing the problem: A strategic interpretative expansion of legal bases

Apart of the risks named above, there is another danger: one that is quite known in the field of political theory, but has not entered the legal discussion on surveillance, and in fact, seems to have gotten little attention in legal debate in general, which is underscored by the fact that a proper term for it does not exist. For the lack of an official term, I will call it a “strategic interpretative expansion of legal bases”, and it will be the focus of this thesis.

a) The problem: Vagueness and interpretability of law

Words carry meaning.⁵⁴ They are never neutral, or objective. And their meaning – this is particularly important – is not arbitrary. According to theorists of social constructivism (but also to dominant schools of Neo-Marxism⁵⁵), words are given meaning in the context of a “dominant” (in Marxist terms: “hegemonic”) discourse or a “linguistic régime”.⁵⁶ This means that dominant political forces fill language with meaning according to their values. Within the political discourse of a representative democracy, for instance, “democracy” has a positive connotation, whereas other forms of régime are linguistically devalued – for example, “totalitarianism”.⁵⁷ This is not limited to words describing the political system itself; the determination of meaning happens for every thinkable concept. To enter the realm of criminal law: What is a “criminal”, and what is a “terrorist” – in fact, what exactly does “terror” constitute? All of these concepts are given meaning within a certain political context.

In the past, this was easy to spot: When a ruler states “L’état, c’est moi”⁵⁸, it is clear that it is him who decides what exactly constitutes a crime. In the modern system of a liberal democracy, to prevent arbitrary treatment and ensure the principle of equality, a body of text defines what is a “criminal” based on fixed criteria – a body of text called “law”. The dominant ontological school of thought in this field, legal positivism, acknowledges that society is created by human-made social rules (instead of a god determining what is just), and also recognizes that, since law is in essence a

54 Michel Foucault, ‘Truth and Power’, *POWER/KNOWLEDGE - Selected interviews and other writings 1972 - 1977* (Pantheon Books 1980).

55 Antonio Gramsci, *SELECTIONS FROM THE PRISON NOTEBOOKS* (Lawrence & Wishart 1971).

56 Foucault (n 54) 112.

57 *ibid* 116.

58 LOUIS XIV (1638-1715), King of France on 13 April 1655 before the Parlement of Paris, see Lucien Bély, *Louis XIV : Le plus Grand Roi Du Monde* (Éditions Jean-paul Gisserot 2005) 77.

body of text, it is inherently vague and therefore to a certain degree open to interpretation.⁵⁹ This vagueness is not necessarily bad; on the contrary, it allows for a certain flexibility in the application of law to a variety of cases. As legal scholar Kaufmann puts it, “a legal computer “programmed only once *per saecula saeculorum*” would scare even the most unshakable positivists”.⁶⁰ The prosecutor thus always has a certain degree of interpretative freedom on whether and how to prosecute.⁶¹ Within legal positivism, as described, for instance, by the prominent scholar Raz, this vagueness is accepted, because law is interpreted by legitimate institutional authorities that are servants of democracy.⁶²

b) The background: The rise of illiberalism and autocratic legalism

And here, exactly, lies the problem. Since law is based on words, and words are given meaning by the authority in power, whenever power changes, this meaning is also subject to change. And change is happening at the moment. “Illiberal”, “antidemocratic”, “authoritarian” forces are gaining power in many democracies, while at the same time, democratic freedoms seem to decline.⁶³ These developments threaten liberal democracies, but they are less easy to assess and address than other, more obvious antidemocratic ideologies like fascism: for they make use of the very system they aim to dismantle.⁶⁴ Legal scholar Scheppele describes this as “autocratic legalism” and explains that autocrats are using democratic institutions and processes to “capitalize on the normative force of formal constitutional procedures to justify their actions”.⁶⁵ Changing law in formally compliant ways, autocratic forces maintain a legal façade while undermining substantive rights. Similar to Scheppele’s analysis, legal scholar Sajó names this process “rule by law” instead of “rule of law” and describes how autocratic forces make use of legal loopholes to enforce their illiberal agenda.⁶⁶

59 See e.g., HLA Hart, *The Concept of Law* (Oxford University Press, Usa 2012).

60 Felix Kaufmann quoted in David Lanius, ‘Der strategische Einsatz von Unbestimmtheit im Recht’ (*Forum für Streitkultur*, 27 February 2017) <<https://forum-streitkultur.de/strategische-unbestimmtheit/>> accessed 23 June 2025. Translation by author.

61 Elisa Hoven, ‘Antisemitische Äußerungen Als Gegenstand Des Strafrechts’ (2025) 4/25 *Zeitschrift der Kriminalpolizei* <<https://kripoz.de/2025/01/31/antisemitische-aeusserungen-als-gegenstand-des-strafrechts/>> accessed 19 June 2025.

62 Joseph Raz, *The Authority of Law: Essays on Law and Morality* (Oxford University Press 1979).

63 Freedom House, ‘Freedom in the World 2025 - The Uphill Battle to Safeguard Rights’ (Freedom House 2025) <https://freedomhouse.org/sites/default/files/2025-03/FITW_World2025digitalN.pdf> accessed 21 July 2025; Berch Berberoglu, *The Global Rise of Authoritarianism in the 21st Century: Crisis of Neoliberal Globalization and the Nationalist Response* (Routledge 2020).

64 Scheppele (n 7) 571.

65 *ibid* 563.

66 See András Sajó, ‘Militant Rule of Law’ (*Verfassungsblog*, 20 December 2023) <<https://verfassungsblog.de/militant-rule-of-law/>> accessed 9 May 2025. Another term for it is “constitutional capture”, see Jan-Werner Müller, ‘Rising to the Challenge of Constitutional Capture’ *Eurozine* (21 March 2014) <<https://www.eurozine.com/rising-to-the-challenge-of-constitutional-capture/>> accessed 19 June 2025.

Instead of basing themselves on liberalism, these autocrats solely value legalism: as long as legal compliance is ensured, they argue, political integrity is upheld, regardless of the content and context of a case.⁶⁷ Autocratic legalists do not believe in the necessity of limiting public power or holding it accountable.⁶⁸ Hence, part of their repertoire (coined “script tactics”⁶⁹) is handing more and more power to the executive, including law enforcement. Another problematic part of this process is a ripple effect: As Sajó explains with regard to autocratic developments within international and constitutional courts, once courts manifest their amended behavior through judgments, those judgments normalize a new reality, leading to similar judgments in future.⁷⁰ He urges courts to understand that their decisions exist within a context where even seemingly minor judgments can accelerate democratic decline.

In the long run, autocratic legalism hollows out democracy itself: Formally compliant procedures serve to consolidate power in ever fewer hands. While preserving “the shell of the prior liberal state”, its moral core is eroded, until finally, the system itself becomes replaceable. Scheppele compares this process to Tocqueville’s explanation of the French Revolution: “for a revolution to topple the ancien régime, the ancien régime must have already been hollowed out from within”.⁷¹ This becomes easier in times of crisis, when the democratic restraints of liberalism, such as preserving freedoms despite this leading to a state of less security, seem less appealing.

At the same time, countering autocratic legalism is difficult. Firstly, a respect for the rule of law deeply enshrined within democratic institutions makes it hard for its actors to stop these tendencies. For instance, “judges are not socialized to become moral arbitrators, and even less moral heroes”⁷² - circling back to the ontological tradition of positivism, wherein judges are not supposed to base their decisions on a higher moral ground but upon a fixed set of rules deriving their value from their (presumably democratic) institutional environment. Secondly, when judges declare a certain law or case to be legal, this claim is backed by their authority; after all, who else could decide upon the legality of anything. Like Foucault and Raz describe, the system is legitimized by those in power, and in this way, “the possibility that it is normally insincere or based on a conceptual mistake is ruled out”.⁷³ Thirdly, autocratic legalism is emerging just now, and there is no script for all avenues which autocrats may take to dismantle liberal democracy.⁷⁴ Finally, asserting power through legal

67 Scheppele (n 7) 563.

68 *ibid* 571.

69 *ibid* 547.

70 Sajó (n 66).

71 Scheppele (n 7) 570.

72 Sajó (n 66).

73 Joseph Raz, *Ethics in the Public Domain: Essays in the Morality of Law and Politics* (Oxford University Press 1995) 217.

74 Scheppele (n 7) 557.

means is difficult to spot.⁷⁵ While historical knowledge exists of classic antidemocratic avenues leading to fascism, there is a tendency to believe that “unless those precise things happen, the danger is not very great”.⁷⁶ Spotting developments of autocratic legalism thus requires spotting less visible cues. Lastly, to justify their illiberal actions, autocratic legalists use democratic and constitutional language.⁷⁷ Hence, they use the same words – but in a new setting: the context of illiberalism.

c) The mechanism: Strategic interpretative expansion of legal bases

Describing what happens when autocratic legalists gain power, Scheppele and Sajó have both focused on certain tactics those actors use, such as replacing important positions within constitutional courts with loyal figures, or overburdening courts to disable them.⁷⁸ But an important tactic is yet to enter their list of “script tactics”: the strategic interpretative expansion of legal bases.⁷⁹ Hereby, legal authorities use the same law, the same words, but expand their meaning. This process does not happen arbitrarily. Autocratic legalists use it as a strategy to repress their political opponents and decrease dissenting voices. For instance, they might strategically inflate the interpretation of a law against “terrorism”, applying it to their opponents by initiating legal actions against them, and invalidate them through the accusation of being “terrorists”.⁸⁰ Because of this intentionality, merely speaking of a legal “concept creep” or “drift” would not be an appropriate term. Additionally, a change of legal interpretation could also be a “shift” from one interpretation to another one, but in this thesis, the focus lies on a change that increases a certain meaning - hence an “expansion”. As the creation and maintenance of a dominant discourse is inherent to all political systems⁸¹, the use of this strategy is not limited to autocratic forces; but here, it will only be analyzed within the setting of illiberalism rising.

⁷⁵ *ibid* 548.

⁷⁶ *ibid* 571.

⁷⁷ *ibid* 562.

⁷⁸ *ibid* 550; Sajó (n 66); Müller (n 66).

⁷⁹ In German, this translates to “Strategische Ausweitung von Befugnisgrundlagen”, part of “Strategische Rechtsumdeutung”.

⁸⁰ A textbook example of this is the application of the national security law of the SAR Hong Kong to political opponents, accusing them of terrorism, subversion, secession or collusion with foreign forces, see The Law of the People’s Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (National Security Law) 2020; International Service for Human Rights, ‘The National Security Law for Hong Kong: Impacts on Civic Space and Civil Society Engagement with the UN’ (2022) <https://ishr.ch/wp-content/uploads/2022/09/ISHR_Report-Impact-of-HK-National-Security-Law_web.pdf> accessed 27 May 2025.

⁸¹ Foucault (n 54) 115.

Importantly, the term does not refer to the creation of *new* legal provisions – presumably, this would spark a public debate quicker, since in this case, there is an official legal change enacted by a parliament, which would potentially be subject to public scrutiny. It also does not mean using a specific law for an *entirely different purpose*, thereby not reinterpreting but simply applying a law in a formally illegitimate way.⁸² This would be a more obvious rights infringement, and might therefore be challenged more easily, for instance, in a constitutional court. The difficulty in identifying (and acting upon) a strategic interpretative expansion of legal bases is that the authorities applying the law are still *formally* compliant, only *substantially* infringing upon a subject's rights. Hence, in this thesis, the term will be defined as *the conscious effort by political forces to inflate the interpretation of certain legal terms with the aim of advancing their power and devaluating their opponents*.

A clear definition of this concept is lacking in legal publications, probably at least in part attributable to legal studies' positivist tradition and formalist tenets. To contextualize the concept, I will therefore briefly outline its anchoring in other academic fields as well as related concepts in the legal field.

Firstly, due to its (social constructivist/ Neo-Marxist) ontological origin in political theory, there are several publications addressing this phenomenon in this academic field: for instance, the concept of a "strategic reinterpretation of terms" by Pfahl-Traughber, who defines this "reevaluation of values" to be part of a "cultural revolution" strategy by right wing forces.⁸³ Similar to this, Liedtke, Wengeler and Böke describe this as "concept occupation", and Raulf, taking a Neo-Marxist stance, describes it as a "cultural strategy to obtain cultural hegemony".⁸⁴

A somewhat similar concept can be found in the field of psychology under the term "concept creep", coined by Haslam who analyzes the inflation of the meaning of certain psychological terms over time – importantly though, in his conceptualization, it is indeed an unintentional "creep" and not a conscious effort that is part of a political strategy.⁸⁵

While not explicitly mentioned in the legal field, related debates and schools of thought do exist.

Naturally, in legal studies, many scholars are concerned with the interpretation of law⁸⁶ - but largely

82 Which is forbidden by recognized principles of law, see e.g., European Convention on Human Rights 1953 (ECHR) art 18.

83 Armin Pfahl-Traughber, 'Die „Umwertung der Werte“ als Bestandteil einer Strategie der „Kulturrevolution“' in Wolfgang Gessenharter and Thomas Pfeiffer (eds), *Die Neue Rechte — eine Gefahr für die Demokratie?* (VS Verlag für Sozialwissenschaften 2004).

84 Simon Raulf, 'Sprache und Kultur als Strategie der Neuen Rechten zur Erlangung kultureller Hegemonie' CampusPublik - Schriften zur politischen Bildung; Frank Liedtke and others (eds), *Begriffe Besetzen: Strategien Des Sprachgebrauchs in Der Politik* (Westdeutscher Verlag 1991).

85 Nick Haslam, 'Concept Creep: Psychology's Expanding Concepts of Harm and Pathology' (2016) 27 *Psychological Inquiry* 1.

86 See e.g., Ronald Dworkin, *Law's Empire* (Belknap Press of Harvard University Press 1997); Raz (n 62); Hart (n 59).

without connecting this to political theory, for instance, by discussing legal interpretation as an antidemocratic strategy. This seems peculiar, considering that certain legal scholars did attend to the relationship of law and power: namely, a range of scholars publishing in fascist regimes of the twentieth century, such as Carl Schmitt. A popular Nazi jurist at the time, Schmitt called for “rethinking the legal terms” already in 1933,⁸⁷ and the subsequent fascist regime followed suit.⁸⁸ After that, it took until the 1970s for the field of “Critical Legal Studies” (CLS) to emerge: a number of left academics who connected law to power through focusing on law’s function to uphold a certain political status quo.⁸⁹ They aimed to demonstrate the ambiguity of supposedly impartial and rigid legal doctrines, and (mirroring developments in critical political theory) were split into Neo-Marxist and deconstructivist schools of thought. Considered by some more of a movement and less of an academic school, they were criticized as “radicals”, and their influence faded in the 1980s.⁹⁰ While CLS did not explicitly address the phenomenon of a strategic interpretative expansion, the term might neatly fit into this school of thought.

Another concept connecting law and power is the concept of “lawfare”, describing the political exploitation of the legal system to achieve one’s own ideological objectives. This term has been used in various legal contexts since the 1950s, but is nowadays primarily applied in a military context (using “lawfare” as a weapon in political conflicts, for instance, in the “war on terror” led by the US).⁹¹

What becomes apparent is that more attention is given to the relationship of law and power whenever concrete political developments reveal it more clearly (for instance, in the US during the 1970s or post-9/11). It thus does not surprise that in recent years, correlating with a political shift towards illiberalism, scholars like Scheppele and Sajó have once again emphasized this relationship through coining terms like “autocratic legalism” and “rule by law”.⁹² This thesis is no exception to this, as it develops the concept of a strategic interpretative expansion and analyzes its concrete risk for the legal application of RBIS against the backdrop of an increasingly illiberal political sphere.

87 Carl Schmitt, *Gesammelte Schriften 1933-1936: mit ergänzenden Beiträgen aus der Zeit des Zweiten Weltkriegs* (1st edn, Duncker & Humblot 2021).

88 IJ Gallin, *Rechtsetzung Ist Machtsetzung: Die Deutsche Rechtsetzung in Den Niederlanden 1940-1945*, vol 2736 (PETER LANG 1999).

89 Important thinkers were, among others, US American scholars Duncan Kennedy and Karl Klare, Roberto Unger, and in Europe, the sociologist Pierre Bourdieu.

90 Anja Oberkofler, ‘Kritische Ansätze im amerikanischen Rechtsdenken’ (2001) 132 UTOPIE kreativ 925.

91 The first usage of the concept within this context is Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (People’s Liberation Army Literature and Arts Publishing House 1999).

92 Both have a working background in Hungary, one of the first European countries to experience democratic backsliding.

d) The solution: Liberal constitutionalism

So, what now? According to political theorist Ypi, legal scholars need to move beyond their “abstract, seemingly eternal body of rules” and enter the realm of politics.⁹³ Once again, legal scholarship has to acknowledge the relationship between law and power, and specifically, language as a mechanism of power within an illiberal agenda. According to Ypi, this relationship is currently only understood and instrumentalized by right-wing forces hijacking democratic institutions. To prevent this, legal reforms as well as the established legal order need to be critically analyzed.⁹⁴ For doing so, as Sajó states, *mala fides*, or “bad faith”, needs to become the standard assumption.⁹⁵ Legal reforms thus have to be evaluated assuming bad intentions by involved authorities – for instance, by law enforcement. Hence, in a scenario of autocratic legalism, the positivist notion that law is lawful when exercised by an institutional authority within a democracy is no longer valid.

For developing an alternative approach, the formalist tenet of (autocratic) legalism needs to be replaced by a liberal tenet: one that moves beyond mere compliance for the evaluation of legal applications, to one based on values that underlie existing law. Scheppele calls this “liberal” or “democratic” constitutionalism, and describes it as “democracy reinforcing”.⁹⁶ To enable this, all branches of government need to be bound to defending the individual freedoms needed to retain the capacity of democratic citizens – and, to that end, need to be subjected to strong control mechanisms.⁹⁷ In a similar manner, Sajó calls for a “preventive militant rule of law”, which entails “a systematic revision of the existing institutional and doctrinal arrangements of the legal order”.⁹⁸ According to Ypi, when reviewing law, special attention needs to be paid to the autocratic mechanism of a “progressive assertion of the executive over all other branches of the state”.⁹⁹ Autocratic forces aim at strengthening executive powers, for instance, through granting more power to law enforcement. Hence, when reviewing legal reforms, those that expand executive powers need to be assessed first, also because they potentially cause a ripple effect, affecting the overall capacity of subjects to exercise their democratic rights. Additionally, the fact that autocratic legalists do not follow the script book of fascism implies that attention needs to be paid to the small and seemingly insignificant moves, too.

93 Lea Ypi, ‘Bringing politics back in’ [2024] *Bundeskanzler Helmut Schmidt Stiftung Magazine* „For a Just Democracy!“ <<https://www.helmut-schmidt.de/aktuelles/detail/bringing-politics-back-in>> accessed 12 May 2025.

94 *ibid.*

95 Sajó (n 66).

96 Scheppele (n 7) 558.

97 *ibid.*

98 Sajó (n 66).

99 Ypi (n 93).

To avoid missing out on any avenue that autocratic legalists might take, and to move the discussion from an abstract to a concrete stage, I argue that these reviews need to take place for every single legal instrument of the executive – because the ripple effect of even a single instrument’s legal basis being expanded can not be known beforehand, and should hence not be underestimated.

Additionally, at times, better insights can be gained by looking at concrete practices than by reviewing an entire legal system on an abstract level; in extension, by doing so, concrete improvements (such as robust control mechanisms over executive forces’ use of RBIS) are more achievable than in an attempt to improve the entire legal system – especially when autocratic forces already exercise influence within this debate.¹⁰⁰

e) A first evaluation criterion: The need for mechanisms to control against a liberal constitutionalist baseline

Because autocratic legalists enforce an illiberal agenda, for instance, through a strategic interpretative expansion of legal bases, legal reforms, especially the ones strengthening the executive, need to be evaluated through a liberal constitutionalist lens. Therefore, the AIA provisions legalizing law enforcement’s use of live and public RBIS will be critically evaluated in this thesis. The aim is to subsequently establish criteria for RBIS control mechanisms to sufficiently safeguard against the adverse effects of a strategic interpretative expansion of legal bases. However, a first criterion has already become clear from the theory above: Control mechanisms do not merely need to ensure formal compliance, but need to safeguard fundamental rights for retaining individuals’ capacities for acting as democratic citizens, too.

What does this entail for a mechanism controlling a strategic interpretative expansion of legal bases? Since an *expansion* necessarily means an increase, or growth, any mechanism controlling this needs to establish a certain *baseline* to notice an increase. A baseline could be numeric; for instance, by controlling the total quantity of RBIS usage against the quantity of the previous year, or against any hypothetical numeric baseline (i.e., defining X amount of yearly usages as “norm”). But using a quantitative baseline would only lead to noticing an increase in usage, without being able to attribute this increase to any shift in a legal interpretation, and would hence fail to control for it effectively. Additionally, the definition of any quantitative baseline of this kind would be arbitrary (since defining X amount as “norm” is a subjective decision). Hence, a qualitative baseline is needed. But at least in theory, an interpretative expansion could also happen in an arbitrary, non-

¹⁰⁰ Of course, evaluations and improvements of legal instruments nevertheless need to take place on both levels, analyzing each single instrument as well as the overall legal system.

strategic way, not threatening substantial democratic rights of citizens, and might in that case be unproblematic. Consequently, a qualitative baseline does not need to control *any* kind of interpretative expansion, but specifically one that strategically threatens fundamental democratic rights.

One option to define such a baseline would be to attach it to the past, by setting the “original legislative intent” as a baseline. A mechanism controlling for a strategic interpretative expansion would thus need to control whether a legal application of RBIS is still in line with the original legislative intent. However, even the original legislative intent might not necessarily have been aligned with substantial democratic rights. Acknowledging the relationship between law and power, it has to be recognized that the creation of law always happens within a specific political context, which might not always favor the fundamental rights of all citizens equally.¹⁰¹

Another option is to connect this baseline not to legislative intent, but to fundamental rights. This would mean that mechanisms controlling RBIS would always check whether its legal application is still in line with “a fundamental rights oriented interpretation of the law” (or, put simply, whether the legal application is still in line with fundamental rights). This is coherent with the framework of liberal constitutionalism, and would also be congruent with previous CJEU judgments ruling that new EU law must always be interpreted in light of fundamental rights.¹⁰² So, for a mechanism to effectively spot (and retain) potential adverse effects caused by a strategic interpretative expansion, it needs to control the legal application of RBIS against a fundamental rights baseline. Therefore, a first criterion for evaluating the AIA’s control mechanisms’ sufficiency is *whether these mechanisms entail controlling against a fundamental rights baseline*.

101 The “Adenauer-Erlass” in Germany in 1950 might serve as an example. This decree was installed to ensure the constitutional loyalty of civil servants and was officially directed against both right-wing and left-wing extremist groups. However, its primary legislative intent was to curb communist or communist-influenced associations. See Lukkas Busche, ‘Kommunistenverfolgung in der alten Bundesrepublik’ <<https://www.bpb.de/themen/deutschlandarchiv/225517/kommunistenverfolgung-in-der-alten-bundesrepublik/>> accessed 22 July 2025.

102 In particular, judgments of 20 May 2003, *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 et C-139/01, EU:C:2003:294, para 68 et seq.); of 4 March 2010, *Chakroun* (C-578/08, EU:C:2010:117, para 44 et seq.); of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, para 68 et seq.); of 11 September 2014, *A* (C-112/13, EU:C:2014:2195, para 51 et seq.); of 6 October 2015, *Orizzonte Salute* (C-61/14, EU:C:2015:655, para 49 et seq.); of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650, para 38 et seq.) and of 21 December 2016, *Tele2 Sverige and Watson and Others*. (C-203/15 and C-698/15, EU:C:2016:970, para 91 et seq.), see CJEU Research and Documentation Directorate, ‘Field of Application of the Charter of Fundamental Rights of the European Union’ (2021) 1 <https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-05/fiche_thematique_-_charte_-_en.pdf> accessed 14 July 2025.

2. Analysis of the AI Act's provisions

a) AI Act's provisions on live and public RBIS

The AI Act provides a Europe-wide regulatory framework for law enforcement's use of live and public RBIS (Chapter II, Art 5(1)(h)). Although the chapter itself is named "Prohibited AI Practices", and point (h) starts by stating that RBIS use by law enforcement is "prohibited", it continues with "unless" and names three broad case clusters wherein its use is permitted: firstly, for searching victims of abduction, human trafficking, sexual abuse as well as missing persons (i). Secondly, for preventing specific, substantial, and imminent threats to life or safety, or a potential terrorist attack (ii), and lastly, for localizing or identifying a suspect of certain criminal offenses, to investigate, prosecute or execute a penalty against them (iii). In this case cluster, its use is only allowed for 16 specific offenses listed in Annex II, among others, "terrorism", "sabotage", and "the participation in a criminal organization involved in one or more of the offenses listed above". Additionally, the listed offenses must be punishable with a maximum period of at least four years. Since none of these offenses share a common European definition, they are treated differently in each member state, potentially leading to RBIS being allowed for a certain offense in one state while being prohibited for the same offense in another.¹⁰³

Since law enforcement's use of RBIS is recognized to be highly infringing upon the rights of data subjects, and incompatible with the requirement of informed consent,¹⁰⁴ a variety of control mechanisms are stipulated in the subsequent paragraphs (Art 5(2)-(9)), which will be analyzed in section III.2(c). Apart of those mechanisms, some general prerequisites are that RBIS can only be used to confirm the identity of a specific individual (Art 5(2)).¹⁰⁵ Also, each consideration on whether a use is appropriate needs to take into account the caused "seriousness, probability and scale of the harm [...] if the system were not used" and its "consequences [...] for the rights and freedoms of all persons concerned" (Art 5(2)(a)-(b)).¹⁰⁶ Each use needs to be limited in terms of time, personal and geographic scope (Art 5(2)(b)). Member states have to register their respective RBI software in a Europe-wide high-risk AI database managed by the European Commission (EC) (Art 5(2)(b); Rec 131). While this database is publicly accessible, AI systems used by law

103 Giannini and Tas (n 2).

104 EDRI (n 11); Bettina Schöndorf-Haubold and Christopher Giogios, 'KI im Einsatz für die Sicherheit' (*Verfassungsblog*, 10 December 2024) <<https://verfassungsblog.de/ki-im-einsatz-fur-die-sicherheit/>> accessed 7 July 2025.

105 However, the specific identity of a suspect may not be clear in certain cases, for instance, in the case cluster of Art 5(1)(h)(ii) for the prevention of a terrorist attack threat, see Giannini and Tas (n 2).

106 Another point of criticism is that while mentioning that these elements should be considered, the AIA does not specify who should consider them how and when exactly, see *ibid*.

enforcement are exempt from this.¹⁰⁷ Lastly, member states can decide for which of the offenses listed in Annex II they want to allow RBIS use, and can also introduce additional restrictions and control mechanisms to the ones set in the AIA (Art 5(5)) – a point of particular importance for this thesis.

i) What these regulations don't cover

The “prohibition with exceptions” framework sheds light on a number of additional cases that do not fall under the prohibition, and they deserve some attention.

Firstly, since Article 5 only restricts *live* RBI, *post* RBI – i.e., a retrograde identification – does not fall under these “prohibited practices”. Instead, AI systems for post RBI are treated as “high risk AI systems” with their respective obligations (Arts 6-49). The control mechanisms over post RBIS are less robust – for instance, when post RBI is used, law enforcement does not need a judicial authorization for it.¹⁰⁸ Secondly, the prohibition does not cover individual and consent-based live and public RBI – e.g., when a person preregisters their biometric data and consents to being automatically identified for entering a public but access-restricted area.¹⁰⁹ Thirdly, Article 5 only deals with live and public RBI for law enforcement – hence, its usage is not banned for other public or private actors.¹¹⁰ For its use by other actors, the systems are again treated as high-risk AI with respective obligations applying, and of course, additional applications such as specified in the GDPR also apply.¹¹¹ As a fourth exception, Article 5 does not apply at national borders, since, according to the compromise text, borders are not part of the “public space”.¹¹² Individuals entering a member state to request asylum can hence be legally subjected to RBI. Lastly, and not

¹⁰⁷ This exception has also been criticized, see *ibid*.

¹⁰⁸ The distinction between live and retrograde identification has been criticized as futile by some scholars, since it is “purely technical” (see Michael Veale and Frederik Zuiderveen Borgesius, ‘Demystifying the Draft EU Artificial Intelligence Act’ (Social Science Research Network, 31 July 2021) <<https://papers.ssrn.com/abstract=3896852>> accessed 7 July 2025.). Some argue that retrograde RBI has the same consequences for the surveillance of citizens (see Federica Paolucci, ‘Shortcomings of the AI Act’ (*Verfassungsblog*, 14 March 2024) <<https://verfassungsblog.de/shortcomings-of-the-ai-act/>> accessed 7 July 2025.), others argue that it is even more problematic with regards to individual freedoms, see Hahn (n 5) 145. Additionally, it might be unclear when exactly a system is live and when it is retrograde, and this loophole could be used for an application of RBIS to fall under less strict regulation, see Müller (n 33).

¹⁰⁹ EDRi (n 11).

¹¹⁰ *ibid*.

¹¹¹ This has also been criticized by civil society actors, who advocated for the AIA to ban any “placing or making available on the market or putting into service of remote biometric identification systems”, see *ibid*.

¹¹² Meineck, Köver and Leisegang (n 3).

unimportantly, AI systems designed for national security purposes, military, or defense are anyway exempt from the AIA (Art 2(3)).¹¹³

¹¹³ Civil society actors have called this general exception clause a “carte blanche” and have tried to prevent it, see Amnesty International and AlgorithmWatch (n 3).

ii) A guiding example

Example case: Activist suspected of participating in a ‘section 129 organization’ involved in ‘sabotage’

To understand what an interpretative expansion of legal bases would entail for the legal application of RBIS as per AI Act, a guiding example will be introduced. It is based on case cluster (iii): an individual under suspicion of having committed a criminal offense listed in Annex II; specifically, the offense of ‘participation in a criminal organization’ involved in ‘sabotage’. In Germany, this is regulated in section 129 ‘Forming criminal organizations’ of the Criminal Code (*Strafgesetzbuch*, StGB), a section written to counter serious organized crime, punishable with a maximum of at least five years. Participating in a ‘section 129 organization’ falls under the category of organizational crimes, meaning that mere membership (and even support) constitutes a crime.¹¹⁴ Secondly, ‘sabotage’ is dealt with in various sections of the StGB, depending on the target of the sabotage (e.g., s 109e ‘Sabotage against means of defense’, s 88 ‘Anti-constitutional sabotage’, but also s 315b ‘Dangerous interference with road traffic’). The offenses of ‘participation in a criminal organization’ involved in ‘sabotage’ are chosen as example since both cases leave considerable room for interpretation.

The suspect in the example is a climate activist participating in events of the German climate group “Die Letzte Generation” (“The last generation”, hereafter LG) which conducts “non-violent resistance”¹¹⁵ through various forms of protest (famously gluing their hands to streets to cause traffic interruptions, but also painting and damaging public places and private property). Currently, German police statistics count over 1.000 people as participants of this group.¹¹⁶ The scenario is that with illiberalism rising in Germany, autocratic legalists increasingly interpret groups like LG as criminal organizations under section 129, leading to a state where a growing number of climate activists can be subjected to RBIS. In this scenario, the legal basis for “what constitutes a criminal organization” is expanded, as well as the definition of “sabotage” – for instance, the interpretation of ‘dangerous interference with road traffic’ can slowly be expanded to softer acts such as simply blocking street traffic through gluing oneself to the road.

The scenario is not far-fetched: In the states of Bavaria, Brandenburg, and Schleswig-Holstein,

114 Since supporting a section 129 organization is punishable only up to three years, supporters could not legally be subjected to RBIS.

115 Letzte Generation, ‘Werte & Protestkonsens’ (*Letzte Generation*) <<https://letztegeneration.org/mitmachen/werte-protestkonsens/>> accessed 24 June 2025.

116 Bundeskriminalamt, ‘„Letzte Generation“ Lagebild -Fortschreibung Nr. 2’ (Bundeskriminalamt 2024) Ausarbeitung 31.

members of LG are currently being investigated under section 129 (charges against five members in Brandenburg and one person in Schleswig-Holstein).¹¹⁷ In Brandenburg and Bavaria, district courts already confirmed the initial suspicion of LG being a section 129 organization.¹¹⁸ Also in Rhineland-Palatinate and Hamburg, public prosecutors have initiated section 129 investigations against LG activists.¹¹⁹ The charges against LG Bavaria led to a raid as well as the freezing of accounts, the wiretapping of 13 telephones, among them LG's press phone, raids at cooperating law firms and advertising agencies, the confiscation of addresses of 5.000 people associated with Fridays for Future (who were not charged), and a temporary blocking of the LG website.¹²⁰ Activists' homes were raided (13 in 2022 and 15 in 2023), members were put in preventive detention, and multiple LG demonstrations were prohibited. All of these measures were based on an initial section 129 suspicion. Additionally, while 'sabotage' is currently not the primary charge against LG activists (these are primarily s 240 StGB 'Coercion' (63%) and s 303 'Property damage' (15%)), 2% of all convictions are based on s 315b 'Dangerous interference with road traffic', a case counted as sabotage.¹²¹ With enough political will, LG could thus be interpreted as a criminal organization involved in sabotage, leading to a state wherein any climate activist merely suspected of participating in LG – e.g., publishing on LG's social media channels or being present at LG events – could potentially be subjected to live and public RBI.

117 Amnesty International, 'Deutschland: Paragraf-129-Anklage gegen Letzte Generation verschärft Kriminalisierung von Protest' (*Amnesty International*, Mai 2024) <<https://www.amnesty.de/pressemitteilung/deutschland-paragraf-129-anklage-gegen-letzte-generation-kriminalisierung-protest>> accessed 24 June 2025; Letzte Generation, 'Stellungnahmen zum §129-Verfahren am Landgericht Flensburg eingereicht' (*Letzte Generation*, 25 December 2024) <<https://letztegeneration.org/pm/38472/>> accessed 24 June 2025.

118 Dennis Bock and Benjamin Mischke, 'Die „Letzte Generation“ Als Kriminelle Vereinigung?' [2024] *Zeitschrift der Gewerkschaft der Kriminalpolizei* <<https://www.kriminalpolizei.de/ausgaben/2024/maerz/detailansicht-maerz/artikel/die-letzte-generation-als-kriminelle-vereinigung.html>> accessed 24 June 2025; Mathias Hausding, 'Letzte Generation: Landgericht Potsdam sieht Klimakleber als kriminelle Vereinigung' *MOZ* (15 May 2023) <https://www.moz.de/nachrichten/brandenburg/letzte-generation_-landgericht-potsdam-sieht-klimakleber-als-kriminelle-vereinigung-70631589.html> accessed 24 June 2025.

119 Bundeskriminalamt (n 116) 10.

120 Anna Biselli, 'Telekommunikationsüberwachung: Polizei soll monatelang die Letzte Generation abgehört haben' (*netzpolitik.org*, 23 June 2023) <<https://netzpolitik.org/2023/telekommunikationsueberwachung-polizei-soll-monatelang-die-letzte-generation-abgehört-haben/>> accessed 29 May 2025; Green Legal Impact Germany, 'Gericht Gibt Elinor Recht: Vorgehen Gegen Klimaprotest Beschränkt Zivilgesellschaftliches Engagement' (2023) <https://www.greenlegal.eu/wp/wp-content/uploads/2023/12/GLI_Stellungnahme_Elinor.pdf> accessed 24 June 2025; Anna Biselli, 'Letzte Generation: Der fossile Rechtsstaat rast gegen die Wand' *netzpolitik.org* (25 May 2023) <<https://netzpolitik.org/2023/letzte-generation-der-fossile-rechtsstaat-rast-gegen-die-wand/>> accessed 24 June 2025.

121 Bundeskriminalamt, '„Letzte Generation“ Lagebild -Fortschreibung Nr. 2' (Bundeskriminalamt 2024) Ausarbeitung 39.

b) AI Act's Controlling authorities for live and public RBIS

i) Data Protection Authorities

The AI Act is based on a multi-stakeholder model for ensuring compliance.¹²² Hence, multiple authorities play a role in controlling RBIS, among them the Data Protection Authorities (DPA). They are the primary authorities overseeing and advising questions of data protection. Therefore, they are tasked with overseeing data processing by private and public bodies in member states, including law enforcement. Their mandate is to ensure fundamental rights and freedoms of individuals when their data is processed (Art 51 GDPR), and their tasks with regard to law enforcement are laid out in the LED. The AIA is written in accordance with these previously defined tasks and does not override them (Rec 157 AIA). According to the LED, the DPA need to be an independent federal authority (Art 42 LED). Among their concrete duties for overseeing data processing by law enforcement are: monitoring data protection (Art 46(1)(a)), following up on individuals' complaints (46(1)(f); 2; 3; 52), giving recommendations to legislators (46(1)(c)), writing annual activity reports (49), raising awareness on data protection among the processing authorities (46(1)(d)), and helping them with their data protection impact assessments (27; 28).¹²³ Next to these general duties, the DPA need to have "effective corrective powers" over law enforcement's data processing, which need to be specified by each member state (Art 47(2)). Among these powers is the conduction of investigations in case of suspected data protection breaches, for which they need to have access to sensitive information (Arts 46(1)(h)(i); 47(1)). They can also issue warnings to controllers or processors (Art 47(2)(a)), and importantly, they can order compliance with data protection, for instance, through rectification (b) or even imposing a ban (c). An important exception is that the DPA are not responsible for overseeing data processing by courts when those act in their judicial capacity (Art 54(2)).

ii) Market Surveillance Authorities

Just like data protection, market surveillance (and its authorities, the MSA) has played an important role already before the AI Act. The mandate of the MSA is to ensure compliance of market products with their respective laws; in case of AI products, the MSA oversee their compliance based on their

122 European Commission, 'Governance and Enforcement of the AI Act' (*European Commission*) <<https://digital-strategy.ec.europa.eu/en/policies/ai-act-governance-and-enforcement>> accessed 10 July 2025.

123 More on the Data Protection Impact Assessment in section IV.2(b).

role specified in the AIA. Together with the “notifying authorities” (Art 70(2) AIA), they are the “national competent authority” for AI products. Moreover, the MSA functions as the “single point of contact” for the national implementation of the Act (Art 70(2)).

All member states need to appoint one main MSA by 2nd August 2025 (Art 70(2)), and can decide whether they want to create a new authority for this, or appoint an existing one. Importantly, the authority needs to be independent, impartial, and unbiased (Art 70(1)). For certain products, member states can appoint an additional MSA (Art 74). For instance, for high-risk AI systems such as RBIS used by law enforcement (specified in Annex III), member states should either appoint the DPA as MSA, “or any other authority designated pursuant to the same conditions” (Art 74(8)).

As the MSA are the primary enforcers of the Act (Art 70), they need to be equipped with powers to investigate and enforce compliance.¹²⁴ Recital 159 AIA explicitly stipulates that MSA need to have “effective investigative and corrective powers” for controlling biometric systems used by law enforcement. However, it specifies only the power to access processed data and all necessary information as a minimum requirement in this regard. Also, the MSA need to be equipped with the resources needed to perform their duties competently; for instance, they need to have sufficient competent personnel with “an in-depth understanding of AI technologies” and “fundamental rights” (Art 70(3)). The MSA are also the central point for complaints (Art 85). When the MSA perceive a high-risk system to be risky for a person’s health, safety or fundamental rights, they need to react (Art 79(1)); relevant actions enforcing compliance will be discussed in section III.2(c).

iii) Fundamental Rights Protection Authorities

Lastly, the AIA also instructs member states to appoint one or more Fundamental Rights Protection Authorities (FRPA). Their responsibility is to supervise and enforce that while using AI systems, member states still respect other obligations of Union law concerned with protecting fundamental rights (Art 77(1)). Member states had to appoint their FRPA by 2nd November 2024; a list of appointed bodies is published by the EC.¹²⁵ The powers of the FRPA are firstly that they can access documentation about AI systems when this is necessary for protecting fundamental rights. Secondly, when they perceive the implementation of an AI system to be infringing upon these rights, they can request the MSA to organize a technical test of the respective system (Art 77(3), more on this in section III.2(c)(ii)).

¹²⁴ European Commission (n 122).

¹²⁵ *ibid.*

c) AI Act's control mechanisms for law enforcement's use of live and public

RBIS

The AIA stipulates a variety of control mechanisms which can be sorted into three subcategories: mechanisms controlling each single use of live and public RBIS (“case-by-case”), mechanisms only activated in specific circumstances (“in-case”), as well as mechanisms that control its use on a macro level (“systemic”).¹²⁶

i) case-by-case control

Firstly, for each use of live and public RBIS, law enforcement needs to get an *authorization* by a court or by another independent administrative authority that is able to issue a binding decision (Art 5(3)), implying that the authorizing instance does not necessarily need to be part of the judiciary. Member states need to decide which authority will fill this position. The authorizing request needs to include a reasoning, and should only be granted when perceived as proportionate, necessary, and limited in terms of time and scope. In emergencies, the authorization can also be postponed up to 24 hours after starting the RBIS use. When the authorizing instance then finds that the use is not appropriate, it can stop the process, and results and output need to be deleted immediately and cannot be used. It should authorize it only if it finds the request to be reasonable, based on “objective evidence or clear indications” for the suspicion of crimes mentioned under Article 5(1) (h).

Secondly, every time law enforcement uses live and public RBI, they need to give *notification* to the DPA and MSA (Art 5(4)). Member states specify what needs to be part of this notification, but it has to contain at least information on the number of decisions taken by the authorizing instance, and their result (Art 5(6)). Sensitive operational data should not be included. Also, Article 5(4) does not specify whether the notification happens after or during an ongoing investigation. This is relevant, since the notified instances can theoretically act upon each case when noticing an infringement - but when they are notified afterwards, they can only react after the RBIS use is already completed.

¹²⁶ A control mechanism excluded from this analysis is the Post-Market Monitoring Plan, a stipulation for high-risk AI systems that providers need to implement (Art 72 AIA). The Act does not go into depth on this mechanism; instead, the EC will issue an implementing act detailing provisions for a template and the list of elements to be included in such a plan by 2nd February 2026. Since this information is not available yet, the mechanism is excluded here.

ii) in-case control

DPA and MSA can request a *disclosure of documentation* of the RBIS use from law enforcement in case they have a reasoned need to obtain further information (Art 26(10)). Such a disclosure could, for instance, contain the time, duration and purpose of a use, the authorizing instance, identified data subjects, and its result; again, sensible operational details are excluded. With this documentation, the DPA and MSA can follow up according to their mandates (specified in section III.2(b)).

One of the MSA mandates and another important in-case control mechanism is the *evaluation of high-risk AI systems* (Arts 79(2); 20). Whenever the respective MSA perceives a risk, paying particular attention to risks to vulnerable groups, they carry out an evaluation of the AI system in question. When it perceives a risk to fundamental rights to be at stake, it can carry out a technical test as part of this (Arts 79(2); 77(3)). If the test shows that the system is non-compliant, the MSA can require the operator to take all actions needed to bring the system into compliance, or to withdraw or recall it entirely (Art 79(2)). If the operator does not comply with these requirements, the MSA will restrict or prohibit the system, and notify the EC and member states (Art 79(5)). If the test shows the system to be compliant, but still risky for (among other things) fundamental rights, the MSA can require the operator to take measures to tackle these risks (Art 82). Here, the AIA explicitly acknowledges the possibility of an AI system being formally compliant but nevertheless infringing upon fundamental rights. When defining measures to be taken, the MSA needs to report these to the EC, which will consult with concerned member states and relevant operators to evaluate them. Throughout the entire evaluation (including the testing), the operator needs to cooperate with MSA as well as FRPA (Arts 79(2); 82(2)).

iii) systemic control

A first important systemic control mechanism is the *Fundamental Rights Impact Assessment* (FRIA), a provision for all high-risk AI systems (Arts 5(2)(b); 27). In line with the risk-based approach of the Act, the responsibility to assess the risk of one's system lies with the deployer – in this case, law enforcement. When completed, the FRIA needs to be handed to the MSA, but in cases concerning national security, law enforcement can also refrain from doing so (Art 25(3)).¹²⁷ As an *ex*

¹²⁷ Remembering that for live and public RBI, member states might still appoint the DPA as responsible MSA, in which case the FRIA would be handed to the DPA.

ante mechanism (in addition to *ex post* remedy¹²⁸), the FRIA needs to be completed prior to deploying a system. Since the FRIA is only an assessment and not a recurring evaluation, it only needs to be completed once, and only again if the system significantly changes (Art 27). It should include information on the system's intended use, who will be affected by it and how, and in case of a risk materializing, internal mechanisms to address this. The AIA does not give a predefined list of potential risks; the "specific risks of harm" are to be defined by the deployer. Also, the measures to be taken by the deployer in case of a risk materializing are not defined in detail, the AIA only stipulates that they need to include "arrangements for internal governance and complaint mechanisms" (Art 27(1)(f)). This implies that the responsibility to mitigate risks for fundamental rights of RBIS remains with law enforcement itself. Article 27 does not detail additional binding consequences in case a significant risk for fundamental rights is identified.

To provide guidance to deployers, Article 27(5) stipulates that the AI Office will develop a template. This template has since been provided by ALIGNER, a "forum for exchange between practitioners from law enforcement and policing, civil society, policymaking, research, and industry" funded by the EC, in practice consisting mainly of law enforcement actors such as the Bavarian Police, as well as some actors from academia.¹²⁹ On its website, a FRIA template can be downloaded for use.¹³⁰ It is based on four categories of fundamental rights, following the definition by the Charter of Fundamental Rights of the European Union (CFR):¹³¹ the presumption of innocence and right to an effective remedy and to a fair trial; the right to equality and non-discrimination; the freedom of expression and information; as well as the right to respect for private and family life and right to protection of personal data. The template also provides predefined risks based on these categories, for instance: "There is no mechanism to limit the deployment of the AI system to suspected individuals", "The AI system targets members of a specific social group", and "There are no mechanisms for the user to exercise control over the processing of personal data".

A second template identifies risk mitigation measures based on these risks. It is based on the definition of trustworthy AI by the EC.¹³² ALIGNER advises law enforcement to conduct the FRIA

128 Something that has often been criticized as insufficient with regard to fundamental rights (see e.g., Philip Alston and Joseph Weiler, 'An "Ever Closer Union" in Need of a Human Rights Policy: The European Union and Human Rights' (1998) 9 European Journal of International Law 658.). Another point of criticism concerning the FRIA is that such instruments always permit for a residual risk, instead of fully preventing negative consequences. A stricter stance is for instance used in the GDPR, see e.g., Alessandro Mantelero, 'Fundamental Rights Impact Assessments in the DSA' [2022] Verfassungsblog <<https://verfassungsblog.de/dsa-impact-assessment/>> accessed 7 July 2025.).

129 ALIGNER, 'About Aligner' (ALIGNER H2020) <<https://aligner-h2020.eu/about/>> accessed 7 July 2025; ALIGNER, 'ALIGNER - Towards a More Secure Europe' <https://aligner-h2020.eu/wp-content/uploads/ALIGNER_Flyer_AFRIA.pdf> accessed 7 July 2025.

130 'Fundamental Rights Impact Assessment (FRIA) | aligner' <<https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/>> accessed 7 July 2025.

131 Charter of Fundamental Rights of the European Union 2000 (CFR).

132 European Commission, 'Ethics Guidelines for Trustworthy AI | Shaping Europe's Digital Future' (*digital-strategy.ec.europa.eu*, 8 April 2019) <<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy->

with a “diverse and multidisciplinary team” and also advises involving the organization's data protection officer.¹³³

Another systemic control mechanism is the *annual reports*: firstly, by DPA and MSA to the EC (Art 5(6)); secondly, based on these, an aggregate report by the EC to the public (5(7)). For the first report, the EC will provide a template. Article 5(6) does not stipulate whether this report should be made public. The reports need to include the total number of decisions taken on RBIS use and their result (i.e., whether an authorization was granted or denied). They do not include information on the content of RBIS uses, such as the subjects affected, for which categories of crime it was used, or whether its use had the desired effect (the identification of the person in question). Also, while the reports specify the number of cases in which an authorization was denied, they do not specify the reasons for this decision.

A last systemic control mechanism is the establishment of a *Risk Management System* (RMS) (Art 9). Unlike the FRIA, the RMS is not explicitly mentioned under Article 5, but since RBIS becomes a high-risk AI system when not prohibited, it can be assumed that this provision also applies to it. The RMS must be set up by the deployer (Art 9(1)) and is part of a broader *Quality Management System* (QMS) (Art 17). Only the RMS will be analyzed here, since it is the most relevant part of the QMS with regard to risks deriving from RBIS usage. As a “continuous iterative process”, the RMS is open-ended, and also includes risks that were unforeseen in the beginning (Art 9(2)(c)). The system and its risk mitigation measures are to be tested to identify the best measures (Art 9(6)). The RMS provisions explicitly mention risks for fundamental rights of subjects (Art 9(2)) and state that special attention must be paid to vulnerable groups (9(9)). Importantly, they also include risks that occur when the system “is used in accordance with its intended purpose”, again acknowledging that even a compliant system can still be risky (Art 9(2)(a)). As can be implied from Article 9(5)(a), the risks in focus are the ones arising from the design and development of the AI system. Deployers need to be trained in the risks of their system and the specific context wherein it will be used (Art 9(5)(c)). If a risk is identified, the deployer is tasked with eliminating it, or otherwise developing “adequate mitigation and control measures” (Art 9(5)(b);(d)).¹³⁴ The AIA does not specify what the mitigation measures need to contain to be appropriate. The RMS is not subject to any external oversight.

ai> accessed 7 July 2025.

133 Donatella Casaburo and Irina Marsh, ‘How to Use the ALIGNER Fundamental Rights Impact Assessment Template’ 4 <https://aligner-h2020.eu/wp-content/uploads/ALIGNER_How-To-Use-FRIA.pdf> accessed 7 July 2025.

134 Here, the aforementioned general point of criticism of allowing for a residual risk again applies. This is also visible in Art 9(4), stipulating that all factors at play must be weighed to minimize risks effectively while “achieving an appropriate balance”.

3. Interplay of AI Act and German legal bases

a) Law enforcement's use of RBIS in Germany before the AI Act

While currently not having an explicit legal basis, law enforcement authorities in Germany use both retrograde and live RBI in public places.

German police applies RBIS for retroactively identifying thousands of suspects each year: The German Federal police (*Bundespolizei*, BPol) and the Federal Criminal Police Office (*Bundeskriminalamt*, BKA) conduct around 20.000 searches annually, and predict that they will likely expand RBIS use in future due to an increasing availability of images.¹³⁵ On a state level, the Criminal Police Offices (*Landeskriminalamt*, LKA) and State Police (*Landespolizei*, LPol) use RBIS with the last available data showing 75.000 annual searches and a steady increase over the years.¹³⁶ Both use the BKA's facial recognition system (*Gesichtserkennungssystem*, GES).¹³⁷ While identification is done by the GES software, BKA specialists confirm the technical result in order to ensure human oversight.¹³⁸ Recently, the GES was renewed: Now "based on AI", it is promoted as one of the world's most powerful identification systems.¹³⁹ For the search, the GES compares biometric data with the police information system (INPOL), a database containing images of convicted offenders as well as images of individuals undergoing identification procedures and images of asylum seekers.¹⁴⁰ In addition to photos officially taken in identification procedures, mobile phone photos or recordings from video cameras in public spaces are also used for the query;

135 'Drucksache 20/5781 - Antwort Der Bundesregierung Auf Die Kleine Anfrage Der Abgeordneten Andrej Hunko, Žaklin Nastić, Victor Perli Und Der Fraktion DIE LINKE.' (Deutscher Bundestag) 6 <<https://dserver.bundestag.de/btd/20/057/2005781.pdf>> accessed 19 April 2025; Christian Rath, 'Gesetzentwurf zur Gesichtserkennung lässt Fragen offen' *Legal Tribune Online* (8 December 2024) <<https://www.lto.de/recht/hintergruende/h/gesetzentwurf-zur-gesichtserkennung>> accessed 16 April 2025; BKA, 'Gesichtserkennung' (*Bundeskriminalamt*) <<https://perma.cc/NZ3K-B555>> accessed 19 April 2025.

136 Matthias Monroy, 'Neues BKA-System: Polizeiliche Gesichtserkennung geht steil' *netzpolitik.org* (16 December 2024) <<https://netzpolitik.org/2024/neues-bka-system-polizeiliche-gesichtserkennung-geht-steil/>> accessed 2 July 2025.

137 'Drucksache 20/5781 - Antwort Der Bundesregierung Auf Die Kleine Anfrage Der Abgeordneten Andrej Hunko, Žaklin Nastić, Victor Perli Und Der Fraktion DIE LINKE.' (n 135) 6; Rath (n 135).

138 'Drucksache 20/5781 - Antwort Der Bundesregierung Auf Die Kleine Anfrage Der Abgeordneten Andrej Hunko, Žaklin Nastić, Victor Perli Und Der Fraktion DIE LINKE.' (n 135) 24; 'Drucksache 20/7864 - Antwort Der Bundesregierung Auf Die Kleine Anfrage Der Abgeordneten Martina Renner, Nicole Gohlke, Gökay Akbulut, Weiterer Abgeordneter Und Der Fraktion DIE LINKE.' (Deutscher Bundestag) <<https://dserver.bundestag.de/btd/20/078/2007864.pdf>> accessed 19 April 2025; BKA, 'Erkennungsdienst' (*Bundeskriminalamt*) <<https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Erkennungsdienst/erkennungsdienst.html>> accessed 18 June 2025.

139 Monroy (n 136).

140 BKA, 'Gesichtserkennung' (n 135).

nearly half of the INPOL database derives from “non-police sources”.¹⁴¹ As of 2024, the database contains 7.6 million portrait photographs of circa 4.6 million people, and is continuously expanding.¹⁴² In 2024, the German government tried to introduce new legislation to enhance RBIS by adding to INPOL a database of pictures collected from the internet.¹⁴³ While this draft bill was not passed, similar ideas are being discussed again.¹⁴⁴

Regarding live RBI, the German police has conducted tests in public places in the past: at the train station of Mainz between 2006 and 2007, and more recently at the train station Berlin Südkreuz between 2017 and 2018.¹⁴⁵ This project was criticized by a variety of civil society actors and, as far as known, the system was not deployed after the test phase. According to the BKA, the federal police currently does not use live and public RBI.¹⁴⁶ A statement by the Federal Minister of the Interior¹⁴⁷ clarifies that before being implemented, an explicit legal basis would be needed in the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz*, BKAG¹⁴⁸).

However, on a state level, the German police does use live and public RBI: The state of Saxony permitted this from summer 2019 to December 2023 for public roads in the border region.¹⁴⁹

Following an evaluation, the authorization was not extended, since the “technical and personnel effort” was evaluated as too great, and the “professional success had not been achieved in practical operation”.¹⁵⁰ Now, a legal basis no longer exists,¹⁵¹ but Saxon police authorities continue to use

141 Monroy (n 136).

142 ‘Drucksache 20/5781 - Antwort Der Bundesregierung Auf Die Kleine Anfrage Der Abgeordneten Andrej Hunko, Žaklin Nastić, Victor Perli Und Der Fraktion DIE LINKE.’ (n 135); ‘Drucksache 20/7864 - Antwort Der Bundesregierung Auf Die Kleine Anfrage Der Abgeordneten Martina Renner, Nicole Gohlke, Gökyay Akbulut, Weiterer Abgeordneter Und Der Fraktion DIE LINKE.’ (n 138); BKA, ‘Erkennungsdienst’ (n 138).

143 Drucksache 20/12805 - Entwurf eines Gesetzes zur Verbesserung der inneren Sicherheit und des Asylsystems 2024.

144 Andre Meister, ‘Gesichtserkennung und KI: Innenminister Dobrindt plant neues Sicherheitspaket’ *netzpolitik.org* (23 July 2025) <<https://netzpolitik.org/2025/gesichtserkennung-und-ki-innenminister-dobrindt-plant-neues-sicherheitspaket/>> accessed 11 August 2025.

145 BKA, ‘Foto-Fahndung’ (*Bundeskriminalamt*)

<https://www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsprojekteUndErgebnisse/Foto-Fahndung/foto-fahndung_node.html> accessed 7 July 2025; Bundespolizei, ‘Teilprojekt 1 „Biometrische Gesichtserkennung“ Des Bundespolizeipräsidiums Am Bahnhof Berlin Südkreuz Im Zeitraum Vom 01.08.2017 - 31.07.2018’ (2018) Abschlussbericht

<https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf?__blob=publicationFile> accessed 19 April 2025.

146 Kirsten Eckstein and Philipp Girschick, ‘Biometrische Überwachung - ja, nein, vielleicht?’ *Tagesschau* (20 February 2023) <<https://www.tagesschau.de/inland/innenpolitik/ki-verordnung-101.html>> accessed 1 July 2025.

147 ‘Projekt zur Gesichtserkennung erfolgreich’ (*Bundesministerium des Innern*) <<https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2018/10/gesichtserkennung-suedkreuz.html?nn=9390260>> accessed 1 July 2025.

148 Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (*Bundeskriminalamtgesetz*) 2017 (BKAG).

149 Based on Sächsisches Polizeivollzugsdienstgesetz 2019 (SächsPVDG) para 59.

150 Referat Kommunikation und Öffentlichkeitsarbeit and Sächsisches Staatsministerium des Innern, ‘Evaluation des § 59 des Sächsischen Polizeivollzugsdienstgesetzes im Kabinett vorgestellt’

<<https://www.medienservice.sachsen.de/layouts/frontend.html.erb>> accessed 19 April 2025.

151 Based on Sächsisches Polizeivollzugsdienstgesetz para 108.

it.¹⁵² Besides Saxony, North Rhine-Westphalia, Brandenburg, Lower Saxony, Baden-Württemberg, and Berlin currently use live and public RBI.¹⁵³ For this, existing legal bases such as section 98a ‘Drogen investigations’ of the Code of Criminal Procedure (*Strafprozessordnung*, StPO¹⁵⁴) are used.¹⁵⁵ In a somewhat related scenario, state police identifies car license plates (non-biometric personal data), using section 163g StPO ‘Automatic license plate recognition’ as a legal basis. Here, images are taken by publicly installed cameras as well as mobile systems integrated in police cars, and compared by the software *PerIS* (*Personen-Identifikations-System*) against an undisclosed database in order to identify the cars’ drivers.¹⁵⁶

b) Potential implementation of live and public RBIS in Germany

As outlined in section III.2(a), member states can decide whether and in which cases (in line with AIA provisions) they choose to legalize live and public RBIS. When the Act entered into effect, a number of organizations urged the German government to prohibit the use of RBIS entirely.¹⁵⁷ On 4th December 2024, the German government published a draft bill for the implementation of the AI Act. It is divided into two different parts; the part of importance for this thesis being the AI Market Surveillance Act (*Referentenentwurf für ein KI-Marktüberwachungsgesetz*, RefE KIMÜG¹⁵⁸). Due to the discontinuity principle, this draft bill is no longer valid.¹⁵⁹ The German Cabinet was scheduled to debate a new KIMÜG in the first quarter of 2025¹⁶⁰, as the government had to issue a new bill by 2nd August 2025, including the appointment of national competent authorities for the

152 Matthias Monroy, ‘Vorsicht, Gesichtserkennung!’ *Neues Deutschland* (24 October 2023) <<https://www.nd-aktuell.de/artikel/1177253.videoueberwachung-vorsicht-gesichtserkennung.html>> accessed 16 April 2025.

153 Johanna Hahn, ‘Ein Anfang, Mehr Nicht’ (*Verfassungsblog*, 11 December 2024) <<https://verfassungsblog.de/ein-anfang-mehr-nicht/>> accessed 15 April 2025; Daniel Leisegang, ‘Umstrittene Observationstechnik aus Sachsen: Auch Brandenburg betreibt biometrische Videoüberwachung in Echtzeit’ *netzpolitik.org* (5 August 2024) <<https://netzpolitik.org/2024/umstrittene-observationstechnik-aus-sachsen-auch-brandenburg-betreibt-biometrische-videoueberwachung-in-echtzeit/>> accessed 1 July 2025.

154 Strafprozeßordnung 1987 (StPO).

155 Kilian Vieth-Ditlmann and Pia Sombetzki, ‘Stellungnahme Zur Öffentlichen Anhörung Des Ausschuss Für Digitales Am 15. Mai 2024 Zur Nationalen Umsetzung Der KI-Verordnung’ (AlgorithmWatch 2024) <<https://www.bundestag.de/resource/blob/1002768/411c38bedaf76d16f5aaf0c34f729766/Vieth-Ditlmann.pdf>> accessed 2 July 2025.

156 Leisegang (n 153).

157 AlgorithmWatch and others, ‘Offener Brief: Menschenrechte Schützen – Biometrische Fernidentifizierung Verbieten’ (März 2024) <<https://www.amnesty.de/sites/default/files/2024-03/Gemeinsamer-Offener-Brief-Biometrische-Ueberwachung-Maerz-2024.pdf>> accessed 16 April 2025.

158 Regierung der Bundesrepublik Deutschland, Gesetzentwurf der Bundesregierung - Entwurf eines Gesetzes zur Neuordnung der Marktüberwachung.

159 Marlene Schreiber and Pascal Bronner, ‘Der Referentenentwurf Für Ein Gesetz Zur Durchführung Der KI-Verordnung’ (2025) ITR 7/2025 juris PraxisReporte.

160 ‘Drucksache 20/12948 - Antwort Der Bundesregierung Auf Die Kleine Anfrage Der Fraktion Der CDU/CSU – Drucksache 20/12671 Nationale Umsetzung Des AI Act in Deutschland’ (Deutscher Bundestag 2024) <<https://dserver.bundestag.de/btd/20/129/2012948.pdf>> accessed 15 April 2025.

implementation of the AIA.¹⁶¹ However, it did not meet these requirements due to an early election in February 2025 that created a transitional phase. The new draft bill is currently still being coordinated between the involved ministries.¹⁶²

Currently, a legislative change to legalize the use of live and public RBIS is not being discussed. However, the German government might opt for permitting it in future, since German police has already used it (and LPol currently uses it without explicit legal basis), and while the previous government had explicitly ruled it out in its coalition agreement,¹⁶³ the current coalition has not done so. In its agreement, the coalition proclaims a “security offensive”, and while it does not mention legalizing live and public RBIS yet, it plans to integrate online images into the reference database.¹⁶⁴ As no legal basis exists for live and public RBIS, possible control mechanisms over it are also unclear.¹⁶⁵ However, looking at the current powers of authorities responsible for controlling AI systems as per AIA (in subsection (i)), and outlining the laws that would need to be amended to integrate live and public RBIS in law enforcement practice (subsection (ii)) provides insights about potential control mechanisms in Germany.

i) German authorities that would control law enforcement’s use of live and public RBIS

(1) Fundamental Rights Protection Authorities

Already in November 2024, Germany appointed its FRPA: the federal and state DPA, the Ombudsman of the State Office for Equal Treatment, and the Federal Anti-Discrimination Agency.¹⁶⁶

161 Deutscher Bundestag, ‘Nationale Umsetzung des AI Act in Deutschland’ (*Deutscher Bundestag*, 9 June 2024) <<https://www.bundestag.de/presse/hib/kurzmeldungen-1016762>> accessed 15 April 2025.

162 Felix Rieger, ‘KI-Verordnung: Deutsches Durchführungsgesetz verzögert sich’ (*Medien Bayern*, 4 July 2025) <<https://medien-bayern.de/ki-verordnung-deutsches-durchfuehrungsgesetz-verzoegert-sich/>> accessed 4 August 2025.

163 SPD, Bündnis 90/Die Grünen and FDP, ‘Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit - Koalitionsvertrag 2021–2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP) - 20. Legislaturperiode’ Koalitionsvertrag 86.

164 CDU, CSU and SPD, ‘Verantwortung für Deutschland – Koalitionsvertrag zwischen CDU, CSU und SPD - 21. Legislaturperiode’ Koalitionsvertrag.

165 Johanna Hahn, *Automatisierte Gesichtserkennung in Der Strafverfolgung* (Nomos Verlagsgesellschaft mbH & Co KG 2025) 34.

166 European Commission (n 122).

(2) Data Protection Authorities

Due to the federal structure of the German government, DPA exist on a federal and on a state level, with each state's DPA controlling the data protection of its respective law enforcement authorities (LKA and LPol). On a federal level, the DPA is the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*, BfDI), an independent supreme federal authority organized into specialized departments, including one overseeing federal law enforcement authorities (i.e, BKA and BPol). On a state level, the DPA are the State Commissioners for Data Protection (*Landesbeauftragte für den Datenschutz*, LfD). If the respective state has a freedom of information or transparency law, the LfDs also act as supervisory authorities in this regard.¹⁶⁷ Among the duties of the German DPA, stipulated in the Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG¹⁶⁸), is that the BfDI gives recommendations for improving data protection to legislators (s 14(1)-(2) BDSG). The BfDI is also responsible for raising awareness among authorities controlling data, including law enforcement (s 14 (1)(4)). Regarding infringements on data protection, the BDSG grants a number of controlling powers to the BfDI: If DPA notice a data protection infringement by an individual operating within a public body, the BfDI can file an application to the public prosecutor's office (s 42). Additionally, individuals can lodge complaints against the data processing of public bodies with the BfDI (s 60), upon which the BfDI has to follow up (s 14(1)(6)). In case of data protection infringements, the BfDI is tasked with conducting investigations (s 14 (1)(8)). When this infringement is suspected of a law enforcement authority, the BfDI is granted access over data that are otherwise classified as "special official secret" (s 16(3)), and needs to receive access to law enforcement's premises at all times, to its systems and equipment and to all "personal data and information necessary for the performance of their duties" (s 16(4)). When an infringement is found, the BfDI can notify the responsible supervisory authority, such as the ministry under which a respective law enforcement authority operates, and issue a complaint (s 16(2)). This is important: While the BfDI is responsible for "enforcing the application" of the BDSG and other provisions on data protection (s 14(1)), and the LED explicitly requires that DPA are provided with "effective legal remedies" (Art 47(2) LED), when it comes to powers over law enforcement, the BfDI can only investigate, notify and issue complaints. It cannot issue bans or fines.¹⁶⁹

167 BfDI, 'Landesbehörden' (*Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) <<https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html>> accessed 2 July 2025.

168 Bundesdatenschutzgesetz 2017 (BDSG).

169 See BfDI, 'Aufgaben Und Befugnisse Der BfDI' (*Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) <<https://www.bfdi.bund.de/DE/BfDI/Inhalte/BfDI/AufgabenBFDI.html>> accessed 12 July 2025.; a fact that some legal scholars have criticized as incompatible with EU law, see Paul Friedl and Louis Rolfes,

With regard to the resources of the BfDI, section 6(2) BDSG stipulates that the BfDI needs to be equipped with the resources necessary to perform its tasks and “to maintain his or her expertise”. The current German government plans to reform data protection powers and responsibilities. As specified in their coalition agreement, the government plans to bundle more responsibilities with the BfDI that previously belonged to the LfDs, a centralization that might lead to considerable financial and personnel hurdles.¹⁷⁰

(3) Market Surveillance Authorities

There is no final decision on the MSA appointed for RBIS used by law enforcement, and a new RefE KIMÜG is not available yet. While different authorities are being advocated for the position,¹⁷¹ the appointment ultimately remains a normative political decision.¹⁷² However, it is likely that a new bill will appoint the same authorities as the previous bill.¹⁷³ Therefore, the German MSA as per the first draft bill will be outlined here.

The previous RefE KIMÜG appointed the Federal Network Agency (*Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, BNetzA) as general MSA for AI products. For market surveillance over high-risk systems like RBI used by law enforcement, the AIA specifically names the DPA or “or any other authority designated pursuant to the same conditions” as appropriate MSA (Art 74(8) AIA). Accordingly, the BfDI states on its website that it intends to act as MSA in this regard.¹⁷⁴ The BNetzA states on its own website that this mandate will

‘Datenschutz gegen digitalen Autoritarismus’ (*Verfassungsblog*, 21 August 2024)

<<https://verfassungsblog.de/datenschutz-gegen-digitalen-autoritarismus/>> accessed 17 June 2025.

170 CDU, CSU and SPD (n 164); LTO, ‘Datenschutzaufsicht: Droht eine teure Mammuthbehörde?’ *Legal Tribune Online* <<https://www.lto.de/recht/hintergruende/h/datenschutz-aufsicht-bfdi-koalitionsvertrag-datenschutzbeauftragte-bonn>> accessed 31 July 2025.

171 Mario Martini and Jonas Botta, ‘Nationale KI-Aufsicht: Aufgaben, Befugnisse und Umsetzungsoptionen’ (Bertelsmann-Stiftung 2024) <<https://www.bertelsmann-stiftung.de/doi/10.11586/2024054>> accessed 2 July 2025; Lajla Fetic, ‘Nationale Spielräume Bei Der Umsetzung Des Europäischen Gesetzes Über Künstliche Intelligenz’ 8; Datenschutzkonferenz (DSK), ‘Orientierungshilfe Der Konferenz Der Unabhängigen Datenschutzaufsichtsbehörden Des Bundes Und Der Länder Vom 6. Mai 2024’ (Datenschutzkonferenz (DSK) 2024) Orientierungshilfe <https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf> accessed 2 July 2025; Deutscher Bundestag, ‘Nationale Aufsicht bei Künstlicher Intelligenz komplex’ (*Deutscher Bundestag, Parlamentsnachrichten*, 16 May 2024) <<https://www.bundestag.de/presse/hib/kurzmeldungen-1003008>> accessed 4 July 2025.

172 Fetic (n 171) 8.

173 A fact supported by recent information posted on the website of the Bundesnetzagentur, see Bundesnetzagentur, ‘KI Service Desk’ (*Bundesnetzagentur*) <https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/start_ki.html> accessed 4 August 2025.

174 BfDI, ‘Technische Anwendungen - Die KI-Verordnung Der EU’ (*Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) <<https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/KI-Verordnung.html>> accessed 23 September 2024.

be exercised by itself.¹⁷⁵ The RefE KIMÜG stipulated the formation of an independent subauthority: the independent market surveillance chamber (*Unabhängige Marktüberwachungskammer*, UKIM), since the BNetzA was not seen as sufficiently independent for controlling law enforcement.¹⁷⁶ This agency was supposed to be completely independent from instructions of the BNetzA, while still having access to its resources (s 3(5) RefE KIMÜG). The KIMÜG names “difficulties in demarcation” as an argument against appointing the DPA, specifically unclear responsibilities and different contact persons for companies and administration, and difficulties for attaining a uniform interpretation and application (s 3).

Regarding their resources, as “national competent authority” for AI, the MSA needs to be equipped with resources to perform their duties competently, including a “sufficient number of personnel permanently available” with an in-depth understanding fundamental rights (Art 70(3) AIA). The UKIM would still have access to the resources of the BNetzA. Since the BNetzA has recently taken on a new mandate (concerning the Digital Services Act), it has grown in terms of financial and personnel resources, expecting further growth in future.¹⁷⁷ An allocation of further resources is expected to ensure the fulfillment of its AIA mandate. However, some legal scholars doubt that the UKIM’s mandate and resources with regard to fundamental rights are congruent with the requirements set in the AI Act.¹⁷⁸

ii) German laws that would regulate law enforcement’s use of live and public RBIS

Currently, RBI in Germany is practiced based on general clauses of the StPO. These are, however, insufficient as a legal basis, since they do not specify RBIS’ material requirements, technical procedures or precautions for the process.¹⁷⁹ Additionally, the legal basis section 98 StPO ‘Dragnet investigations’ does not suffice because it only concerns the comparison between images, not the creation of a photo or video to identify a suspect.¹⁸⁰ Hence, Germany would need new laws if it were to allow the use of live and public RBIS by law enforcement.

175 Bundesnetzagentur, ‘Marktüberwachung’ (*Bundesnetzagentur*) <https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/14_Marktueberwachung/start.html> accessed 4 August 2025.

176 Deutscher Bundestag (n 171).

177 Fetic (n 171) 8.

178 Schreiber and Bronner (n 159).

179 Antonia Buchmann and Dieter Kugelmann, ‘Big Brother Is Analyzing You’ (*Verfassungsblog*, 11 December 2024) <<https://verfassungsblog.de/big-brother-is-analyzing-you/>> accessed 7 July 2025.

180 Stephan Schindler, ‘Im Auge der Polizei’ (*Verfassungsblog*, 20 December 2021) <<https://verfassungsblog.de/os3-auge-polizei/>> accessed 7 July 2025.

If Germany were to legalize RBIS, its concrete procedures and control mechanisms would need to be specified firstly in an AIA implementation bill, and secondly by amending existing laws, the choice of which depends on the authorities and cases for which the government would want to allow live and public RBI. Often, these legal changes are introduced as part of a “security package” (*Sicherheitspaket*), a tactical move to prevent nitpicking on single legal changes and to demonstrate the government’s determination to act, for instance after forming a new government.¹⁸¹

Firstly, the StPO would need to be amended, to detail provisions for the use of live and public RBIS, most likely by adding a new section (like section 100b that was added recently to allow for conducting ‘Online searches’). The StGB would not need to be amended, as it only provides the definitions of the specific offenses named in AIA Annex II, such as section 129 ‘Forming criminal organizations’. Secondly, the BKAG would possibly need to be amended. The BKA is responsible for “coordinat[ing] crime suppression at national and international level”, and does so on the one hand through the prevention of crimes, on the other hand through investigating them.¹⁸² It is, for instance, responsible for preventing and investigating cases of international crime, as well as matters of “state security” (*Polizeilicher Staatschutz*) in cases of politically motivated crime. When the BKA investigates, its legal basis is the StPO; when it acts in a preventive way, its legal basis is the BKAG. If live and public RBIS were to be legalized for crime prevention in Germany, the BKAG would need to be amended (specifically section II, subsection I “data collection”, subsection II “data processing”, and subsection III “data transfer”). Thirdly, the Federal Police Act (*Bundespolizeigesetz*, BPolG¹⁸³) might an amendment. The BPol is responsible for the protection of all goods that fall outside of state jurisdiction, such as aviation security, railway, sea, and border protection. As with the BKA, the BPol’s tasks are preventative (with the BPolG as legal basis) as well as investigative (with the StPO as legal basis). Were the BPol to use live and public RBIS for the prevention of crimes against the aforementioned goods, the BPolG would need to be changed (specifically section II, subsection II “data collection, processing and usage”). Additionally, in the federal structure of Germany, police legislation is a state matter, and therefore, each state has its own Police Duties Act (*Polizeiaufgabengesetze*, PAG) specifying powers and duties of its police (of course without contradicting the provisions of StPO and StGB). In case the German government would want to legalize its use for police on a state level, the respective PAGs of each state would need to be amended. Lastly, the BDSG as the legal text determining the responsibilities of the

181 See e.g., ‘Sicherheitspaket der Bundesregierung’ (*Bundesministerium des Innern*) <<https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/sicherheitspaket/sicherheitspaket-artikel.html?nn=21255176>> accessed 13 August 2025; Meister (n 144).

182 ‘BKA - Our Mandate’ <https://www.bka.de/EN/TheBKA/OurLegalMandate/ourmandate_node.html> accessed 4 July 2025.

183 Gesetz über die Bundespolizei (*Bundespolizeigesetz*) 1994 (BPolG).

German DPA might need to be amended as well, if the BfDI would take on new tasks during the RBIS process that exceed its current mandate.

How exactly these laws would be changed, and specifically, which control mechanisms would be integrated within them, will need close attention – according to Hahn, their design is “a key challenge for security legislation today”.¹⁸⁴ For now, the mechanisms that can be evaluated are the ones outlined as minimal condition in the AIA, to see whether they suffice with regard to controlling risks to (and infringements on) fundamental rights caused by an interpretative expansion of legal bases.

Example case: Law enforcement’s use of live and public RBIS against activist suspected of participating in a ‘section 129 organization’ involved in ‘sabotage’ in Germany

Location chosen: Bavaria. Based on the strategic interpretative expansion of LG Bavaria as a ‘criminal organization’ under s 129 StGB involved in ‘sabotage’ under s 315b, to subject an unidentified climate activist to live and public RBIS, firstly, the StPO as well as the Bavarian PAG are amended to include an additional section on live and public RBIS. The supervisory structures concerning its usage are stipulated in the new KIMÜG.

Before any application of RBIS, the Bavarian LKA conducts a FRIA for the system, and identifies mitigation measures against its risks to fundamental rights. These might be controlled by the respective German MSA (BfDI or UKIM), but might also fall under the national security exception, exempting them from external control. Also, the RBIS is tested by the Bavarian LKA as part of their RMS (without external supervision).

In a concrete application case, the LKA requests an authorization for identifying an unknown activist by a judge or an “independent administrative authority” (the authority will be specified in the StPO). This authority decides that the method is appropriate and necessary; less invasive means of identification are not available. The LKA films the unidentified climate activist during a demonstration, and, in real time, the GES runs his biometric data set against the INPOL to identify him. One scenario further, the StPO and respective PAGs are amended to also allow checking these data points against a database containing “various pictures from the internet” similar to the software of *ClearviewAI*¹⁸⁵. In this scenario, even individuals who are not registered in INPOL could be identified, for instance through images on their social media accounts. The activist is subsequently identified, enabling the Bavarian LKA to charge him for his LG membership in court. At some point, the Bavarian LfD and the MSA are notified of the request and result of the

¹⁸⁴ Hahn (n 165) 21.

¹⁸⁵ ‘Clearview AI | Facial Recognition’ (*Clearview AI*) <<https://www.clearview.ai>> accessed 13 August 2025.

RBIS use. The LfD could request the Bavarian LKA to disclose documentation on this case, without getting access to sensitive operational data. At a later stage, the RBIS activity appears as a number in the annual report submitted by the BfDI and the MSA to the EC; it reappears as a number in the aggregated annual report by the EC to the public. If the MSA at any stage notices a risk for fundamental rights, it can evaluate the RBIS. If it finds it to be legally compliant but still infringing upon fundamental rights, it can order corrective measures to the Bavarian LKA to restrict the system's negative impact.

IV. Legal evaluation

1. Evaluation of the AI Act's control mechanisms' sufficiency and identification of controlling criteria

Having outlined the AIA's control mechanisms as well as a potential implementation in Germany, this section will now evaluate whether these mechanisms are sufficient. Specifically, section III.1(e) established that liberal constitutionalism, when applied to the risk of a strategic interpretative expansion, needs to control the use of a surveillance mechanism on its impacts for fundamental rights. From this, two first important criteria for control mechanisms can be deduced, namely:

- 1) The mechanism needs to control the use of RBIS *substantially*, not only formally. To spot a strategic interpretative expansion and prevent its adverse effects on fundamental rights, it needs to *control against a fundamental rights baseline*.
- 2) This needs to happen for controlling RBIS' *impact on a case-by-case as well as on a systemic level, controlling before as well as after the fact*.

Case-by-case, the adverse impact of each single RBIS use on fundamental rights of the affected person or third parties needs to be controlled. This includes assessing the potential impact (i.e. the *risk*) before any authorization, as well as rights *infringements* caused by a concrete use.

Additionally, even multiple non-infringing single cases can lead to adverse impacts on society as a whole. Hence, on a systemic level, the overall impact of RBIS use on fundamental rights in a society needs to be controlled (again controlling risks as well as infringements).

However, spotting such an adverse effect is only one part of an effective control. Evaluating the AIA's control mechanisms might lead to the identification of further criteria necessary not only for spotting, but also for sufficiently retaining a potential fundamental rights-infringing use.

a) Authorization

Since surveillance usually happens covertly, the suspect has no way of legally defending himself against it. Hence, in cases of invasive surveillance mechanisms (as is also the case for sections 100a StPO 'Telecommunications surveillance', 100b 'Online search'), judicial reservation is installed to guarantee the protection of fundamental rights in the suspect's place.¹⁸⁶ In this way, the rights infringement intrinsic to such a surveillance measure is supposed to be counterbalanced.

When a judge or another appointed independent administrative authority receives an authorization request for live and public RBIS by law enforcement, it decides over it based on the following questions: firstly, whether the suspect is under investigation for one of the specified crimes (Art 5(2) (h) AIA, and in case of (iii), Annex II). Secondly, to guarantee personal limitation, it controls whether the measure is taken only to confirm the identity of this specific individual, and thirdly, whether the parameters set for temporal and geographic limitation are compliant with defined procedural law (Art 5(2)-(3)). These first three criteria all solely answer questions of compliance: as long as the request complies with these procedural formalities, it will be authorized. The next criteria for an authorization are whether the RBIS use is "necessary" in the specific case; meaning whether less invasive methods might lead to the same result, and whether the use is "proportionate" (Art 5(3)). This last criterion is particularly important: Here, the harm done when a measure is used is balanced against the harm done when not used. Such a balance could potentially include criteria that fall outside of mere compliance, including risks for fundamental rights. However, in practice, the answer to this proportionality test is derived from positively answering the first four questions: If the crime is listed, the request limited in terms of scope, and less invasive methods unavailable, the request will be considered proportionate, and consequently authorized. It follows that the control mechanism of authorization merely considers formal compliance; none of the criteria consider "whether a use of RBIS is in line with fundamental rights". Therefore, this mechanism cannot spot a fundamental rights risk based on a strategic interpretative expansion.¹⁸⁷

186 Silke Hüls, 'Der Richtervorbehalt – Seine Bedeutung Für Das Strafverfahren Und Die Folgen von Verstößen' (2009) 4 Zeitschrift für Internationale Strafrechtsdogmatik 160.

187 Since the authorization happens prior to the deployment, a mechanism needs to control for risks rather than infringements.

A second question is whether this mechanism, if it were to spot such a risk, could sufficiently *retain* it. Since authorization is a legally binding mechanism (no RBIS use without authorization), it theoretically has effective controlling powers. However, a closer look at the practice of authorization reveals that while theoretically powerful, it has significant practical shortcomings. Firstly, by allowing the authorization to be done by any “independent administrative authority”, the division of powers between state authorities is lost, since administration and law enforcement both form part of the executive.¹⁸⁸ Therefore, legal scholars have argued that this mechanism has to be exercised by a judicial court, also referencing European Court of Justice (ECJ) case *Pierre Corbiau v Administration des contributions* which stipulates when an authorization has high impacts on an individual’s rights, it needs to be exercised by an independent body genuinely separate from the administration¹⁸⁹. Another cited argument is ECHR case *Glukhin v. Russia* wherein the Court pointed out that the authorizing procedure for public RBIS needs a “high level of justification” which can only be granted by an independent judicial body.¹⁹⁰

Secondly, the practice of judicial reservation in Germany has been titled “practically ineffective” and a legal “fig leaf”,¹⁹¹ since these processes happen so frequently that the authorizing entity lacks the resources to read each request in-depth.¹⁹² In a number of evaluated cases, judges even instructed law enforcement authorities to use their exception clause (postponing the authorization process), since meaningfully granting authorization was not perceived as manageable.¹⁹³

Authorizing judges have also reported that it is common practice to not read each request but trust the requesting entity, and therefore simply add date and signature (which has been dubbed a “copy-and-paste-practice”).¹⁹⁴ Also, due to the nature of RBIS use (often coupled with either an imminent threat or a spontaneous possibility to identify a suspect), authorization is usually requested on short notice, leaving limited time for a deeper reflection on every use’s proportionality.¹⁹⁵ The time factor often leads to the authorization being exercised retroactively, another point of criticism: In this case, law enforcement authorities themselves decide on when to temporarily bypass the judge, practically implying that “the body being controlled decides on the intervention of the supervisory authority”.¹⁹⁶ Studies show that this exception clause has become the rule, as a majority of measures

188 Andreas P Müller, ‘Orwell’sche Gleichgültigkeit und Europäische Demokratie’ (*Verfassungsblog*, 23 January 2024) <<https://verfassungsblog.de/orwellsche-gleichgultigkeit-und-europaische-demokratie/>> accessed 7 July 2025.

189 Federica Paolucci, ‘Shortcomings of the AI Act’ (*Verfassungsblog*, 14 March 2024) <<https://verfassungsblog.de/shortcomings-of-the-ai-act/>> accessed 7 July 2025; Müller (n 188); *Pierre Corbiau v Administration des contributions* [1993] European Court of Justice C-24/92.

190 *Glukhin v Russia* [2023] European Court of Human Rights 11519/20 [86]; Paolucci (n 189).

191 Paolucci (n 189); Müller (n 188); Hans Lilie, ‘Verwicklungen im Ermittlungsverfahren’ (1999) 111 ZStW 807, 807.

192 Hans Meyer-Mews, ‘„Keine Bloße Formsache“ – Notizen Zum Richtervorbehalt’ (2020) 7 HRRS 294.

193 Hüls (n 186) 162.

194 Meyer-Mews (n 192) 286.

195 Hüls (n 186) 161.

196 *ibid.*

controlled by judicial reservation are only authorized retroactively.¹⁹⁷ They also show that a high percentage of surveillance requests are granted without any changes, which might indicate that law enforcement and judiciary share views on the proportionality of such requests, without the judiciary acting as a critical controlling instance.¹⁹⁸ This overall devaluation of the judicial reservation has even been deemed unconstitutional by jurisprudence of the BverfG.¹⁹⁹ To conclude, the mere linking of surveillance mechanisms to judicial reservation does not seem to suffice for a meaningful control. From this, several additional criteria can be deduced for a control mechanism to sufficiently retain a risk for fundamental rights based on a strategic interpretative expansion:

- 3) The mechanism needs to have *legally binding consequences*.
- 4) The legally binding consequences need to be enacted by an *independent authority* that is not part of the executive.
- 5) The controlling entity needs to be provided with *sufficient resources* to exercise its control in a meaningful way.

b) Notification

As stipulated in Article 5(4), DPA and MSA need to be informed of the authorizing request and its result. This means that both authorities know *that* an RBIS use was authorized (or prohibited), but do not have information on the underlying legal basis of the request, or the reason for prohibiting or authorizing it. Without access to information about the content of a case, they cannot qualitatively evaluate the measure; among other things, whether the measure taken poses significant risks to fundamental rights (or in case it is already completed, whether it caused an infringement). The notification only serves to inform DPA and MSA, and enables the DPA to subsequently report the total annual use (see section III.2(c)(iii)).

Secondly, again looking at the potential of this mechanism to not only spot but also *retain* a rights risk or infringement, it can be noted as a positive point that both DPA and MSA are independent bodies (see criterion (4)). Their powers to enact legal consequences (see (3)) as well as their available resources (see (5)) differ; arguably, the MSA has more resources and effecting powers than the DPA (see section III.2(b)).

¹⁹⁷ *ibid.*

¹⁹⁸ *ibid* 165.

¹⁹⁹ Meyer-Mews (n 192) 294.

It is important to note that Article 5(4) does not specify when exactly DPA and MSA should be notified. This is, however, relevant, since they can only make use of any interventive powers when they are notified in time. Taking bad faith as a baseline assumption, without stipulation of the exact time of the notification, there is a danger that law enforcement will use this loophole to postpone a notification in a way that serves to avoid being controlled effectively. This leads to two additional criteria for a control mechanism to suffice:

6) The mechanism needs to control RBIS not only quantitatively, but also qualitatively. It thus needs access to the *content* of each RBIS request.

7) The mechanism's procedures need to be *specific* rather than vague, closing any legal loopholes that might otherwise be exploited by the executive.

c) Disclosure of documentation

This mechanism alleviates the deficits of b) Notification to an extent: DPA and MSA can request the disclosure of documentation from law enforcement (Art 26(10)). The only limit to such a disclosure is the exclusion of sensitive operational data. This increases the transparency over RBIS use for DPA and MSA. Since in this case, qualitative information (such as the use's content and grounds for authorization) is provided, they might be able to spot whether an RBIS use is no longer in line with fundamental rights. Of course, simply having access to this information does not guarantee a control against a fundamental rights baseline.

Also, as an "in-case control", the disclosure of documentation only happens upon a specific request, not automatized or on an otherwise regular basis. This might lead to the controlling authorities only conducting spot checks, either arbitrarily or upon suspicion of an infringement, and hence not having an overview of all RBIS cases. In this way, they might find, but might also miss out on a rights-infringing use based on a strategic interpretative expansion. For spotting it, this mechanism is thus necessary, but insufficient. Hence, two additional criteria can be added:

8) The mechanism needs to be exercised *systematically*, not just "in-case".

9) The entity of evaluation needs to be "*all the cases*", not merely "multiple single cases".

d) Evaluation of high-risk AI system

As stipulated in Article 79(2), whenever the MSA perceives a risk, it carries out an evaluation of the AI system in question. If it has “sufficient reason to consider a risk” to fundamental rights, it can additionally conduct a technical test of the system. The AIA does not specify what such an evaluation and/or technical test would contain, but based on the test’s results - potentially leading to “formal non-compliance” (Art 83) - it can be deduced that this mechanism primarily evaluates the procedural compliance of a system’s use. Additionally, a technical test can evaluate whether the technology itself complies with AIA requirements. This control mechanism thus does not focus on detecting uses that might be compliant in terms of procedure and technology, but still infringe upon fundamental rights.

On top of that, the same point of criticism as under c) Disclosure of documentation applies: Like that mechanism, the evaluation (and potentially a technical test) is only conducted ad hoc upon perceiving a risk, not on a systematic basis. Another point with regard to the ability to spot a rights-infringing use is the concrete MSA mandate assignment: Depending on the authority chosen and its respective mandate and resources, the instance might be differently equipped to spot and evaluate uses that infringe upon fundamental rights (see section III.2(b)).

With regards to *retaining* risks or infringements, Article 79(2) orders law enforcement to “cooperate as necessary” with the MSA; as such, it grants effective controlling powers to the MSA. These powers include effecting legally binding consequences: If an AI system is found to be non-compliant, it can be banned, and providers can be sanctioned. With Article 82 on “Compliant AI systems which present a risk”, the AIA also acknowledges the possible scenario of a compliant, but still rights-infringing use. However, for such a case, it fails to specify consequences. The MSA can only require law enforcement to take “appropriate measures” to ensure that the system no longer presents that risk. What such measures would entail is not specified. Also, unlike in the case of formal non-compliance, Article 82 does not mention the possibility of a system’s ban. While sanctioning deployers would not be appropriate when they have acted in a compliant way, effective consequences such as a ban need to be stipulated nevertheless, to effectively retain an RBIS use that poses a risk or infringes upon fundamental rights. Similar to the discussion under b) Notification concerning the vagueness of a control mechanism’s procedure, it can thus be deduced:

10) For the case of a compliant but still fundamental rights-risking or -infringing application, the mechanism needs to stipulate *concrete consequences*, including the possibility of a *ban*.

e) Fundamental Rights Impact Assessment

The FRIA is done by law enforcement (and handed to the MSA) prior to the implementation of a high-risk AI system to assess and mitigate its potential impacts on fundamental rights (Art 27). Since this instrument specifically addresses fundamental rights, it might be suited to assess and address fundamental rights risks based on a strategic interpretative expansion. However, as described in section III.2(c)(iii), the ALIGNER-template operationalizes the FRIA by naming four relevant categories of fundamental rights, and predefines risks within these categories. All listed risks concern either the development of the technology itself (e.g., “The AI system targets members of a specific social group”) or procedural questions related to data protection (e.g., “There are no mechanisms for the user to exercise control over the processing of personal data”). As such, the FRIA template ignores what is acknowledged in parts of the AI Act, namely, that a technically and procedurally sound implementation of an AI system can still pose risks to fundamental rights. Additionally, by limiting the impact to four fundamental rights categories, the template overlooks that impacts on other fundamental rights might also occur.²⁰⁰ By its design, the template thus excludes risks that are less direct, and hence less visible, as well as risks that are not among the commonly known risks (described in section II.5). From the theoretical part of this thesis, it has become clear that autocratic legalists do not follow the script book of fascism – their strategies might hence not be clear in advance. Also, they use and abuse law in all possible ways, often in a legally compliant fashion. To spot indirect and abstract risks to fundamental rights, the FRIA would hence need to be operationalized in an open-ended way, not preemptively excluding unforeseen risks. Also, since the FRIA is executed only once prior to the deployment of the system, and only repeated if the technical system itself changes significantly, this mechanism cannot integrate unforeseen risks that become apparent at a later stage. From this, two additional criteria can be deduced:

- 11) The mechanism needs to be formulated in an *open-ended* way to integrate risks for fundamental rights that are less direct and less foreseeable.
- 12) To enable the integration of previously unforeseen risks, the control needs to be *repeated* over time (in a systematic way (8), by evaluating “all the cases” (9)).

200 Muhammed Demircan, Heidi Waem and Jeanne Dauzier, ‘Fundamental Rights Impact Assessments under the EU AI Act: Who, What and How?’ (*Technology’s Legal Edge*, 7 March 2024) <<https://www.technologyslegaledge.com/2024/03/fundamental-rights-impact-assessments-under-the-eu-ai-act-who-what-and-how/>> accessed 7 July 2025.

A second consideration when judging the ability of this mechanism to spot the risk in question is whether the body executing the FRIA is well-equipped to do so. In conducting the assessment, law enforcement is supported by templates of ALIGNER - a working group mainly consisting of law enforcement actors. The lack of involvement of other actors within the FRIA has been a common point of criticism by civil society organizations.²⁰¹ The argument is that law enforcement might not be suited to spot such risks, since their mandate is *enforcing* the law. It is not “questioning” or “critically assessing” law, so they might not be equipped to spot risks arising through a legally compliant system application. Also, due to their specific mandate, law enforcement is under a certain pressure to present perpetrators,²⁰² which might incline them to use potent systems such as RBIS in order to fulfill their mandate effectively, and might be less inclined to assess this system critically.

Secondly, coupled with the question of a proper mandate with regard to fundamental rights, is the question of the necessary resources in this regard; primarily in terms of an in-depth knowledge of fundamental rights and related risks. This complex body of knowledge, consisting of extensive case law by CJEU as well as ECHR, requires an in-depth and holistic understanding²⁰³ - a knowledge that, due to their mandate, law enforcement might not possess. It has already been established that the body enacting binding controls needs to be independent from the executive (see (4)), and that it needs to be sufficiently resourced (see (5)). To this, another criterion can be added:

13) The independent controlling instance needs to be equipped with a *mandate and an in-depth knowledge of fundamental rights*.

With regard to the question whether the FRIA is able to *retain* a risk once identified, the second ALIGNER- template (“AI System governance”) offers insights, as it identifies possible measures to mitigate risks identified in the first template.²⁰⁴ These measures are categorized into different clusters. While - congruent with the risk operationalization - most of these clusters concern technical and procedural compliance, one category is titled: “Democracy and societal wellbeing”, based on the statement of the EC that the potential “societal impact should be carefully considered” for “all human beings, including future generations”.²⁰⁵ The template offers two mitigation

201 Alice Giannini and Sarah Tas, ‘AI Act and the Prohibition of Real-Time Biometric Identification’ (*Verfassungsblog*, 10 December 2024) <<https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/>> accessed 23 June 2025.

202 Hüls (n 186) 161.

203 Demircan, Waem and Dauzier (n 200).

204 ‘Fundamental Rights Impact Assessment (FRIA) | aligner’ (n 130).

205 European Commission (n 132).

measures: firstly, that “there are procedures to assess the broad social impact of the AI system (e.g., chilling effect, power asymmetry, trust, ...).”²⁰⁶ What these procedures need to contain is left open for interpretation by law enforcement. The same criterion as defined under b) Notification applies here; namely, that control mechanisms need to be specific rather than vague, to leave little room for a *mala fides* interpretation by the executive. The second mitigation measure is that “there are mechanisms to limit the deployment of the AI system to groups of individuals on the basis of suspicion/objective criteria”.²⁰⁷ Here, the mitigation measure fails to acknowledge risks that lie beyond compliance; that when “suspicion/objective criteria” are interpreted in bad faith, the use of a compliant system might still result in substantial risks in need of mitigation.

Lastly, to mitigate the fact that the risk assessment is conducted by the deployer himself, Article 27(3) stipulates that the MSA needs to be notified of the FRIA’s results through receiving the filled out template. In case the MSA notices a remaining risk to fundamental rights, it can proceed with its usual mandate (including an evaluation, see section III.2(c)(ii)). But: In cases concerning national security (Art 46(1)), deployers do not need to notify the MSA (27(3)). Since law enforcement itself decides when national security is at stake, and thus when their own controlling instance is to be bypassed, the potential binding consequences of this mechanism are factually undermined. From this, another essential criterion can be deduced, namely:

14) The “national security” general exception clause (Art 46(1)) *should not be applicable when controlling risks for fundamental rights*.

f) Annual reports

The annual reports, firstly by DPA and MSA to the EC (Art 5(6)), secondly the aggregate report by the EC (5(7)), serve to generate transparency over the use of RBIS to the general public. In fact, the annual reports by the EC are the *only* piece of information that provides public transparency over RBIS use: The mechanisms of b) Notification and c) Disclosure only enhance transparency for DPA and MSA, while d) Evaluation and e) FRIA are not published at all. As per AIA provisions, even the report by DPA and MSA to the EC is not necessarily published. Again taking bad faith as baseline assumption, it is important to ensure as much public scrutiny as possible. Therefore, reporting is essential for public scrutiny over potential infringements on fundamental rights.

²⁰⁶ ‘Fundamental Rights Impact Assessment (FRIA) | aligner’ (n 130).

²⁰⁷ *ibid*.

The same drawback as noted under b) Notification applies for the annual reports: Since they only publish the number of requested uses, as well as the requests' results, they do not contain any qualitative information, and without this, a rights-infringing use based on a strategic interpretative expansion cannot be found (see (6)). On top of that, while the reports include the requests' results, they exclude the reasons for each result, which are important: Knowing why certain requests were denied might shed light on the legal process itself. It would potentially enable evaluating whether legal procedures surrounding the application are still functioning well, and specifically, whether they are sufficiently spotting rights-risking or -infringing uses. Hence, two additional criteria for sufficient control mechanisms are:

15) The control mechanism needs to include information *on the legal process itself*, rather than only on content and outcome. This information should be evaluated on a macro-level, by controlling whether the overall legal process can still guarantee a fundamental rights based application of RBIS.

16) To ensure maximum transparency to the public, the *reporting also needs to include qualitative information* on content and legal process, rather than only quantitative information.

With regards to *retaining* rights-infringing uses, as a reporting mechanism, it does not have any legally binding consequences. Additionally, since no quantitative threshold exists regarding RBIS use (e.g., defining everything above X amount of yearly usage as “too much”), the reports naturally do not have any consequence, no matter how high the number of reported uses. As argued in section III.1(e), such a numeric threshold is not desirable – a qualitative threshold is needed instead, which the reports do not include.

g) Risk Management System

A provision for all high-risk AI systems, the RMS tries to take into account all risks that may arise through the use of live and public RBIS, explicitly including risks for fundamental rights (Art 9(2) (a)). Additionally, it includes “risks that may emerge when the high-risk AI system is used in accordance with its intended purpose” (9(2)(b)), acknowledging rights-infringing risk dimensions beyond mere compliance. Also, the RMS is open-ended: As risks and their management measures are identified and evaluated iteratively, this mechanism has the potential to include risks for fundamental rights that were unforeseen in the beginning. As evaluated in the previous sections, all

of these are important criteria for a control mechanism to sufficiently spot a risk for rights arising from a strategic interpretative expansion. As law enforcement itself is to conduct the RMS, even the content of past RBIS cases could potentially be evaluated. Another positive point is that for eliminating or reducing risks, the “presumable context in which the system is intended to be used” shall be taken into consideration (Art 9(5)(c)). As has become clear in the theoretical section, the societal context (of illiberalism and autocratic legalism) is important for a strategic interpretative expansion. While the AIA does not specify further how the context should be factored into the evaluation, the following criterion can be deduced from it:

17) In addition to evaluating fundamental rights impact as well as legal process, the mechanism needs to evaluate the *societal context* wherein it will be used.²⁰⁸ This applies for controls on a case-by-case as well as on a systemic level.

On the other hand, the same shortcomings as evaluated under e) FRIA apply, namely, that law enforcement might not be sufficiently equipped to conduct a risk evaluation with regard to fundamental rights. Also, while Article 9 does not predefine the risks likely arising, it does mention that mitigation measures should be taken “as far as technically feasible through adequate design and development of the high-risk AI system” (Art 9(5)(a)). This points to a lens of analysis focused on risks arising from design and development of the technology, and not on abstract risks for fundamental rights that are not manageable through technical compliance. Taking this into account, it is less likely that the RMS will be able to detect the risk in question.

Regarding this mechanism’s ability to *retain* a rights-infringing use, the AIA stipulates that the risks identified and evaluated need to be eliminated or reduced “as far as technically feasible”. This is congruent with the risk-based approach of the Act: Where a risk cannot be eliminated, rather than just forbidding a use, it allows for a residual risk. This should be controlled through “adequate mitigation and control measures” (Art 9(5)(b)) – the AIA does not specify what measures would be adequate, or legal consequences in case a risk is not adequately mitigated. Most importantly, though, it does not stipulate any external control over the RMS, or the need for the RMS to be accessible to the general public. The result is a state where not only risk assessment (FRIA), but also the evaluation and mitigation of risks are left to the executive. Thus, this mechanism cannot adequately control the rights-risking or -infringing use in question.

²⁰⁸ While the evaluation of *societal context* and *legal process* might overlap, they are mentioned as two separate points here to underline their respective importance.

2. Evaluation of sufficiency of control mechanisms besides the AI Act and identification of further controlling criteria

Since the AIA provisions are supplementary to already existing frameworks such as the GDPR and national law, it serves to evaluate whether any established regulations provide relevant control mechanisms over law enforcement's use of live and public RBIS. Due to scope limitations, I will focus on the most relevant ones in this field: firstly, the Data Protection Impact Assessment, since this is a tool specifically designed for safeguarding the fundamental right of data protection. And as this thesis focuses on Germany, it will include an instrument that has recently been introduced as a national pilot project: the Overall Surveillance Account.

a) Data Protection Impact Assessment

The Data Protection Impact Assessment (DPIA) is regulated in Article 27 LED for all European law enforcement authorities, and is embedded in German national law in the BDSG (s 67), state data protection laws, PAGs, as well as the StPO.²⁰⁹

The DPIA needs to be exercised when a system is “likely to result in a high risk to the rights” of individuals (Art 27 LED), and assesses the procedure and purpose (the legal basis) of the data processing, the necessity and proportionality of this processing, the risks for the rights of affected persons, and the measures in place for securing against potential risks for data protection (s 67(4) BDSG). In this way, DPIAs help controllers to ensure “data protection by design”.²¹⁰ The DPIA thus controls whether a system's use is in line with fundamental rights. However, it only evaluates the impact on one specific right: the right to personal data protection,²¹¹ thereby using an even narrower lens of analysis than the FRIA (which assesses four fundamental rights).

As a holistic assessment, the DPIA is based on the principle of “comprehensive presentation”, acknowledging that a certain aspect of data processing can become important because of being embedded in a certain constellation²¹² - an important lens for spotting the rights-infringement in question. Also, the DPIA takes the legal process of a system's use into account (see criterion (15));

209 Pursuant to Art 288(3) Treaty on the Functioning of the European Union (TFEU), see Schindler (n 180).

210 European Data Protection Supervisor, ‘Data Protection Impact Assessment (DPIA)’ (*European Data Protection Supervisor*, 7 July 2025) <https://www.edps.europa.eu/data-protection-impact-assessment-dpia_en> accessed 8 July 2025.

211 As, for instance, defined in Charter of Fundamental Rights of the European Union art 8.

212 Dr Christoph Wambsganz, ‘Risikoanalyse und Datenschutz-Folgenabschätzung - Systematik, Anforderungen, Beispiele’ [2022] Der Bayerische Landesbeauftragte für den Datenschutz 8.

however, it still looks at “single points of risks” and accumulates them,²¹³ and does not consider the societal context wherein a system is used (see (17)). This is important: With a focus on “how secure” data is processed, the DPIA evaluates whether the technology used and the procedures in place are compliant.²¹⁴ It does not entail a risk scenario of data processed in a compliant fashion, but still posing a substantial risk for fundamental rights. In fact, unlike the AIA, the entire BDSG does not seem to address risks arising from compliant but substantially infringing data processing.²¹⁵ Like the FRIA, the DPIA is done *ex ante*. It can hence not integrate unforeseen risks that become apparent in the course of a system’s application (see (12)), and does not evaluate the content of concrete RBIS uses (see (6)). Lastly, the DPIA is not published, so public oversight is not possible (see (16)). The authority responsible for carrying out a DPIA is the controller himself, i.e., law enforcement, but section 67(3) BDSG stipulates that the DPA should be involved in its conduct. In this way, criterion 13, namely, that a strategic interpretative expansion can only be spotted when the controlling instance is equipped with a mandate and an knowledge of fundamental rights, is fulfilled. However, the BDSG does not specify how exactly and to what extent law enforcement should involve the DPA.

When it comes to not only spotting, but *retaining* the use in question, section 67(5) stipulates that law enforcement “shall carry out a review to determine whether the processing complies with the requirements resulting from the DPIA”. It does not stipulate that any other controlling entities, like the DPA, should be involved in this review. Hereby, law enforcement once more determines the sufficiency of its measures, incompatible with criterion 7, that the legally binding consequences need be enacted by an independent authority. Assuming bad faith, a possible scenario is that law enforcement involves the DPA to a minimal degree in the assessment itself, and without any further consultation, determines in its review that minimal measures taken by itself do indeed suffice. Hence, this control mechanism has no legally binding consequences (criterion (3)): not for a situation wherein the DPA notice that a system will probably not be compliant once in use, as the DPA are not involved in the DPIA review, and the BDSG stipulates no other legal consequences than this review. Also, the DPIA does not assess situations where a system might be formally compliant but still pose a risk for or infringe upon fundamental rights.

213 *ibid* 22.

214 *ibid* 10.

215 Evaluating this in-depth lies outside the scope of this thesis.

b) Overall Surveillance Account

The Overall Surveillance Account (*Überwachungsgesamtrechnung*, ÜGR) is a project to estimate the “overall surveillance burden” resulting from the multitude of surveillance powers of state authorities in Germany.²¹⁶ It is not anchored as a legal instrument in German law, but is based on the reception of a BVerfG judgment from 2010 on the instrument of data retention, wherein the BVerfG said that whenever the legislator considers introducing new surveillance methods, it has to take into account the various surveillance methods that already exist, and practice restraint.²¹⁷ Based on this, a legal discussion evolved about establishing an “overall surveillance account” that enables the legislator to know the total amount of already existing surveillance mechanisms. The first ÜGR was conducted as a pilot project in 2024/25 by the Max-Planck-Institut (MPI) on behalf of the Ministry of Justice and the Ministry of the Interior, and was published in January 2025.²¹⁸ It is based on data provided to the institute by German federal and state authorities for all surveillance activities of the reference year 2022; from intelligence agencies to law enforcement.²¹⁹ In total, the ÜGR includes 10.000 data records of 4.686 official authorization norms. These data records were collected, quantified, and evaluated based on empirical parameters developed by the MPI.²²⁰ The result is a prototype calculation that can be used again in future on a regular basis or ad hoc whenever the government considers introducing a new surveillance instrument. Similar to measuring degrees of freedom or the punitivity of a country, the ÜGR evaluates the intensity of a surveillance measure and quantifies it.²²¹ This number is multiplied by the frequency of use for each instrument, resulting in a surveillance index.

Although its name sounds promising – an aggregate surveillance account (see criterion (9)) – the ÜGR is unlikely to spot rights infringements of RBIS based on a strategic interpretative expansion. Firstly, it does not control against any fundamental rights baseline (see (1)). As it measures the intensity of an instrument, it might theoretically be able to capture the intensity of an impact on fundamental rights. But instead of using a fundamental rights baseline, it develops an arbitrary mean point, thereby falling prone to an anchoring bias: the cognitive bias that makes individuals

216 Ralf Poscher and others, ‘Überwachungsgesamtrechnung für Deutschland - Pilotstudie basierend auf der wissenschaftlichen Evaluation ausgewählter Überwachungsbefugnisse der Sicherheits- und Strafverfolgungsbehörden (ÜGR)’ (Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht 2025) 6.

217 *Vorratsdatenspeicherung* [2010] Bundesverfassungsgericht 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, BVerfGE 125, 260 (324); Poscher and others (n 216) 6.

218 Poscher and others (n 216).

219 However, many authorities refused to provide data for the ÜGR.

220 Poscher and others (n 216) 7.

221 *ibid* 20–21.

rely on the first piece of information given on a certain topic.²²² In this operationalization, the status quo becomes the “norm”, and everything further away from it is consequently “extreme” – which fails to consider the possibility that the status quo might already be “extreme”, for instance, extremely deviating from fundamental rights. Secondly, while evaluating the instruments’ quantity and intensity, it does not take into account the content of the measures – for instance, the legal bases for each use (see (6)). It also does not evaluate the legal process or the societal context in which it was embedded (see (15),(17)).

Positive aspects of this control mechanism are firstly that it is published, increasing public transparency and oversight (see (16)). Secondly, the ÜGR allows for systematic repetition by providing exact instructions as well as calculations for repetition (see (8),(12),(7)). The MPI itself recommends an evaluation on a regular basis – something that has yet to be installed. As the ÜGR was only a pilot study, it is unclear whether it will be repeated in future. Given that it was heavily criticized because of “constitutional concerns” at the conference of the Ministry of the Interior in 2024,²²³ it might not be institutionalized any time soon. Based on this, a last criterion for a control mechanism can be added:

18) The control mechanism needs to be *anchored in national law*.

Another positive aspect of the ÜGR is that this mechanism is exercised by a body independent of the executive (see (4)) equipped with a mandate and in-depth knowledge on fundamental rights (see (13)). However, as a body operating outside of government, the MPI does not have any powers to *retain* rights-infringing uses when spotted. Additionally, while it does contain a (quantitative) baseline, it does not contain any threshold: It does not define when the surveillance measured is “too much”. As has been clarified before, a numeric threshold is not useful; instead, a qualitative threshold is needed. Only with a qualitative threshold in place, concrete consequences can be taken when the overall surveillance becomes “too infringing upon fundamental rights” (see (10)). Without this, an ÜGR calculating even the most extensive index remains inconsequential.

222 Muzafer Sherif, Daniel Taub and Carl I Hovland, ‘Assimilation and Contrast Effects of Anchoring Stimuli on Judgments’ (1958) 55 Journal of Experimental Psychology 150, 150.

223 Ständige Konferenz der Innenminister und -senatoren der Länder, ‘Sammlung Der Zur Veröffentlichung Freigegebenen Beschlüsse Der 221. Sitzung Der Ständigen Konferenz Der Innenminister Und -Senatoren Der Länder Vom’ (Ständige Konferenz der Innenminister und -senatoren der Länder 19. bis 21.06.24) 62.

3. Conclusion

The evaluation of control mechanisms led to the identification of a number of criteria needed for mechanisms to sufficiently spot and retain a use of live and public RBIS that risks or infringes upon fundamental rights due to a strategic interpretative expansion. For the sake of completeness, Table 1 provides an overview of all control mechanisms tested against the deduced criteria (see page 59). Of course, it is neither necessary nor desirable for one single control mechanism to fulfill all criteria. Rather, a comprehensive framework needs to ensure that even though multiple authorities are responsible for different parts of the control, the criteria are sufficiently fulfilled: controlling the relevant points, at the relevant moments, for the relevant bodies.

In this respect, the existing framework has a number of shortcomings. Most notably, the majority of mechanisms *control only on technical and procedural compliance*. Only two mechanisms, namely FRIA and RMS, include risks to fundamental rights. However, in their operationalization, both again fall back on criteria centered around compliance, except the risk mitigation for “democracy and societal wellbeing” in the FRIA, which is not defined any further. A related shortcoming is that the AIA does not stipulate *concrete consequences for “compliant but rights-infringing uses”* (which seems to also apply to the BDSG, at least with regards to the DPIA). While the Act stipulates concrete powers for MSA and DPA to take action against non-compliant uses, the authorities’ powers to retain compliant but infringing uses are limited to ordering the deployer to take “appropriate measures”, which are not specified and do not mention a ban. Both DSA and MSA are mainly tasked with compliance (of law enforcement’s RBIS use with national law, and of national law with the AIA).²²⁴ Additionally, in Germany, the DPAs’ power over law enforcement is limited to accessing information and issuing complaints. This considerably lowers the overall capability of the DPA to exercise meaningful control over the use of surveillance instruments by law enforcement. Another important point is that precisely the two measures that do include a fundamental rights dimension are *enacted and controlled by law enforcement itself*, which is, as established, not sufficiently resourced with regard to fundamental rights. Also, assuming bad faith, the executive needs to be controlled by an independent body, especially when evaluating and mitigating potential impacts on fundamental rights. The general AIA’s approach of leaving a significant amount of responsibility for their system to the respective deployers is not appropriate when it comes to potential fundamental rights infringements. This is particularly the case for infringements through covert operations by law enforcement, against which subjects usually cannot defend themselves

²²⁴ The same applies to the AI Office (Art 64), the AI Board (Art 65), and the Scientific Panel of Independent Experts (Art 68), see Hahn (n 153).

(and additionally, authorization as the mechanism to counterbalance this might again be conducted by a branch of the executive). The AIA's general exception clause on "national security" further reduces effective oversight on risks for fundamental rights.

Control mechanism		a) Authorization	b) Notification	c) Disclosure	d) Evaluation	e) FRIA	f) Annual reports	g) RMS	h) DPIA	i) ÜGR
Legal basis		Art 5(3) AIA	Art 5(4) AIA	Art 26(10) AIA	Art 79(2) AIA	Art 27 AIA	Arts 5(6), 5(7) AIA	Art 9 AIA	Art 27 LED; § 67 BDSG	BVerfGE 125, 260 (324)
Responsible authority		Judiciary/ independent administrative authority	DPA/MSA	DPA/MSA	MSA	LE (potentially: MSA)	DPA/MSA, Commission	LE	LE, DPA	MPI
#	Controlling criteria									
1	Control against fundamental rights baseline	X Controls only procedural compliance	X	X	X Controls only procedural and technological compliance	✓	X	✓	X Controls only procedural and technological compliance	X
2	Impact Control (on individual and societal level)	X	X	X	X Controls only procedural and technological compliance	≈ Only assesses prior to use, real impact can not be controlled	X	≈ Depends on operationalization by law enforcement	≈ Only assesses prior to use, real impact can not be controlled	X
3	Legally binding consequences	✓	≈ Vague consequences for compliant but rights-infringing AI	≈ Vague consequences for compliant but rights-infringing AI	≈ Vague consequences for compliant but rights-infringing AI	X “National security” as general exception clause	X	X	X LE itself is to review sufficiency	X
4	Independence	≈ Potentially enacted by “independent admin authority”	✓	✓	✓	≈ Only when FRIA is handed to MSA	n/a	X	X	✓
5	Resource sufficiency	X	≈ MSA yes, DPA less so	≈ MSA yes, DPA less so	≈ MSA yes, DPA less so	X	≈ MSA yes, DPA less so	✓	≈ DPA less so	✓
6	Content control	✓	X	✓	✓	X	X	✓	X	X
7	Specificity of procedures	✓	X	✓	X	X	✓	X	X	✓
8	Systematic control	✓	✓	X	X	✓	✓	✓	X	X
9	Aggregate control	✓	✓	X	X	X	✓	✓	X	✓
10	Specificity of consequences	X	X	X	X	X	n/a	X	X	X
11	Open-ended control	n/a	n/a	n/a	✓	X	n/a	✓	X	n/a
12	Repeated control	✓	✓	X	X	X	✓	✓	X	X
13	Fundamental-rights mandate and resources	X Potentially enacted by “independent admin authority”	≈ DPA equipped for one specific right; MSA less so	≈ DPA equipped for one specific right; MSA less so	≈ DPA equipped for one specific right; MSA less so	X	≈ DPA equipped for one specific right; MSA less so	X	≈ DPA yes, LE no	✓
14	No exception for national security	✓	✓	✓	✓	X	✓	✓	✓	n/a
15	Control over legal procedure	n/a	X	✓	✓	n/a	X	X	✓	X
16	Public transparency over content and procedure	X	X	X	X	X	X	X	X	✓
17	Control over societal context	X	n/a	n/a	X	X	n/a	✓	X	X
18	Legal anchoring	✓	✓	✓	✓	✓	✓	✓	✓	X

Table 1: Evaluation of control mechanisms with regards to deducted sufficiency criteria

V. Recommendations

As has become clear from the conclusion, the AIA's mechanisms mainly control on technical and procedural compliance. This fulfills important functions: It can, for instance, limit common risks associated with RBIS to a certain degree. The risks of accuracy, bias and function creep introduced in section II.5 can be reduced by a robust control over technological compliance. Function creep can furthermore be reduced by strict procedural compliance. When it comes to spread and secrecy, and a chilling effect as their result, as these are characteristics inherent to the nature of surveillance, they can never be fully avoided. However, through strict checks on content and procedure of RBIS use – for instance, strict scope limitations to confine its spread, strong authorization procedures to balance infringements caused by secrecy, and maximum transparency over its use to counter the chilling effect – they can be reduced to a certain extent.

What's missing in the AIA's controls is a *substantial fundamental rights control* on a case-by-case as well as on a systemic level (see criteria (1) and (2)). The evaluation has pointed to a number of criteria needed for sufficient control mechanisms. Based on them, this section recommends a multiplicity of improvements. These recommendations form part of liberal constitutionalism (or preventive militant rule of law) as described by Sajó and Scheppele,²²⁵ and are congruent with the previous CJEU rulings on the interpretation of EU law in light of fundamental rights.²²⁶

At this point, it is important to mention that the most efficient and appropriate control over live and public RBIS would be a ban. Its use is one step further in a process of normalizing surveillance,²²⁷ and in the long run might lead to a loss of anonymity, severe chilling effects, and infringements on fundamental rights, especially in the context of rising illiberalism. A full ban is also the stance of the European Parliament, the European Data Protection Board, and the European Data Protection Supervisor as well as many civil society actors.²²⁸ However, should Germany decide to legalize its use for law enforcement, it needs to ensure that it is controlled sufficiently.

225 Kim L Scheppele, 'Autocratic Legalism' (2018) 85/2 The University of Chicago Law Review 545, 558; András Sajó, 'Militant Rule of Law' (*Verfassungsblog*, 20 December 2023) <<https://verfassungsblog.de/militant-rule-of-law/>> accessed 9 May 2025.

226 CJEU Research and Documentation Directorate, 'Field of Application of the Charter of Fundamental Rights of the European Union' (2021) 1 <https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-05/fiche_thematique_-_charte_-_en.pdf> accessed 14 July 2025.

227 International Working Group on Data Protection in Technology, 'Working Paper on Facial Recognition Technology' (International Working Group on Data Protection in Technology 2022) 14 <https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20230608_WP-Facial-Recognition-Tech-EN.pdf?__blob=publicationFile&v=2> accessed 2 July 2025.

228 *ibid* 28; Vieth-Ditlmann and Sombetzki (n 155) 7; Fetic (n 171) 11.

1. Comprehensive RBIS Control Framework

The AIA explicitly states that member states may introduce, in accordance with Union law, more restrictive laws and additional control mechanisms with regard to live and public RBIS (Art 5(5)), and the BfDI calls on the German government to make use of this clause.²²⁹ Hence, in the case that Germany legalizes it, I am recommending a Comprehensive RBIS Control Framework to be integrated into the new German AI Act implementation bill that is finalized this year (in part one, the KIMÜG), as well as in additional national law. Since the control mechanisms should be specific rather than vague to avoid the executive's use of legal loopholes (see criterion (7)), responsibilities and procedures will be defined as detailed as possible. This framework also serves as a “double proportionality test” similar to the suggestion by Roßnagel²³⁰ based on the 2010 BVerfG judgment: I argue that the proportionality of each surveillance use and instrument needs to be judged not only in the context of the total amount of surveillance instruments already in use, but also in a fundamental rights context.

This alignment with fundamental rights (see (1)) can be evaluated best by integrating the context, process, and impact of RBIS use into the evaluation: Including the *societal context* (see (17)) acknowledges the connection of law and power; specifically, that in times of illiberalism, the positivist notion of basing the legitimacy of law on the legitimacy of functioning democratic institutions is no longer appropriate. The framework controls will evaluate whether the context can still guarantee an RBIS use in line with fundamental rights. Secondly, the theory has shown that especially the executive needs to be thoroughly controlled. Therefore, an evaluation also controls the *legal process* on a macro level (see (15)), evaluating whether the overall legal process surrounding RBIS use is still in line with fundamental rights (also evaluating each use's *content*). Lastly, the potential and actual *impact* (see (2)) needs to be evaluated - for each RBIS use, and on society as a whole. As a strategic interpretative expansion is only one of the many tactics used to hollow out democracy, fundamental rights infringements can have many reasons. Taking into account all the aforementioned factors increases the ability to analyze the cause and effect of rights infringements and attribute an infringement to a strategic interpretative expansion. However,

229 Falk Steiner, “‘Flächenbrand für Bürgerrechte’: Liberale kritisieren KI-Verordnung scharf’ *Heise online* (24 January 2024) <<https://www.heise.de/news/Flaechenbrand-fuer-Buergerrechte-Liberale-kritisieren-KI-Verordnung-scharf-9606490.html>> accessed 16 April 2025.

230 Wissenschaftliche Dienste, ‘Datenbank-Analysen Durch Die Polizei Grundrechte Und Datenschutzrecht’ (Deutscher Bundestag 2020) Ausarbeitung WD 3-3000-018/20 15 <<https://www.bundestag.de/resource/blob/695986/a6f049f44b45eca273cefd410c78c534/WD-3-018-20-pdf.pdf>> accessed 2 July 2025.

spotting the expansion itself is secondary; the alignment with fundamental rights is the important lens of analysis.

Additionally, establishing this framework acknowledges that individual contestation, either by natural persons or civil society actors, can not suffice against rights-infringing uses. While such contestation might be carried out by independent bodies with knowledge of and a mandate on fundamental rights, in practice, they often lack the resources needed (including access to law enforcement's documentation). Also, by its nature, contestation happens ad hoc and after the fact, when an unjust situation has already materialized, and always concerns either a single case or multiple single cases. A sufficient control needs to assess a system already prior to its use, and needs to be exercised in a comprehensive way, firmly anchored in national law (see (18)).

a) National competent authorities

Based on the criteria of independence (4), resource sufficiency (5), fundamental rights resources and mandate (13) for controlling authorities, as well as a mechanism's legal anchoring (18), the following will be suggested: As per Article 74(8) AIA, the appointed MSA for supervising the use of RBIS by law enforcement should be the BfDI. Because its main function is the protection of fundamental rights (of data protection and freedom of information), it is a partial and critical actor whose purpose is to control other branches of the executive. Its independence is constitutionally guaranteed by the CFR to "effectively exercise [its] supervisory function, particularly vis-à-vis the executive".²³¹ Installing the BfDI as MSA is also congruent with the CJEU judgment on data retention, which clarifies that the authority monitoring law enforcement needs to be completely independent.²³² Appointing the BfDI would also alleviate shortcomings in its effecting powers over law enforcement set in the BDSG (where the BfDI can only access information and issue complaints). The alternative body, UKIM, even if no longer dependent on instructions from the BNetzA, does not have a sufficient mandate regarding fundamental rights. The BNetzA can still act as a central point of contact and forward relevant complaints to the BfDI.

However, if the German government moves forward with a new KIMÜG similar to the previous one, the recommendation is to add a clause on equal joint supervision by BfDI and UKIM over the Comprehensive RBIS Control. This would be congruent with the AIA, since Article 79(2) stipulates that the MSA needs to fully cooperate with the national DPA (being the appointed FRPA) when risks for fundamental rights are at stake. The KIMÜG (and an additional clause in the BDSG) could

²³¹ Charter of Fundamental Rights of the European Union art 8.

²³² C-178/22 [2024] Court of Justice of the European Union C-178/22.

simply specify how exactly the UKIM needs to cooperate with the BfDI in this case, specifically when they do not agree in a matter concerning fundamental rights.

Importantly, even the BfDI's fundamental rights mandate and resources are so far limited to guaranteeing data protection and freedom of information. Therefore, the BfDI should be supported by an "RBIS Control Working Group", consisting of experts in the field of fundamental rights and surveillance, particularly scholars, civil society representatives, and LfDs. This is again congruent with Article 5(5) allowing for additional specifications in national law. To gain a holistic understanding of the interplay of RBIS and fundamental rights, the working group needs to include input and feedback from affected individuals, such as activists particularly prone to surveillance measures, or individuals who have been subjected to such measures in the past. The Working Group needs to be equipped with sufficient resources, including dedicated staff only working on monitoring and evaluating RBIS use in relation to fundamental rights.

Additionally, regarding the mechanism of authorization, the StPO should appoint a judicial body to exercise this control to sufficiently preserve the division of state powers. The StPO should also add provisions to make this mechanism meaningful in practice, thereby ensuring that the authorizing instance refrains from a copy-and-paste practice.²³³

b) Tasks

i) Operationalization

The first task of the Working Group, supervised by the BfDI (/UKIM), is the operationalization of factors to be measured for guaranteeing an RBIS use in line with fundamental rights. Qualitative indicators and thresholds for conditions (of the societal context and legal process) to ensure an RBIS application in line with fundamental rights need to be established; similar to the Freedom Index.²³⁴ The impact on fundamental rights needs to be operationalized on a case-by-case and on a systemic level, to enable a competent assessment by authorizing judges as well as BfDI(/UKIM) controlling each use (specified in the following sections). Secondly, on a macro-level, an operationalization serves to control whether the overall impact of RBIS use on society is in line with fundamental rights (similar to, but more specific than the category of "societal wellbeing" in the FRIA template). By operationalizing and measuring this process from beginning to end,

²³³ A demand already formulated by other scholars, see e.g., Hüls (n 186) 70. Detailing such provisions lies beyond the scope of this paper.

²³⁴ 'Freedom Index by Country 2025' (*World Population Review*) <<https://worldpopulationreview.com/country-rankings/freedom-index-by-country>> accessed 4 August 2025.

fundamental rights adherence is controlled in an embedded way. This also prevents the ripple effect of a shifted baseline, where an infringing RBIS use results in a change of context that allows for even more infringing uses. By establishing a qualitative threshold, the Working Group specifies where the AIA remains too vague, i.e., *at what point exactly* an AI System is formally compliant, but still too risky for, or infringing upon fundamental rights.

ii) Initial Assessment

The initial assessment performed by the Working Group is similar to the FRIA. However, it cannot replace the FRIA conducted by law enforcement, as this would overturn EU law. The assessment should be based on the operationalization above, thereby significantly deviating from the ALIGNER-template. It assesses the current societal context and the legal process, current uses of RBIS as introduced in section III.3(a), as well as their current individual and overall impact, all with regard to fundamental rights. This assessment can already lead to a risk perceived (as stipulated in Art 79(2)), which automatically leads to its testing and evaluation (see next section (iii)).

iii) Continuous Testing and Evaluation

The control on fundamental rights risks and infringements needs to be performed systematically, repeatedly, including all cases, and should be open-ended (see criteria (8),(12),(9),(11)). Article 77(3) states that the MSA will organize testing of a system when a risk is perceived “with the close involvement of the requesting public authority or body”. The KIMÜG should specify this close involvement as the involvement by the Working Group performing the testing and evaluation, instructed by BfDI (/UKIM). Based on the reasonable assumption of a *continuous* risk to fundamental rights by the BfDI, this testing should be performed systematically and repeatedly, including all RBIS uses, rather than only ad hoc. Besides a technical test, it should also include a continuous evaluation of context, process, and impact of RBIS based on the operationalization under (i).

The evaluation also needs to include each case’s content (see (6)). Therefore, national law (amending StPO and BDSG) needs to stipulate that the notification to the DPA (discussed in section III.2(c)(i)) also includes a notification on the content of each RBIS request. As long as sensitive operational data remains excluded, this is not in conflict with EU law, as it only expands the requirement to notify on request and result set in AIA Article 5(4). Alternatively, this could also be

legally based on the Act's requirements concerning the disclosure of documentation (Art 26(10), see section III.2(c)(ii)). Here, the Act stipulates documentation to be made available "upon request". The BDSG could specify that BfDI automatically issues a request for each RBIS use, again based on the assumption of a continuous risk to fundamental rights.

iv) Consequences for RBIS uses that pose a risk to or infringe upon fundamental rights

For the case that an evaluation leads to attesting "formal non-compliance", the Act has sufficient legal consequences in place, up to fining and banning deployers (Arts 79(2); 83). But there is a regulatory gap for compliant but rights-risking or -infringing RBIS uses, as Article 82 only stipulates "appropriate measures" to be taken as "corrective action" by law enforcement. Trusting executive bodies with appropriately mitigating their remaining risks, as is also the case in the RMS, goes against the assumption of bad faith. The KIMÜG (and the BDSG for expanding the BfDI's powers) needs to specify what those measures would entail, from corrective action to concrete, legally binding consequences when the corrective action does not suffice (congruent with criteria (3) and (10)).

Based on operationalization (ii) and testing/evaluation (iii), if a qualitative threshold for fundamental rights is still exceeded after corrective measures are taken, the MSA can on a case-by-case level decide to stop the use of a system. While this appears to be in conflict with the judge's authorization given before, the BfDI (/UKIM) would simply enforce fundamental rights compliance. Rather than conflicting criminal procedure law, this creates a dual authorization requirement (adherence to criminal procedure *and* to fundamental rights). On a macro-level, the MSA can also decide to ban a system entirely. This is congruent with Article 79(2) that requires law enforcement to cooperate with the MSA in cases of fundamental rights risks, and with Recital 157 that tasks member states to set up "a specific safeguard procedure [...] for ensuring adequate and timely enforcement against AI systems presenting a risk to [...] fundamental rights".

v) Reporting

The KIMÜG should require that the content, procedure and result of all tasks of the Working Group are reported by the BfDI to the public regularly to enable public scrutiny via maximum transparency (see (16)). This requirement only expands the annual reporting defined in Article 5(6),

extending its content beyond reporting only quantitative information (operational data remains excluded), and extending its addressee to not only be the EC, but the general public as well. Additionally, the KIMÜG should require reporting to be conducted on a basis more frequent than annually, to ensure timely public scrutiny - as opposed to reporting a year after the fact, when a ripple effect might already have caused infringing conditions to have normalized.

vi) Training

The KIMÜG should task the Working Group, supervised by BfDI(/UKIM), to train relevant authorities on the interplay of RBIS use and fundamental rights, for instance, raising awareness on mechanisms like a strategic interpretative expansion. This includes training for law enforcement, which is anyways among the responsibilities of the BfDI (see s 14 BDSG), and the AIA requirement that deployers need to be trained on the risks of their system and the specific context wherein it will be used (as provision for RMS, Art 9(5)(c) AIA).

vii) Cooperation with law enforcement

A number of recommendations concern the FRIA. Per AIA, it needs to be handed to the MSA. In case this position is filled by the UKIM, the KIMÜG should explicitly require the UKIM to share it with the BfDI as part of their joint supervision. The FRIA should also be controlled without exceptions for national security (see (14)). Since member states do not need to make use of this exception clause, the KIMÜG should stipulate a waiving of the clause in this regard. While the FRIA template has already been designed by ALIGNER, this is only done to “facilitate deployers in complying with their obligations” (Art 27(5)); hence, Germany can decide to implement its own FRIA as long as the criteria outlined in Article 27(1) are included. The KIMÜG should instruct the Working Group to design this template based on their operationalization. Additionally, the assessment itself, while primarily executed by law enforcement, will be supported by the Working Group, addressing previous criticisms.²³⁵

Regarding the RMS for RBIS, the KIMÜG should require this to be supervised by the BfDI(/UKIM), including supervising the “adequate mitigation and control measures” defined by law enforcement (Art 9(5)(b);(d)). This is not in conflict with the AIA, since Article 9 does not preclude additional supervision. Like for the FRIA, the RMS categories of risks for fundamental

²³⁵ Giannini and Tas (n 201).

rights should be based on the Working Group's operationalization, since law enforcement does not have the necessary knowledge thereof. The Working Group should also be required to assist law enforcement in the conduction of the RMS with regard to fundamental rights. Next to that, the KIMÜG should predefine a temporal aspect on how often the RMS needs to be reiterated, to avoid any potential legal loophole that law enforcement might use in its favor.

Furthermore, as part of the Comprehensive RBIS Control Framework, the KIMÜG (and potentially, an amendment of the BDSG) could task the Working Group to assist law enforcement in conducting its DPIAs for RBIS. The BDSG anyway requires the BfDI to be involved in the DPIA (see s 67(3)), but does not specify the extent and form of this involvement. KIMÜG and BDSG could stipulate that the BfDI tasks its subordinate Working Group with assisting in the operationalization of additional risks for data protection caused by RBIS that lie beyond formal compliance, and that the BfDI should also be involved in the review conducted by the controller (see s 67(5)). The DPIAs for RBIS use by law enforcement should be conducted in regular intervals to allow for a continuous assessment of data protection embedded in a changing societal context.

Finally, the KIMÜG should require the FRIA and RMS for RBIS to be published, to increase transparency and control, and a corresponding amendment to the BDSG should require the publication of DPIAs.

2. Additional recommendations

Some last recommendations concern the ÜGR, and hence lie outside of the scope of the KIMÜG. As evaluated, the pilot project of the MPI is a necessary but insufficient mechanism for reporting on surveillance mechanisms, specifically with regard to fundamental rights infringements based on a strategic interpretative expansion. To spot such phenomena, the ÜGR would need to tie its baseline to fundamental rights instead of anchoring it to an arbitrary mean value based on the current status quo. Through the development of such a baseline, similar to the operationalization in the RBIS Control Framework, it would be possible to develop qualitative thresholds to enable spotting and reporting when the overall use of a surveillance instrument is no longer in line with fundamental rights. Secondly, the ÜGR should in future include reporting on the content of all surveillance requests, to notice patterns or changes in this regard. In a further step, the ÜGR could also report on the overall impact on fundamental rights by the use of surveillance instruments, and potentially include a report on the evolving societal conditions, including the legal process, wherein they are

applied. In this way, the ÜGR would serve as a proper “proportionality test”²³⁶, setting the use of surveillance instruments in proportion qualitatively. When conducted this way, elements of the RBIS Control Framework could inform the ÜGR sections on live and public RBIS. Potentially, the operationalization of the RBIS framework could even provide the basis for a similar operationalization of a future ÜGR, enabling a comprehensive control of all surveillance instruments used in Germany. Lastly, to report on overall surveillance in the long run, the ÜGR needs to be anchored as a legal instrument in German law.

VI. Discussion

This thesis aims to show that guaranteeing fundamental rights when using intrusive surveillance instruments like RBIS is only possible through an expansion of controls beyond technical and procedural compliance,²³⁷ to a fundamental rights oriented framework as part of liberal constitutionalism (or preventive militant rule of law). If this is ignored by the government, it is not only possible but likely that RBIS’ legal bases will be strategically expanded in a way that is beneficial to the illiberal forces on the rise in Germany. This will not only affect the example case’s unwitting climate activist, but anyone considered undesirable for their agenda. Political activists, migrants, queers, people of color, homeless, poor, disabled people – anyone considered either querulous or superfluous will be among the first to notice these subtle but nevertheless effective changes.

However, the evaluation and recommendations of this thesis are only a first step in applying the abstract concept of “liberal constitutionalism” to practice. If one were to proceed with the thoughts formulated here, several points need additional consideration.

Firstly, the formulated recommendations grant significant controlling power to the DPA. But especially in a scenario of autocratic legalism, power distribution needs to be examined critically. Therefore, due consideration needs to be given to potential avenues for co-opting the DPA; the flipping of the Hungarian DPA serves as a cautionary tale in this regard.²³⁸ Potential avenues for this

236 Wissenschaftliche Dienste (n 230) 15.

237 These are, of course, still important. Investigating additional improvements in this regard is also needed, for instance, improving requirements for technical robustness, such as considering the adoption of standards for biometric protection such as the ISO/IEC 24745:2022⁶⁸ and the use of renewable and revocable biometric references, as well as privacy preserving biometric systems – see International Working Group on Data Protection in Technology (n 227) 36.

238 Friedl and Rolfes (n 169).

might be the replacement of commissioners, changing their appointment process, or attacking their budgetary independence.²³⁹

A second point in need of further development is the concrete case of disagreement between MSA and DPA/FRPA, should they be separate bodies practicing joint supervision (BfDI/UKIM). An implementation bill would ideally include an additional provision that, in case of disagreement on whether and to what extent an RBIS use causes an infringement upon fundamental rights, the FRPAs' assessment is prioritized over the MSA's, enabling the FPRA to instruct the MSA to follow up on it (for instance, with a ban) – but this might not be compatible with the AIA's provisions. Here, an effective procedure that does not infringe upon EU law would need to be developed. Another note concerns the scope of recommendations: The Comprehensive RBIS Control Framework is, for now, a framework that controls the alignment with fundamental rights specifically for the legal application of RBIS. However, as indicated under the recommendations for the ÜGR, it might be valuable to develop a similar comprehensive framework for all other surveillance mechanisms (and their combined impact). Lastly, the thesis was concerned specifically with the threat arising for fundamental rights by a strategic interpretative expansion of legal bases, showing that impacts on these rights might occur even in a state of full legal compliance. But this is only one of the many avenues that autocratic legalists take. In times of illiberalism, every single potential avenue these forces might take needs to be carefully evaluated - to ensure fundamental rights, and with it, to safeguard democracy.

239 *ibid.*

Bibliography

- AlgorithmWatch and others, 'Offener Brief: Menschenrechte Schützen – Biometrische Fernidentifizierung Verboten' (März 2024)
<<https://www.amnesty.de/sites/default/files/2024-03/Gemeinsamer-Offener-Brief-Biometrische-Ueberwachung-Maerz-2024.pdf>> accessed 16 April 2025
- ALIGNER, 'About Aligner' (*ALIGNER H2020*) <<https://aligner-h2020.eu/about/>> accessed 7 July 2025
- , 'ALIGNER - Towards a More Secure Europe'
<https://aligner-h2020.eu/wp-content/uploads/ALIGNER_Flyer_AFRIA.pdf> accessed 7 July 2025
- Alston P and Weiler J, 'An "Ever Closer Union" in Need of a Human Rights Policy: The European Union and Human Rights' (1998) 9 *European Journal of International Law* 658
- Amnesty International, 'Deutschland: Paragraf-129-Anklage gegen Letzte Generation verschärft Kriminalisierung von Protest' (*Amnesty International*, Mai 2024)
<<https://www.amnesty.de/pressemitteilung/deutschland-paragraf-129-anklage-gegen-letzte-generation-kriminalisierung-protest>> accessed 24 June 2025
- Amnesty International and AlgorithmWatch, 'Offener Brief an Die Bundesminister Marco Buschmann Und Robert Habeck'
<https://algorithmwatch.org/de/wp-content/uploads/2023/09/Offener-Brief_28.09.23.pdf> accessed 16 April 2025
- Bély L, *Louis XIV : Le plus Grand Roi Du Monde* (Éditions Jean-paul Gisserot 2005)
- Berberoglu B, *The Global Rise of Authoritarianism in the 21st Century: Crisis of Neoliberal Globalization and the Nationalist Response* (Routledge 2020)
- BfDI, 'Aufgaben Und Befugnisse Der BfDI' (*Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) <<https://www.bfdi.bund.de/DE/BfDI/Inhalte/BfDI/AufgabenBFDI.html>> accessed 12 July 2025
- , 'Landesbehörden' (*Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*)
<<https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html>> accessed 2 July 2025
- , 'Technische Anwendungen - Die KI-Verordnung Der EU' (*Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*)
<<https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/KI-Verordnung.html>> accessed 23 September 2024
- Biselli A, 'Letzte Generation: Der fossile Rechtsstaat rast gegen die Wand' *netzpolitik.org* (25 May 2023) <<https://netzpolitik.org/2023/letzte-generation-der-fossile-rechtsstaat-rast-gegen-die-wand/>> accessed 24 June 2025
- , 'Telekommunikationsüberwachung: Polizei soll monatelang die Letzte Generation abgehört haben' (*netzpolitik.org*, 23 June 2023)

<<https://netzpolitik.org/2023/telekommunikationsueberwachung-polizei-soll-monatelang-die-letzte-generation-abgehört-haben/>> accessed 29 May 2025

BKA, 'Erkennungsdienst' (*Bundeskriminalamt*)

<<https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Erkennungsdienst/erkennungsdienst.html>> accessed 18 June 2025

——, 'Foto-Fahndung' (*Bundeskriminalamt*)

<https://www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsprojekteUndErgebnisse/Foto-Fahndung/foto-fahndung_node.html> accessed 7 July 2025

——, 'Gesichtserkennung' (*Bundeskriminalamt*) <<https://perma.cc/NZ3K-B555>> accessed 19 April 2025

'BKA - Our Mandate'

<https://www.bka.de/EN/TheBKA/OurLegalMandate/ourmandate_node.html> accessed 4 July 2025

Bledsoe WW, *A Facial Recognition Project Report* (King Hurley Research Group 1093)

Bock D and Mischke B, 'Die „Letzte Generation“ Als Kriminelle Vereinigung?' [2024] *Zeitschrift der Gewerkschaft der Kriminalpolizei*

<<https://www.kriminalpolizei.de/ausgaben/2024/maerz/detailansicht-maerz/artikel/die-letzte-generation-als-kriminelle-vereinigung.html>> accessed 24 June 2025

Buchmann A and Kugelmann D, 'Big Brother Is Analyzing You' (*Verfassungsblog*, 11 December 2024) <<https://verfassungsblog.de/big-brother-is-analyzing-you/>> accessed 7 July 2025

Bundeskriminalamt, '„Letzte Generation“ Lagebild -Fortschreibung Nr. 2' (Bundeskriminalamt 2024) Ausarbeitung

Bundesnetzagentur, 'KI Service Desk' (*Bundesnetzagentur*)

<https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/start_ki.html> accessed 4 August 2025

——, 'Marktüberwachung' (*Bundesnetzagentur*)

<https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/14_Marktueberwachung/start.html> accessed 4 August 2025

Bundespolizei, 'Teilprojekt 1 „Biometrische Gesichtserkennung" Des Bundespolizeipräsidiums Am Bahnhof Berlin Südkreuz Im Zeitraum Vom 01.08.2017 - 31.07.2018' (2018) Abschlussbericht <https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf?__blob=publicationFile> accessed 19 April 2025

Buolamwini J and Gebru T, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification'

Busche L, 'Kommunistenverfolgung in der alten Bundesrepublik'

<<https://www.bpb.de/themen/deutschlandarchiv/225517/kommunistenverfolgung-in-der-alten-bundesrepublik/>> accessed 22 July 2025

Casaburo D and Marsh I, ‘How to Use the ALIGNER Fundamental Rights Impact Assessment Template’ <https://aligner-h2020.eu/wp-content/uploads/ALIGNER_How-To-Use-FRIA.pdf> accessed 7 July 2025

CDU, CSU and SPD, ‘Verantwortung für Deutschland – Koalitionsvertrag zwischen CDU, CSU und SPD - 21. Legislaturperiode’ Koalitionsvertrag

CJEU Research and Documentation Directorate, ‘Field of Application of the Charter of Fundamental Rights of the European Union’ (2021)
<https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-05/fiche_thematique_-_charte_-_en.pdf> accessed 14 July 2025

‘Clearview AI | Facial Recognition’ (*Clearview AI*) <<https://www.clearview.ai>> accessed 13 August 2025

Datenschutzkonferenz (DSK), ‘Orientierungshilfe Der Konferenz Der Unabhängigen Datenschutzaufsichtsbehörden Des Bundes Und Der Länder Vom 6. Mai 2024’ (Datenschutzkonferenz (DSK) 2024) Orientierungshilfe <https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf> accessed 2 July 2025

Demircan M, Waem H and Dauzier J, ‘Fundamental Rights Impact Assessments under the EU AI Act: Who, What and How?’ (*Technology’s Legal Edge*, 7 March 2024)
<<https://www.technologyslegaledge.com/2024/03/fundamental-rights-impact-assessments-under-the-eu-ai-act-who-what-and-how/>> accessed 7 July 2025

Deutscher Anwaltverein, ‘PM 06/23: Biometrische Fernidentifizierung verbieten – in Echtzeit und nachträglich!’ (*Deutscher Anwaltverein*, 16 February 2023)
<<https://anwaltverein.de/de/newsroom/pm-06-23-biometrische-fernidentifizierung-verbieten-in-echtzeit-und-nachtraeglich>> accessed 16 April 2025

Deutscher Bundestag, ‘Nationale Aufsicht bei Künstlicher Intelligenz komplex’ (*Deutscher Bundestag, Parlamentsnachrichten*, 16 May 2024)
<<https://www.bundestag.de/presse/hib/kurzmeldungen-1003008>> accessed 4 July 2025

——, ‘Nationale Umsetzung des AI Act in Deutschland’ (*Deutscher Bundestag*, 9 June 2024)
<<https://www.bundestag.de/presse/hib/kurzmeldungen-1016762>> accessed 15 April 2025

‘Drucksache 20/5781 - Antwort Der Bundesregierung Auf Die Kleine Anfrage Der Abgeordneten Andrej Hunko, Žaklin Nastić, Victor Perli Und Der Fraktion DIE LINKE.’ (Deutscher Bundestag)
<<https://dserver.bundestag.de/btd/20/057/2005781.pdf>> accessed 19 April 2025

‘Drucksache 20/7864 - Antwort Der Bundesregierung Auf Die Kleine Anfrage Der Abgeordneten Martina Renner, Nicole Gohlke, Gökay Akbulut, Weiterer Abgeordneter Und Der Fraktion DIE LINKE.’ (Deutscher Bundestag) <<https://dserver.bundestag.de/btd/20/078/2007864.pdf>> accessed 19 April 2025

‘Drucksache 20/12948 - Antwort Der Bundesregierung Auf Die Kleine Anfrage Der Fraktion Der CDU/CSU – Drucksache 20/12671 Nationale Umsetzung Des AI Act in Deutschland’ (Deutscher Bundestag 2024) <<https://dserver.bundestag.de/btd/20/129/2012948.pdf>> accessed 15 April 2025

Dworkin R, *Law’s Empire* (Belknap Press of Harvard University Press 1997)

Eckstein K and Girschick P, 'Biometrische Überwachung - ja, nein, vielleicht?' *Tagesschau* (20 February 2023) <<https://www.tagesschau.de/inland/innenpolitik/ki-verordnung-101.html>> accessed 1 July 2025

EDRi, 'Remote Biometric Identification: A Technical & Legal Guide' (*European Digital Rights (EDRi)*, 23 January 2023) <<https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/>> accessed 23 June 2025

European Commission, 'Ethics Guidelines for Trustworthy AI | Shaping Europe's Digital Future' (*digital-strategy.ec.europa.eu*, 8 April 2019) <<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>> accessed 7 July 2025

——, 'Governance and Enforcement of the AI Act' (*European Commission*) <<https://digital-strategy.ec.europa.eu/en/policies/ai-act-governance-and-enforcement>> accessed 10 July 2025

European Data Protection Supervisor, 'Data Protection Impact Assessment (DPIA)' (*European Data Protection Supervisor*, 7 July 2025) <https://www.edps.europa.eu/data-protection-impact-assessment-dpia_en> accessed 8 July 2025

European Parliament, '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)' (European Parliament) Amendments P9_TA(2023)0236

'Face Recognition Technology (FERET) | NIST' <<https://perma.cc/3EWX-WC9B>> accessed 18 June 2025

Fetic L, 'Nationale Spielräume Bei Der Umsetzung Des Europäischen Gesetzes Über Künstliche Intelligenz'

Foucault M, 'Truth and Power', *POWER/KNOWLEDGE - Selected interviews and other writings 1972 - 1977* (Pantheon Books 1980)

Freedom House, 'Freedom in the World 2025 - The Uphill Battle to Safeguard Rights' (Freedom House 2025) <https://freedomhouse.org/sites/default/files/2025-03/FITW_World2025digitalN.pdf> accessed 21 July 2025

'Freedom Index by Country 2025' (*World Population Review*) <<https://worldpopulationreview.com/country-rankings/freedom-index-by-country>> accessed 4 August 2025

Friedl P and Rolfes L, 'Datenschutz gegen digitalen Autoritarismus' (*Verfassungsblog*, 21 August 2024) <<https://verfassungsblog.de/datenschutz-gegen-digitalen-autoritarismus/>> accessed 17 June 2025

'Fundamental Rights Impact Assessment (FRIA) | aligner' <<https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/>> accessed 7 July 2025

Gallin IJ, *Rechtsetzung Ist Machtsetzung: Die Deutsche Rechtsetzung in Den Niederlanden 1940-1945*, vol 2736 (PETER LANG 1999)

Gates K, 'Identifying the 9/11 "Faces of Terror": The Promise and Problem of Facial Recognition Technology' (2006) 20 Cultural Studies 417

Giannini A and Tas S, 'AI Act and the Prohibition of Real-Time Biometric Identification' (*Verfassungsblog*, 10 December 2024) <<https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/>> accessed 23 June 2025

Gramsci A, *SELECTIONS FROM THE PRISON NOTEBOOKS* (Lawrence & Wishart 1971)

Green Legal Impact Germany, 'Gericht Gibt Elinor Recht: Vorgehen Gegen Klimaprotest Beschränkt Zivilgesellschaftliches Engagement' (2023) <https://www.greenlegal.eu/wp/wp-content/uploads/2023/12/GLI_Stellungnahme_Elinor.pdf> accessed 24 June 2025

Grother P, Ngan M and Hanaoka K, 'Face Recognition Vendor Test Part 3: Demographic Effects' (National Institute of Standards and Technology 2019) NIST IR 8280

Hahn J, 'Ein Anfang, Mehr Nicht' (*Verfassungsblog*, 11 December 2024) <<https://verfassungsblog.de/ein-anfang-mehr-nicht/>> accessed 15 April 2025

——, *Automatisierte Gesichtserkennung in Der Strafverfolgung* (Nomos Verlagsgesellschaft mbH & Co KG 2025)

Hart HLA, *The Concept of Law* (Oxford University Press, Usa 2012)

Haslam N, 'Concept Creep: Psychology's Expanding Concepts of Harm and Pathology' (2016) 27 Psychological Inquiry 1

Hausding M, 'Letzte Generation: Landgericht Potsdam sieht Klimakleber als kriminelle Vereinigung' *MOZ* (15 May 2023) <https://www.moz.de/nachrichten/brandenburg/letzte-generation_-landgericht-potsdam-sieht-klimakleber-als-kriminelle-vereinigung-70631589.html> accessed 24 June 2025

Hill K and Mac R, "'Thousands of Dollars for Something I Didn't Do'" *The New York Times* (31 March 2023) <<https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html>> accessed 18 June 2025

Hornung G and Schindler S, 'Das biometrische Auge der Polizei' (2017) 5 ZD 203

Hoven E, 'Antisemitische Äußerungen Als Gegenstand Des Strafrechts' (2025) 4/25 Zeitschrift der Kriminalpolizei <<https://kripoz.de/2025/01/31/antisemitische-aeusserungen-als-gegenstand-des-strafrechts/>> accessed 19 June 2025

Hüls S, 'Der Richtervorbehalt – Seine Bedeutung Für Das Strafverfahren Und Die Folgen von Verstößen' (2009) 4 Zeitschrift für Internationale Strafrechtsdogmatik

International Service for Human Rights, 'The National Security Law for Hong Kong: Impacts on Civic Space and Civil Society Engagement with the UN' (2022) <https://ishr.ch/wp-content/uploads/2022/09/ISHR_Report-Impact-of-HK-National-Security-Law_web.pdf> accessed 27 May 2025

International Working Group on Data Protection in Technology, 'Working Paper on Facial Recognition Technology' (International Working Group on Data Protection in Technology 2022)

<https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20230608_WP-Facial-Recognition-Tech-EN.pdf?__blob=publicationFile&v=2> accessed 2 July 2025

Kappeler K, Festic N and Latzer M, ‘Qualitative Evidence on Chilling Effects—How Users’ Imaginaries of Dataveillance Lead to Inhibited Digital Behavior’, *AoIR Selected Papers of Internet Research* (2022)

Knoche M, Hörmann S and Rigoll G, ‘Susceptibility to Image Resolution in Face Recognition and Training Strategies to Enhance Robustness’ (2022) 8 *Leibniz Transactions on Embedded Systems* 01:1

Koops B-J, ‘The Concept of Function Creep’ (2021) 13 *Law, Innovation and Technology* 29

Lanius D, ‘Der strategische Einsatz von Unbestimmtheit im Recht’ (*Forum für Streitkultur*, 27 February 2017) <<https://forum-streitkultur.de/strategische-unbestimmtheit/>> accessed 23 June 2025

Leisegang D, ‘Umstrittene Observationstechnik aus Sachsen: Auch Brandenburg betreibt biometrische Videoüberwachung in Echtzeit’ *netzpolitik.org* (5 August 2024) <<https://netzpolitik.org/2024/umstrittene-observationstechnik-aus-sachsen-auch-brandenburg-betreibt-biometrische-videoueberwachung-in-echtzeit/>> accessed 1 July 2025

Letzte Generation, ‘Stellungnahmen zum §129-Verfahren am Landgericht Flensburg eingereicht’ (*Letzte Generation*, 25 December 2024) <<https://letztegeneration.org/pm/38472/>> accessed 24 June 2025

——, ‘Werte & Protestkonsens’ (*Letzte Generation*) <<https://letztegeneration.org/mitmachen/werte-protestkonsens/>> accessed 24 June 2025

Li SZ and Jain AK (eds), *Handbook of Face Recognition* (Second Edition, Springer 2011)

Liang Q and Xiangsui W, *Unrestricted Warfare* (People’s Liberation Army Literature and Arts Publishing House 1999)

Liedtke F and others (eds), *Begriffe Besetzen: Strategien Des Sprachgebrauchs in Der Politik* (Westdeutscher Verlag 1991)

Lilie H, ‘Verwicklungen im Ermittlungsverfahren’ (1999) 111 *ZStW* 807

LTO, ‘Datenschutzaufsicht: Droht eine teure Mammutbehörde?’ *Legal Tribune Online* <<https://www.lto.de/recht/hintergruende/h/datenschutz-aufsicht-bfdi-koalitionsvertrag-datenschutzbeauftragte-bonn>> accessed 31 July 2025

Mantelero A, ‘Fundamental Rights Impact Assessments in the DSA’ [2022] *Verfassungsblog* <<https://verfassungsblog.de/dsa-impact-assessment/>> accessed 7 July 2025

Martini M and Botta J, ‘Nationale KI-Aufsicht: Aufgaben, Befugnisse und Umsetzungsoptionen’ (Bertelsmann-Stiftung 2024) <<https://www.bertelsmann-stiftung.de/doi/10.11586/2024054>> accessed 2 July 2025

Meineck S, Köver C and Leisegang D, ‘Grundrechte in Gefahr: Die sieben quälendsten Fragen zur KI-Verordnung’ *netzpolitik.org* (26 January 2024) <<https://netzpolitik.org/2024/grundrechte-in-gefahr-die-sieben-quaelendsten-fragen-zur-ki-verordnung/>> accessed 16 April 2025

Meister A, 'Gesichtserkennung und KI: Innenminister Dobrindt plant neues Sicherheitspaket' *netzpolitik.org* (23 July 2025) <<https://netzpolitik.org/2025/gesichtserkennung-und-ki-innenminister-dobrindt-plant-neues-sicherheitspaket/>> accessed 11 August 2025

Meyer-Mews H, '„Keine Bloße Formsache“ – Notizen Zum Richtervorbehalt' (2020) 7 HRRS

Monroy M, 'Vorsicht, Gesichtserkennung!' *Neues Deutschland* (24 October 2023) <<https://www.nd-aktuell.de/artikel/1177253.videoueberwachung-vorsicht-gesichtserkennung.html>> accessed 16 April 2025

——, 'Neues BKA-System: Polizeiliche Gesichtserkennung geht steil' *netzpolitik.org* (16 December 2024) <<https://netzpolitik.org/2024/neues-bka-system-polizeiliche-gesichtserkennung-geht-steil/>> accessed 2 July 2025

Müller AP, 'Orwell'sche Gleichgültigkeit und Europäische Demokratie' (*Verfassungsblog*, 23 January 2024) <<https://verfassungsblog.de/orwellsche-gleichgultigkeit-und-europaische-demokratie/>> accessed 7 July 2025

Müller J-W, 'Rising to the Challenge of Constitutional Capture' *Eurozine* (21 March 2014) <<https://www.eurozine.com/rising-to-the-challenge-of-constitutional-capture/>> accessed 19 June 2025

Oberkofler A, 'Kritische Ansätze im amerikanischen Rechtsdenken' (2001) 132 UTOPIE kreativ 925

Öffentlichkeitsarbeit RK und and Innern SS des, 'Evaluation des § 59 des Sächsischen Polizeivollzugsdienstgesetzes im Kabinett vorgestellt' <<https://www.medienservice.sachsen.de/layouts/frontend.html.erb>> accessed 19 April 2025

Paolucci F, 'Shortcomings of the AI Act' (*Verfassungsblog*, 14 March 2024) <<https://verfassungsblog.de/shortcomings-of-the-ai-act/>> accessed 7 July 2025

Pech L, 'The Concept of Chilling Effect - Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU' [2021] Open Society - European Policy Institute

Penney JW, 'Chilling Effects: Online Surveillance and Wikipedia Use' (btlj, 2016)

Pfahl-Traugher A, 'Die „Umwertung der Werte“ als Bestandteil einer Strategie der „Kulturrevolution“' in Wolfgang Gessenharter and Thomas Pfeiffer (eds), *Die Neue Rechte — eine Gefahr für die Demokratie?* (VS Verlag für Sozialwissenschaften 2004)

Poscher R and others, 'Überwachungsgesamtrechnung für Deutschland - Pilotstudie basierend auf der wissenschaftlichen Evaluation ausgewählter Überwachungsbefugnisse der Sicherheits- und Strafverfolgungsbehörden (ÜGR)' (Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht 2025)

'Projekt zur Gesichtserkennung erfolgreich' (*Bundesministerium des Innern*) <<https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2018/10/gesichtserkennung-suedkreuz.html?nn=9390260>> accessed 1 July 2025

Purshouse J and Campbell L, 'Automated Facial Recognition and Policing: A Bridge Too Far?' (2022) 42 Legal Studies 209

- Rath C, 'Gesetzentwurf zur Gesichtserkennung lässt Fragen offen' *Legal Tribune Online* (8 December 2024) <<https://www.lto.de/recht/hintergruende/h/gesetzentwurf-zur-gesichtserkennung>> accessed 16 April 2025
- Raulf S, 'Sprache und Kultur als Strategie der Neuen Rechten zur Erlangung kultureller Hegemonie' CampusPublik - Schriften zur politischen Bildung
- Raz J, *The Authority of Law: Essays on Law and Morality* (Oxford University Press 1979)
- , *Ethics in the Public Domain: Essays in the Morality of Law and Politics* (Oxford University Press 1995)
- Rieger F, 'KI-Verordnung: Deutsches Durchführungsgesetz verzögert sich' (*Medien Bayern*, 4 July 2025) <<https://medien-bayern.de/ki-verordnung-deutsches-durchfuehrungsgesetz-verzoegert-sich/>> accessed 4 August 2025
- Russell S and Norvig P, *Artificial Intelligence, Global Edition* (4th edn, Pearson Education 2021)
- Sajó A, 'Militant Rule of Law' (*Verfassungsblog*, 20 December 2023) <<https://verfassungsblog.de/militant-rule-of-law/>> accessed 9 May 2025
- Scheppele KL, 'Autocratic Legalism' (2018) 85/2 *The University of Chicago Law Review* 545
- Schindler S, *Biometrische Videoüberwachung* (1st edn, Nomos Verlagsgesellschaft mbH & Co KG 2021)
- , 'Im Auge der Polizei' (*Verfassungsblog*, 20 December 2021) <<https://verfassungsblog.de/os3-auge-polizei/>> accessed 7 July 2025
- Schmitt C, *Gesammelte Schriften 1933-1936: mit ergänzenden Beiträgen aus der Zeit des Zweiten Weltkriegs* (1st edn, Duncker & Humblot 2021)
- Schöndorf-Haubold B and Giogios C, 'KI im Einsatz für die Sicherheit' (*Verfassungsblog*, 10 December 2024) <<https://verfassungsblog.de/ki-im-einsatz-fur-die-sicherheit/>> accessed 7 July 2025
- Schreiber M and Bronner P, 'Der Referentenentwurf Für Ein Gesetz Zur Durchführung Der KI-Verordnung' (2025) ITR 7/2025 *juris PraxisReporte*
- Schroff F, Kalenichenko D and Philbin J, 'FaceNet: A Unified Embedding for Face Recognition and Clustering', *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (IEEE 2015) <<https://ieeexplore.ieee.org/document/7298682>> accessed 18 June 2025
- Semsrott A, *Machtübernahme - Was passiert, wenn Rechtsextremisten regieren* (Droemer Knaur 2024)
- Sherif M, Taub D and Hovland CI, 'Assimilation and Contrast Effects of Anchoring Stimuli on Judgments' (1958) 55 *Journal of Experimental Psychology* 150
- 'Sicherheitspaket der Bundesregierung' (*Bundesministerium des Innern*) <<https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/sicherheitspaket/sicherheitspaket-artikel.html?nn=21255176>> accessed 13 August 2025

Simmler M and Canova G, 'Facial Recognition Technology in Law Enforcement: Regulating Data Analysis of Another Kind' (2025) 56 Computer Law & Security Review 106092

SPD, Bündnis 90/Die Grünen and FDP, 'Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit - Koalitionsvertrag 2021–2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP) - 20. Legislaturperiode' Koalitionsvertrag

Staben J, 'Der Abschreckungseffekt auf die Grundrechtsausübung', *Strukturen eines verfassungsrechtlichen Arguments* (Mohr Siebeck GmbH & Co KG 2016)

Ständige Konferenz der Innenminister und -senatoren der Länder, 'Sammlung Der Zur Veröffentlichung Freigegebenen Beschlüsse Der 221. Sitzung Der Ständigen Konferenz Der Innenminister Und -Senatoren Der Länder Vom' (Ständige Konferenz der Innenminister und -senatoren der Länder 19. bis 21.06.24)

Steiner F, "'Flächenbrand für Bürgerrechte': Liberale kritisieren KI-Verordnung scharf' *Heise online* (24 January 2024) <<https://www.heise.de/news/Flaechenbrand-fuer-Buergerrechte-Liberale-kritisieren-KI-Verordnung-scharf-9606490.html>> accessed 16 April 2025

'The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda'

Tistarelli M and Champod C (eds), *Handbook of Biometrics for Forensic Science* (Springer International Publishing 2017)

Tomaszewska-Michalak M, 'Biometric Technology 20 Years After 9/11 – Opportunities and Threats' (2022) 63 *Studia Politologiczne*

Veale M and Zuiderveen Borgesius F, 'Demystifying the Draft EU Artificial Intelligence Act' (Social Science Research Network, 31 July 2021) <<https://papers.ssrn.com/abstract=3896852>> accessed 7 July 2025

Vieth-Ditlmann K and Sombetzki P, 'Stellungnahme Zur Öffentlichen Anhörung Des Ausschuss Für Digitales Am 15. Mai 2024 Zur Nationalen Umsetzung Der KI-Verordnung' (AlgorithmWatch 2024) <<https://www.bundestag.de/resource/blob/1002768/411c38bedaf76d16f5aaf0c34f729766/Vieth-Ditlmann.pdf>> accessed 2 July 2025

Wambsganz DC, 'Risikoanalyse und Datenschutz-Folgenabschätzung - Systematik, Anforderungen, Beispiele' [2022] Der Bayerische Landesbeauftragte für den Datenschutz

Wissenschaftliche Dienste, 'Datenbank-Analysen Durch Die Polizei Grundrechte Und Datenschutzrecht' (Deutscher Bundestag 2020) Ausarbeitung WD 3-3000-018/20 <<https://www.bundestag.de/resource/blob/695986/a6f049f44b45eca273cefd410c78c534/WD-3-018-20-pdf.pdf>> accessed 2 July 2025

Woodward JD, 'Super Bowl Surveillance: Facing Up to Biometrics' [2001] RAND

Ypi L, 'Bringing politics back in' [2024] *Bundeskanzler Helmut Schmidt Stiftung Magazine „For a Just Democracy!“* <<https://www.helmut-schmidt.de/aktuelles/detail/bringing-politics-back-in>> accessed 12 May 2025

‘ACLU NEWS Newspaper of the American Civil Liberties Union of Northern California Volume LXVI, No. 1’ (2001) <<https://www.aclunc.org/sites/default/files/Winter%202001%20ACLU%20News.pdf>> accessed 18 June 2025

Drucksache 20/12805 - Entwurf eines Gesetzes zur Verbesserung der inneren Sicherheit und des Asylsystems 2024

Regierung der Bundesrepublik Deutschland, Gesetzentwurf der Bundesregierung - Entwurf eines Gesetzes zur Neuordnung der Marktüberwachung

Bundesdatenschutzgesetz 2017 (BDSG)

Charter of Fundamental Rights of the European Union 2000 (CFR)

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Law Enforcement Directive) 2016 (LED)

European Convention on Human Rights 1953 (ECHR)

Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz) 2017 (BKAG)

Gesetz über die Bundespolizei (Bundespolizeigesetz) 1994 (BPolG)

Grundgesetz für die Bundesrepublik Deutschland 1949 (GG)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) 2016 (GDPR)

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) 2024 (AI Act)

Sächsisches Polizeivollzugsdienstgesetz 2019 (SächsPVDG)

Strafprozeßordnung 1987 (StPO)

The Law of the People’s Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (National Security Law) 2020