Original Research Article

BIG DATA & SOCIETY

Big Data & Society
July–September: 1–15

DOI: 10.1177/20539517241255108
journals.sagepub.com/home/bds
Sage

In Palantir we trust? Regulation of data analysis platforms in public security

Lena Ulbricht[1,2] **and Simon Egbert**[3]

Abstract

Organizations increasingly rely on digital technologies to perform tasks. To do so, they have to integrate data banks to make the data usable. We argue that there is a growing, academically underexplored market consisting of data integration and analysis platforms. We explain that, especially in the public sector, the regulatory implications of data integration and analysis must be studied because they affect vulnerable citizens and because it is not just a matter of state agencies overseeing technology companies but also of the state overseeing itself. We propose a platform-theory-based conceptual approach that directs our attention towards the specific characteristics of platforms—such as datafication, modularity, and multilaterality and the associated regulatory challenges. Due to a scarcity of empirical analyses about how public sector platforms are regulated, we undertake an in-depth case study of a data integration and analysis platform operated by Palantir Technologies in the German federal state of Hesse. Our analysis of the regulatory activities and conflicts uncovers many obstacles to effective platform regulation. Drawing on recent initiatives to improve intermediary liability, we ultimately point to additional paths for regulating public sector platforms. Our findings also highlight the importance of political factors in platform regulation-as-a-practice. We conclude that platform regulation in the public sector is not only about technology-specific regulation but also about general mechanisms of democratic control, such as the separation of power, public transparency, and civil rights.

Keywords

Palantir technologies, public security, police databanks, data protection, platform regulation, civil rights

Regulatory challenges of data integration and analysis platforms in public security

In many countries, public agencies want to exploit the benefits of big data, and for several years, critical data studies have considered this issue (e.g., boyd and Crawford, 2012). What has recently changed is that public agencies are increasingly relying on platforms that allow them to integrate and analyze various data sources (Bigo, 2020). This platformization of the state promises to allow better decision-making due to large databases, fast data analysis, and sophisticated data visualization (Brayne, 2021; Ferguson, 2017; Ulbricht, 2020). While much attention has been paid to the societal benefits and risks of state-agency use of big data analysis to classify citizens (e.g., Dencik et al., 2018), the same cannot be said about the *regulation* of state automation, especially when it comes to public sector platforms (Bellanova and De Goede, 2022).[1]

Public agencies must meet high standards when using citizen data; hence, these practices are subject to democratic oversight. There are consequently many regulatory challenges associated with accessing large data banks with citizen data and using them for automated analysis.[2] For this reason, regulation has been a major research topic in platform research, which has explored how governments try to hold technology companies accountable for the activities that happen within their platforms (Borges, 2023; Gillespie, 2010). This research has not yet been connected sufficiently with the literature on state automation. More generally, studies that empirically analyze platform regulation are still rare, especially when it comes to public sector technology use and specifically to data integration and

[1]Politics of Digitalization Department, WZB Berlin Social Science Center, Berlin, Germany
[2]Research Group Technology, Power, and Domination, Weizenbaum Institute for the Networked Society, Berlin, Germany
[3]Faculty of Sociology, Bielefeld University, Bielefeld, Germany

Corresponding author:
Lena Ulbricht, WZB Berlin Social Science Center, Politics of Digitalization Department, Weizenbaum Institute for the Networked Society, Research Group Technology, Power, and Domination, Hardenbergstr. 32, D-10623 Berlin, Germany.
Email: lena.ulbricht@wzb.eu

analysis platforms. These are very relevant because they are the basis upon which any kind of decision-support system relies.

Consequently, in our paper, we answer the following research questions: *How does platform regulation play out in public sector automation? And how do public agencies that engage in data integration and analysis platform projects ensure that the participating technology companies respect regulation?*

We answer these questions based on an empirical case study concerning the implementation of hessenDATA, a modified Gotham platform from Palantir Technologies, which is being used by the police force in the German federal state of Hesse.

This study of the deployment of Palantir software by the German police force is relevant beyond Germany. In international comparisons, Germany is regarded as having high regulatory standards for the use of digital technologies in public affairs. Moreover, it has a long history of data protection laws, and the German government has been striving to improve the digital sovereignty of state authorities for some years now (Möllers, 2021). Palantir, in turn, has been criticized as opaque due to its business model and its unclear but seemingly close relationship with the US state security agencies (e.g., Brigham, 2020). Therefore, hessenDATA is an interesting case to study regarding whether and—if so, how—the worldwide expansion of digital security platforms can be brought in line with regulatory requirements.

What makes Palantir's Gotham software even more relevant is that it enables security authorities to conduct cross-database research and data analysis, which is currently a widely shared goal among public agencies around the world (Bigo, 2020; Egbert, 2019; Gates, 2019; Wilson, 2021). Last but not least, Palantir is one of the most powerful data analysis firms today—not only in security, but also in public health and potentially many other public services, including social policy and education (Taylor et al., 2020). Surprisingly, studies on academic analyses of the company and its sociotechnical infrastructure are still rare (exceptions: Brayne, 2017; Iliadis and Acker, 2022; Munn, 2018). The few existing studies focus primarily on Palantir's US activities, emphasizing the surveillance dimension of their software, but they do not address the question (and difficulty) of regulating such platforms.

Our argument begins with a review of the academic discourse on digital platforms with particular reference to public security platforms and platform regulation. We next discuss the implementation of Palantir software in German police forces and describe the study's methodological approach. Then we analyze the empirically observed regulatory activities and related political conflicts in the case of hessenDATA. In our conclusion, we summarize our findings and call for a new regulatory approach to data integration and analysis platforms in public security that draws on liability structures as (now) known from social media platforms.

Digital platforms, platformization, and regulation

Unlike the many studies about data-driven policing that use the concepts of "surveillance", "securitization", or the "industrial-security complex" to address the subject of analysis and that zoom in on the specificities of public security (Aradau and Blanke, 2015; Ferguson, 2017; Ulbricht, 2018), we focus on characteristics that are typical for digital *platforms* as we assume they will engender particular regulatory challenges and dynamics.

Digital platforms

Digital platforms are one of the most discussed phenomena in current academic debates on digitalization. Various studies have paid attention to social media platforms like YouTube and Facebook and their curation power (Gillespie, 2010; Gorwa, 2019) and to the economic and work-related repercussions of platform companies like Google, Microsoft, Apple, Airbnb, and Uber (e.g., Vallas and Schor, 2020). While the phenomena related to the term "platform" are very diverse, they still share some basic traits: a connectivity-oriented infrastructure that aims to facilitate interactions by at least two third parties, a mode of functioning based on massive and diverse data, and a modular architecture (e.g., Andersson Schwarz, 2017; Rieder and Hofmann, 2020; van Dijck et al., 2018). Platforms are often connected to novel ways of monetizing surveillance, data, and data-driven decision-making (Srnicek, 2016; Zuboff, 2019). Hence, digital platforms can be understood as "infrastructural arrangements that situate digital operability on proprietary systems that are, to some degree, programmable and/or customizable by the system users, making possible one- or multi-sided market exchanges" (Andersson Schwarz, 2017: 375). Andersson Schwarz adds that, as "surfaces on which social action takes place, digital platforms mediate—and to a considerable extent—dictate economic relationships." (Andersson Schwarz, 2017: 375). Referring to this mediating capacity, most authors agree that, although many platform companies try to convince the public otherwise (Gillespie, 2010), platforms have a performative dimension, as they "do not simply connect social and economic actors but fundamentally steer how they connect with each other" (van Dijck et al., 2018: 24, emphasis removed). This is why "a platform is a mediator rather than an intermediary" (van Dijck, 2013: 29).

In summary, the platform literature agrees that platforms are characterized by three properties: datafication, modularity, and multilaterality. In addition, platforms develop in

markets that are often transnational and oligopolistic and their public image reveals a tension within platforms as neutral intermediaries versus influential mediators.

Digital platforms for public security

Given this tension within platforms as intermediaries and mediators, it is crucial to take a closer look at digital platforms in the public sector.[3] As mediators, they generate steering knowledge for state agents, whose decision-making practices are mostly addressed to citizens and often affect their civil rights. Because state agencies are able to make decisions that impact citizens' lives, in modern democracies their powers need to be legitimate and subject to many legal and ethical norms (Bigo et al., 2011). A new level of risk arises when private actors are brought on board in the decision-making or decision-support process. This may occur in the form of public-private partnerships, which are commonly used in digital technology projects (Bossong and Wagner, 2017). Here, private corporate actors get access to data that should typically be the sole preserve of state actors and is hence subject to strict rules (Anstis, 2021: 9). Moreover, when complex technologies are the basis for a private company's service, an information asymmetry may arise between the company and the state agency (Anstis, 2021: 9). Data integration and analysis platforms also bring about epistemic shifts in public agencies that need to be critically scrutinized. In the public security field, such epistemic shifts include the use of big data, unstructured data, and heuristics that tend to rely on correlations and good predictors instead of causal theory (e.g., Amoore, 2013). These aspects have been heatedly discussed for several years, as they have manifold implications for the rule of law in modern democracies (e.g., Ferguson, 2017). They are especially relevant for data integration and analysis platforms, as their key aim is to enhance the interoperability between databases for "smart analysis", the "so-called smart way to connect the dots and to avoid continuing to work in 'silos' with segmented information networks" (Bigo, 2020: 410). As a consequence, the regulation of public security platforms deserves more academic attention. Platform regulation is therefore a fruitful research topic.

Platform regulation

Relevant research has pointed to the many risks associated with the advent of digital platforms, for example, the proliferation of illegal or undesired online content and the discrimination, manipulation, and exploitation directed against users and workers alike. Other problems of platforms include risks linked to data protection, privacy, discrimination, and social sorting due to invasive and large-scale surveillance; the limited transparency, observability, and accountability of data-related practices of large online platforms; and the lack of clarity on governments' data sovereignty in collaborations with (often foreign) technology companies (Helberger, 2020; van Dijk et al., 2018). These risks and problems have led to various calls for stricter regulation of platform-based companies and services (Hildebrandt, 2020; Pasquale, 2015).

Much engagement with the question of platform regulation has occurred in recent years; there have been many regulatory initiatives by legislative bodies such as the European Commission,[4] increased judiciary activity,[5] and intensive academic research. The overall impetus is to make platforms accountable for practices that take place within their structures and to force them to take measures to prevent harm (Gorwa, 2019). Typical regulatory instruments associated with this *intermediary liability* are companies' reporting duties towards the public or towards oversight authorities, reporting and flagging systems for users, notice-and-takedown protocols, and sanctions for noncompliance (European Commission, n.d.).

However, regulation is not easy: Scholars have noted many obstacles to platform regulation and pointed out that regulation is often inadequate or ineffective (Pasquale, 2015; Zuboff, 2019). One set of obstacles to platform regulation concerns the properties of digital technologies, for example, the fact that many digital services are highly opaque, making it hard to trace which data are collected, stored, and used by whom and for what purpose. This opacity can be rooted in the complexity of digital practices, which may rely on semi- or unsupervised machine learning. Opacity, especially when it comes to security practices, can also originate from business or state secrecy, as companies and state agencies often protect their data-related practices from public scrutiny and therefore from legal and democratic control (Bloch-Wehba, 2021). Limited accountability is a familiar problem of public-private partnerships (Bovaird, 2004). The other set of obstacles to platform regulation stems from the societal conditions in which digital platforms arise: the monopolistic features of digital markets prevent rights-preserving business models from flourishing (Colangelo and Maggiolino, 2018) and oversight agencies are understaffed such that regulation is not properly implemented (Jori, 2015).

Bellanova and de Goede rightly state that (2022: 107), "concerning security algorithms as a target of regulation, there is [still] a need for greater understanding of how the operationalization and legal enforcement of values (…) take place in and through data architectures." Further to this, we must add that analyses that study concrete *practices* and not just *formal* norms are needed to understand platform regulation. At present, most research about platform regulation focuses on the formal norms of regulation, such as existing and proposed legislation (Hildebrandt, 2020) and the terms, conditions, and codes of conduct issued by technology companies (Gorwa et al., 2020; Pasquale, 2015).

Studies that have scrutinized the actual *practices* of platform regulation, including legislative processes, day-to-day rule implementation, and monitoring, are very rare. A few empirical studies have indicated that technology companies often have a large leeway to define whether and how they comply with regulation and that they are lenient towards themselves; this is evident with regard to the self-monitoring of rule enforcement (Gillett et al., 2022), and with regard to assessing and preventing racism (Siapera and Viejo-Otero, 2021). Other studies have analyzed legislation in response to platforms—pertaining to sharing economy companies such as Uber and Airbnb (Aguilera et al., 2021)—at the national and subnational level, finding that the strictness of state regulation depends upon the overall regulatory strictness in a given policy area, and on domestic power constellations (Gorwa, 2021; Laurer and Seidl, 2021). Platform companies strongly oppose regulation and use various lobbying strategies to defeat it: For example, they lobby against new regulation (Mazur and Serafin, 2023) and in favor of corporate self-regulation (Medzini, 2022), they refuse to collaborate in implementing regulations (Colomb and Moreira de Souza, 2023), they engage in discursive legitimation of their activities (Chan and Kwok, 2022), and they mobilize users and customers in the corporate interest (Yates, 2023).

Societal actors outside the company are usually not involved in regulatory implementation (Bloch-Wehba, 2022).[6] The above-mentioned studies relate to state control over technology *companies*; very few studies address cases where *state* actors make use of technology services and platforms. There is one exception, namely a study about digital governance in the smart city of Shenzhen (China), which showed that growing data centralization reduces the control that public servants at lower administrative levels have over citizen data. The study also showed that the integration of citizen data attracts technology companies (Große-Bley and Kostka, 2021). The details of data governance and regulation were, however, not comprehensively addressed in the study.

We complement these studies by analyzing the rules and practices of regulation in a specific case of a public platform, more concretely in the case of police platformization. In this contribution, we understand regulation as state control—over companies, but also over public agencies, and other societal actors (Koop and Lodge, 2017). The distinctive feature of public sector platform regulation is that it implies two levels of control: first, state agencies controlling their corporate contractors, and second, state agencies (those in charge of regulation and oversight) controlling other state agencies (those who are in charge of the technology project). In principle, public platforms therefore imply both forms of regulation: traditional regulation between state agents and companies; and state self-regulation, with its many problematic implications. Studying platform regulation with regard to public sector platforms is therefore conceptually interesting because it gives insight into how this self-regulation plays out within the state. Similar *laissez faire* mechanisms may be evident here as in corporate self-regulation but there may be entirely different ones at play. In principle, in democracies, many institutional mechanisms are aimed at constraining the power of state agencies and establishing democratic control. These include various forms of power separation, public transparency obligations, and constitutional and civil rights.

We now turn to analyzing a case where public agencies decided to closely cooperate with a corporate platform and had to find ways to comply with regulatory needs that resulted in their utilization of a data integration and analysis platform.

Platformized public security in Germany

Our study focuses on the data integration and analysis platform Gotham by US-based Palantir Technologies and its utilization by police forces, with special emphasis on the case of hessenDATA in the German federal state of Hesse. In this section, we will contextualize the case of hessenDATA in light of overall datafication trends in German policing.

Methodological approach

To understand how the hessenDATA project was implemented, what regulatory problems arose, what regulatory activities took place, and what discourses were relevant, we researched and analyzed a number of publicly available documents. The complete list includes 85 documents, mainly parliamentary and government documents, but also media articles with relevant quotes by persons involved in the regulatory process (see Annex). In addition, to validate our observations and fill the gaps in the publicly available material, we conducted a semi-structured interview with the project team of hessenDATA, which included a demonstration of the platform, and three guided interviews with members of the parliamentary opposition who were part of the parliamentary committee that investigated the tendering process (see the interview list in the Annex). These interviews especially focused on representatives of opposition parties, as we assumed that their perspective would not be sufficiently represented in the official documents, which very closely reflected the government's framing. We combined the various types of data to obtain a comprehensive picture of the implementation process of hessenDATA and the (political) discussion that took place around it.

The documents and the transcripts of the interviews were subjected to a qualitative content analysis by both authors and coded until code saturation was assumed to be achieved. The coding process was based on the content analysis method according to Kuckartz and Rädiker (2023),

which combines both inductive and deductive coding strategies. This meant that the analysis was sufficiently focused on the topic at hand but was, at the same time, sufficiently open for unexpected insights to emerge from the empirical data. Hence, despite its thematic focus, the analysis was able to shift the researchers' preconceptions and generate new knowledge about the subject. For instance, the focus on regulatory challenges and conflicts was not anticipated at the beginning of the analytical process; it emerged in the course of the more detailed analysis of the data, as these suggested that the hessenDATA platform is particularly difficult to regulate. This, we will show, has to do with its platform character.

Palantir Gotham in German policing

The most prominent current trend in police datafication in Germany is the increasing use of data integration and analysis platforms by police forces. Hesse was the first to use the services of US-based Palantir Technologies and its Gotham software. The Hessian police have been using Palantir Gotham since the summer of 2017 (Beverungen, 2021). Soon, other German regions followed: starting in 2021, police in North Rhine-Westphalia piloted a "system for cross-database analysis and research" (called *Datenbankübergreifende Analyse und Recherche* in German, or DAR for short), also based on the Palantir Gotham platform (Landeskriminalamt Nordrhein-Westfalen, 2020), which has been in operation since spring 2022. The Bavarian police have a project called the "Cross-Procedural Search and Analysis Platform" (*Verfahrensübergreifende Recherche und Analyse* in German, or VeRA for short), which led to a contract with Palantir in spring 2022 (Bayerisches Landeskriminalamt, 2022). Although the original plan was to make VeRa (as "VeRa Bund") available to all other federal states in Germany via a framework agreement, coordinated by the Federal Ministry of the Interior, the Federal Minister of the Interior recently decided to stop this plan for now and to instead aim for an in-house system (Zierer et al., 2023).

Founded in 2004, Palantir is a digital technology company commonly regarded as remarkably secretive and publicly controversial, not least due to its deliberately opaque appearance and the controversial image of the company's investor Peter Thiel[7] (e.g., Chafkin, 2021). The main service Palantir offers to security agencies is its data integration and analysis software Gotham. The company describes the scope of its software as follows:

> Our products serve as the connective tissue between an organization's data, its analytics capabilities, and operational execution. Palantir's platforms tie these together by bringing the right data to the people who need it, allowing them to make data-driven decisions, conduct sophisticated analytics, and refine operations through feedback

(Palantir, 2020b). As we will illustrate in the following section, Palantir Gotham relies upon datafication, modularity, and multilaterality—thereby qualifying as a platform.

Like the operators of the digital platforms described in the literature (Gillespie, 2010), the providers of data integration and analysis platforms tend to characterize their software as agnostic and neutral, often denying the mediator status of their platforms. In this vein, Palantir states that they "are not a data company" (Palantir, 2020b), since they do not use data from their clients for their purposes. Instead, they present themselves as a "software company" that is "build(ing) digital infrastructure for data-driven operations and decision-making." Our analysis will show the distinctive regulation-related challenges connected to this form of platform policing.

A platformization pioneer in Germany: hessenDATA

Since the summer of 2017, the police in the state of Hesse have been using Palantir's Gotham software, under the name hessenDATA, to generate time-critical information by means of cross-database research, to access heterogeneous sources and correlation-based context analyses, and to implement this information directly in police operations and strategies (Hessisches Ministerium für Inneres und Sport, 2018: 59). The main goal is to make the policing of "terrorists and serious criminals" more effective (Hessischer Landtag, 2019a: 1).

The program was implemented comparatively quickly since the relevant authorities publicly claimed that there was a sufficiently concrete risk of terrorist attacks in Hesse at that time and a need to quickly make the program operational. Instead of issuing a call for tender, as legally required, the contract was awarded directly to Palantir for a limited time period on the grounds of special urgency; it was later granted permanent status (Hessischer Landtag, 2019b: 20).

The goal of hessenDATA is to enable human analysts to find associations between entities (e.g., people, spaces, objects) with a view to preventing terrorist attacks or discovering organized crime networks. The sales argument was that an investigator interested in a suspect could either spend all their time following that person, or they could set up an alert in the software. According to the 2018 annual report of the Hessian Ministry of the Interior and Sport, before hessenDATA, much data processing was done manually and required the raw data to be forwarded to IT specialist services at the Hessian State Criminal Police Office, where the data were processed within a week or so (Hessisches Ministerium für Inneres und Sport, 2018). The use of hessenDATA purportedly made it possible to cut out these time-consuming manual steps and obtain a complete and structured overview of the data in minutes (Interview Police Hesse).

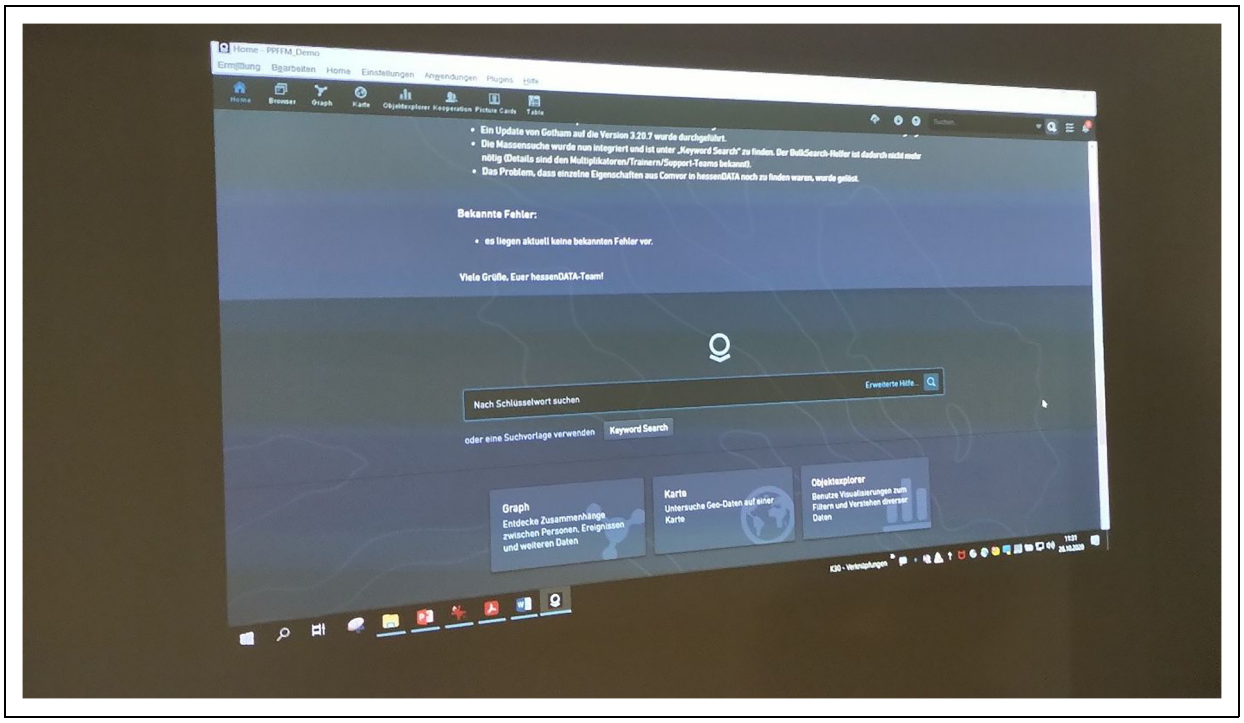

Figure 1. Start screen hessenDATA (Source: Author photo).

The hessenDATA platform works as a "dragnet," as it allows the relationships between people, objects, and places to be represented in the form of a network (see also Brayne, 2017). Investigators can use a search interface (see Figure 1) to analyze this web of relationships from any node. For example, investigators receive a message when certain entities (names of people or places, keywords, and objects) appear in a surveilled person's telecommunications. Palantir offers additional modules that can be added to Gotham, such as Ava, a set of AI functions, and Dossier, a tool for inter-organizational collaboration. In Hesse, additional functions have been added at the police's request, such as the integration of profile pictures and mugshots. A mobile version has also been established (Interview Police Hesse).

Significantly, this type of analysis platform is characterized by the "desilozation" of databases, that is, the breaking up of "data silos," allowing officers to access different data banks within one platform from one central virtual place. Associated with this, there is the potential to link numerous sources of data (internal police data and external data), which enables analyses at high speed. Referencing hessenDATA's software architecture, some commentators have aptly spoken of a "Robocop-Google" (Brühl, 2018) (see also Figure 1). For police operators, hessenDATA's desilozation function is of utmost importance since it makes it much easier to access data from different data banks. In doing so, it enhances the interoperability of different data banks and systems.

The following police and nonpolice data sources are included in hessenDATA analyses: POLAS, CRIME, and ComVor. POLAS (*POLizeiAuskunftsSystem* [Police Information System]) stores law enforcement data. CRIME (Criminal Research Investigation Management Software) is a preventive database, a case-processing system where data necessary for investigative procedures in the future are stored. ComVor (*Computergestützte Vorgangsbarbeitung*) is the standard case-processing system, where all police procedures are kept and where patrol officers document their actions. Furthermore, hessenDATA can also access traffic data from telecommunications surveillance and data from telecommunications providers. In addition, data from seized cell phones can be integrated (forensic extracts). Of particular interest are the telephone numbers and communication data, such as the time of calls, the length of calls, and the people called (who can then be analyzed with the focus on associations). Police telexes, an internal police email system for formal communication, are also included in hessenDATA; these are especially used to investigate criminal cases or share important news, such as the arrest of a high-level suspect. Finally, hessenDATA can also access data from social media sites. This includes both public and nonpublic data—for example, information obtained by Facebook through a mutual legal assistance request to the United States. However, hessenDATA only has access to these networks in individual cases, after a court order.

Summing up, hessenDATA is characterized by datafication, modularity, and multilaterality. Multilaterality results

from the linkage of databases and, hence, data. Palantir Gotham also links different police forces: Officers from diverse units maintain and evaluate data, sometimes beyond the region of Hesse. One consequence of this is that analysts in the back office are given greater power than police officers in the field, whose superior knowledge about the local context and greater field experience is ultimately devalued (Brayne, 2021: 77; Wilson, 2017: 118). The linking of databases is also a regulatory problem in view of earmarking principles and the different legal underpinnings of the databases, as will be scrutinized in the following section.

Analysis: regulatory conflicts and strategies in the case of hessenDATA

Given that new and integrated platforms often raise new questions when they are implemented, it is not surprising that the establishment of hessenDATA created various regulatory conflicts. Against this backdrop, in our empirical analysis, we will engage with these regulatory conflicts in more detail, especially with the concerns raised by the implementation of hessenDATA. The concerns were linked to the three defining features of platforms—datafication, multilaterality, and modularity—triggering conflicts about data protection, civil rights protection, and the overall transparency of the project. Another concern was linked to who would take responsibility for the activities within the platform and whether Palantir could be considered an intermediary; the third set of conflicts was about fair market competition and the procurement process that led to the contract with Palantir.

The defenders of the hessenDATA project were mostly representatives of the Ministry of the Interior, the Hessian police, and elected members of parliament of the majoritarian Christian Democratic Union (CDU). Criticisms of the project were mainly voiced by the opposition parties in the Hessian parliament and by civil rights organizations.

Datafication, multilaterality, modularity, and conflicts about data protection and civil rights

Datafication and conflicts about data protection. The main regulatory challenge of the HessenDATA project emanated from datafication and the related data protection problems. One of the major concerns of the parliamentary opposition was that hessenDATA could foster potentially unlawful forms of state surveillance. The option to combine various data sources prompted particular fears that any citizen could become a target of surveillance and suspicion (Hessischer Landtag, 2019b: 2). In addition, the potential for integrating social media data raised concerns that all kinds of information could be deemed relevant for criminal investigations and lead to a huge increase in the numbers of innocent citizens under surveillance (Hessischer Landtag, 2019a: 2). To address these concerns, the government integrated a new paragraph into the existing public security law to explicitly allow *automated* data analysis of personal data in cases of public interest.[8] The aim was to create a legal basis for hessenDATA, because data protection law generally forbids data mining of sensitive personal information (Hessischer Landtag, 2019b: 2). Data mining, as defined by the German Federal Constitutional Court, is distinct from simple data analysis because it combines massive and multiple data sources to create unexpected insights, thereby creating "new knowledge". According to the Federal Constitutional Court, in its interpretation of the German Federal Data Protection Act, data mining poses a threat to various civil rights and therefore must only be used to achieve important aims, for example, to deal with an imminent threat, and meet specific requirements. The Federal Data Protection Act thus establishes more stringent criteria for data mining than the European Data Protection Law Enforcement Directive (EU) 2016/680, which it implements.[9] Accordingly, the new paragraph of the Hessian Law on Public Security and Order allows for automated analysis of connected data to prevent serious crimes (such as corruption, child pornography, murder, etc.) and to ward off existential threats to the nation. However, a collective of lawyers and civil rights organizations submitted a constitutional complaint against the new legal paragraph in 2019, arguing, among other things, that the conditions for data access and analysis were too broad. In early 2023, six years after the first implementation of hessenDATA, the Federal Constitutional Court ruled mostly in favor of the plaintiffs (Bundesverfassungsgericht, 2023). Consequently, hessenDATA is currently operating on the basis of an unconstitutional law, and the Hessian government has started the process of modifying the relevant passages (Voigts, 2023).

Multilaterality: data-driven policing and civil rights protection. The fact that hessenDATA is multilateral and connects data (banks), but also various units within the Hessian police and potentially links the Hessian police with other German police units—affecting citizens and society as a whole—has triggered concerns about how well citizen rights would be protected with regard to data protection, the presumption of innocence, the freedom of movement, and protection against discrimination. While the parliamentary opposition and (critical) journalists painted a picture of a society characterized by pervasive data-driven policing, frenzied prosecutions, and authoritarian aspirations (Hessischer Landtag, 2019b: 19), the government justified hessenDATA by underscoring its usefulness for prosecuting Islamic terrorists and preventing future terrorist attacks. In these justifications, it referred to the publicly noted lack of collaboration between police units in Germany in the wake of terrorist attacks like the one perpetrated in Berlin in December 2016.

Modularity: transparency problems and modular data protection. The modularity of hessenDATA made it problematic for the public and the parliamentary opposition to keep track of the project. The unclear scope of data collection and use and their societal effects made hessenDATA a topic of public controversy, and the modular structure of Palantir's services was perceived by the parliamentary opposition as an obstacle to financial transparency. They criticized the failure to publish the overall project budget and suspected an overrun of the budget initially stipulated in the procurement process as additional services were added to the initial service description. At the same time, the modular structure of Palantir's services was also used as an argument in favor of the project, mainly as an element of the data protection strategy: The government stressed that Palantir's offer to tailor a modular data protection and data security system to Hessian police's needs had been one of the main reasons to choose Palantir (Interview Police Hesse). Palantir offers to develop data protection concepts for its customers, it has an in-house Privacy and Civil Liberties Engineering Team, and it offers data control nudges and checkpoints in its software (Palantir, 2020a). According to the Hessian police, hessenDATA has various structural and procedural features to ensure data protection and information security in daily data-integration and data-analysis practices. One element concerns the structure of the data bank: hessenDATA limits data flows from police data to hessenDATA, thus making sure that the original police data banks remain unchanged (Interview Police Hesse). In addition, the data used by hessenDATA is still held on police servers and supposedly does not go through Palantir servers; hessenDATA is not connected to the internet but only to the police intranet ("Sondernetz") (Hessischer Landtag, 2019b: 19); in addition, the data fed into hessenDATA are deleted after two years (Interview Police Hesse). Another data protection module facilitates the control of users by a system of access rules and control procedures (based on a "role-based access control" model). Any police analyst who wants to use the system has to request access and provide reasons that justify the use of hessenDATA, the request must be predicated on investigating or preventing some sort of serious crime, and hessenDATA cannot be used for other investigations. Access is granted for a limited period of time and can be restricted to subsets of the data. Users receive a two-day training course prior to their first use of the system. A logging system records all activity in the system, and random checks of appropriate use take place (Interview Police Hesse).

Intermediary responsibility

Did the Hessen government hold Palantir accountable for possible risks or harms with regard to the platform? The data protection and civil rights concerns led to a debate on whether the government and Palantir were exhibiting sufficient responsibility for the project and were accountable to the public. One aspect that attracted attention was the lack of clarity on whether hessenDATA was connected to the internet. A hessenDATA operator testified that it is indeed possible to integrate data from an internet search into hessenDATA (Interview Police Hesse). The 2018 annual report of the Hessian Ministry of the Interior also stated in a section on hessenDATA that matching with information openly viewable on the internet, such as from social networks, was possible (Hessisches Ministerium für Inneres und Sport, 2018: 58). These statements remain ambiguous, as no consistent differentiation is made between publicly viewable and non-publicly-viewable information from social networks and other sources. Also, the statements do not explain how publicly viewable data sets are discovered by the software and how they are added to hessenDATA or whether this is part of Palantir Beagle's scope, which is described by hessenDATA officials as analysis software for the public areas of social networks (Hessisches Ministerium für Inneres und Sport, 2018: 58). Beagle functions as an integrated solution for searches in social networks and in other open sources triggered by individual cases. Another matter of public concern was whether Palantir could access police data in order to improve its products or even to share it with US intelligence agencies. In response, the Hessian government said it had established a system of regulation and oversight, but its details are not accessible to the public. The government has, for instance, stressed that the relevant data protection and information security rules are formalized in guidelines (Interview Police Hesse); however, these have not been shared with the public or with the parliamentary opposition (Interview opposition party 1, 2, 3).

With regard to oversight, hessenDATA is regularly reviewed by the criminal police's internal data protection officer and by Hesse's independent data protection authority (Interview Police Hesse), but, again, the relevant review reports have not been made public. We contacted the data protection authority, but it did not make anyone available to talk to us about its ongoing assessment of hessenDATA; indeed, the authority did not make any public statements on the matter throughout the whole process, with the exception of those made in the oral hearings before the Federal Constitutional Court, where the data protection authority was summoned as an expert witness (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2022). This attitude contrasts with that of the independent data protection authority in North Rhine-Westphalia, which criticized the use of the Gotham-based DAR at an early stage—on the grounds that it represented data mining and that it allowed the use of data collected for another purpose, which would require its own legal basis (Landtag Nordrhein-Westfalen, 2021). The opposition parties in Hesse stated that the

government had been reluctant to respond to information requests and had used public security arguments to justify this opacity (Interview opposition party 1, 2, 3).

In summary, for the wider public and for the parliamentary opposition, it was not clear whether the police and Palantir had handled citizen data in compliance with the law. The government strategy was to shield Palantir from scrutiny instead of making a convincing case that they were effectively overseeing the company and had mechanisms in place for cases of rule violation. For Palantir, this meant that—unlike social media and gig platforms, which are increasingly being made to take responsibility for activities that take place within their infrastructures—it would not have to respond to any kind of public scrutiny, let alone bear any liability. Here, the contractual arrangement is a problem, as we will discuss in the conclusion.

Fair market competition and conflict about the procurement process

Another major regulatory conflict was connected to the question of whether and how to ensure that fair market competition aided the selection of the best and most trustworthy technology company. In contrast to social media and gig platforms, such as Facebook, Twitter, Uber, and Airbnb, which have few serious competitors, there are several companies that offer analysis and integration services and that would have been alternatives to Palantir. Consequently, the opposition accused the government of choosing Palantir without a serious market study, claiming that the government had not taken the necessary steps to establish a legal and fair public procurement procedure. The parliamentary opposition suspected that Palantir initially made a low-price offer in order to secure contracts with a few German police units and create incentives for other police forces to opt for Palantir too. Thus, the opposition established a parliamentary inquiry commission, where the relevant matters of the procurement procedure were debated—partly in public and partly in closed sessions. While the government was able to continue the project despite these accusations, it was obliged to publicly provide evidence that, first, no other company would have been able to make a better offer and, second, Palantir was a trustworthy partner. With regard to competitors, the government argued that urgent security threats, such as looming terrorist attacks, necessitated an abbreviated procurement procedure, with a very short time for tenders (Hessischer Landtag, 2019b: 80). The government also argued that the absence of appeals by possible competitors was proof that Palantir was the only company that was up to the task at that moment—although both arguments were challenged by the parliamentary opposition (Hessischer Landtag, 2019b: 56–57). In addition, the parliamentary opposition pressured the government to justify the collaboration with Palantir, pointing out that its clients and investors included US military and intelligence agencies; the opposition thus requested tight controls to avoid data leaks (Hessischer Landtag, 2019b: 6). According to its own statement, Palantir only processes its customers' data but does not control the data (Palantir, 2020b)—and the Hessian government repeated this argument.

As to this second argument that underscored Palantir's trustworthiness, the government made several points. First, it conceded that complete control of digital data flows would be impossible to achieve and that, in its view, there is no large technology company that does not collaborate with national intelligence agencies (Interview Police Hesse). Second, the government pointed to purportedly successful previous collaborations between Palantir and police forces in the Netherlands and Denmark and with Europol (Interview Police Hesse). Third, the hessenDATA project leaders also stressed that the German Palantir staff had engineering degrees from reputable German universities (Interview Police Hesse). Fourth, according to their statement, the Hessian police conducted extensive security checks on each Palantir agent who had access to the criminal police premises. Fifth, to create a common culture of work and trust, they built mixed teams of Palantir staff members and members of the police, who worked in joint offices (Interview Police Hesse).

Summing up the analysis of regulatory conflicts in the case of Palantir Gotham for hessenDATA, it is clear that the project was facilitated by two simultaneous government strategies. First, the existing public security law was modified and the technological infrastructures and data-related practices were linked by procedural rules whose implementation was only monitored internally, if at all. Second, this strategy of partial control was justified by a discursive strategy that propagated trust—pointing out that comprehensive control could not be achieved and following the rationale that the user benefit would outweigh the possible societal risks. This was enabled by the traditional service-related contractual relationship between the police and Palantir, which implies that there is little clarity for the public on Palantir's motives and responsibilities—as opposed to public-private partnerships, in which state and private actors cooperate with each other as partners and sometimes share accountability (Christensen and Petersen, 2017).

Discussion and conclusion

Data integration, data analysis, and regulation

As expected, the findings reveal that digital security platforms sparked regulatory challenges owing to the special features of contemporary data integration and analysis platforms provided by inherently opaque technology companies. These specific regulatory challenges pertaining to data integration and analysis platforms include, among other things, the integration of various data sources with different

legal foundations (e.g., police data banks and social media data). In this process, new information is generated that cannot be reconciled with the purposes for which the original data were collected. The purpose-limitation principle, which is an important pillar in European data protection regulation, is consequently violated. Another challenge is the modular structure of digital platforms, which makes the software architecture flexible and at the same time hard to grasp, both in conceptual and regulatory terms. An additional challenge is the global scale of platform technology markets, which leads public agencies to collaborate with companies from other nations and jurisdictions, raising doubts about digital sovereignty.

In this case, these challenges resulted in political conflicts—interestingly, not so much between the companies and the state agencies that hired them but rather between the government on one side and opposition parties and civil rights organizations on the other. This is due to the fact that legally, the police were responsible for the project. Even though Palantir played a decisive role in shaping the project according to its product and services and made important decisions about data administration, data access, data protection, and data sovereignty, the company was systemically shielded from political criticism and public scrutiny due to its role as a mere contractor, as the contracts do not contain public-scrutiny and democratic-control provisions. Public security agencies themselves have traditionally been shielded from public scrutiny and accountability, and this opacity has now been extended to cover technology companies. In the main regulatory conflict, therefore, the Hessian police were pitted against other state actors, such as the parliamentary opposition and the Federal Constitutional Court. Here, traditional means of democratic control, such as a parliamentary inquiry committee and a constitutional complaint, were mobilized. The main regulatory agency, the Data Protection Authority, played an ambiguous role: it was formally involved but did not effectively oversee regulatory implementation. There may be many reasons for this, ranging from limited control capacities to cooptation. What is clear is that oversight authorities might be too weak to control politically powerful state agencies, like the police, which are backed by the Ministry of Interior.

Overall, regulation was as much an enabler as a limitation, and the government seems to have been able to conduct the project without much restriction. The regulatory conflicts neither ended nor substantially changed the project. The fact that the parliamentary opposition was not able to fundamentally affect that project was not only due to difficulty in mobilizing public opinion on matters of data protection and data security but was also a general consequence of unequal power relations between parliamentary majorities and minorities in German federal states. This has been a matter of public concern and political science research for decades (Siefken, 2018). On a more positive note, the activation of democratic control procedures based on the separation of powers, such as the parliamentary inquiry committee and the constitutional complaint, was effective in the sense of pressing the government to justify its decisions and actions in public. This public controversy might be a reason why other German states later indicated that they would use European data integration companies rather than Palantir, develop in-house solutions, or even do without such systems (Zierer et al., 2023).

Our case also illustrates how difficult it is to assess and control data integration and analysis: In line with theories in critical algorithm and data studies that emphasize the interrelatedness of algorithms, data, and databank structures and the difficulty of treating them as separate elements (e.g., Dourish, 2016), what we saw in the case of hessenDATA was a definitional effort and dispute. The government and opposition had competing ideas about the nature of Palantir Gotham and whether it would comply with German constitutional norms. This regulatory conflict highlights how digital technologies challenge concepts commonly used in legal regulation: Data protection laws at both German and European levels differentiate between data collection, which is accessible to public agencies, because it is justified by law and is linked to a specific purpose, and data analysis, which, if it is automated, needs to follow much stricter rules. The constitutional complaint highlights a legal dispute about the question of whether data integration and data analysis can be distinguished and more specifically whether data integration is a form of data mining. As noted above, this definitory and hence regulatory difficulty is closely connected to the platform character of the Palantir software.

In summary, we observe that platform regulation *in practice* implies a series of conflicts about the nature of technology and social risks and about what kind of regulation is necessary and sufficient.[10] With regard to the specificities of regulation-as-a-practice with regard to platforms, we observed that state agency regulation meant oversight of the private platform operators with whom they cooperate, mainly through *procedural* rules, but it also meant refraining from claiming *comprehensive* control and relying on *trust*. State self-regulation proved to be ineffective with regard to the oversight agency and rather impactful with regard to democratic control procedures.

Ultimately, we propose a different regulatory path for the data integration and analysis platforms used in state services that would entail handling platform vendors as liable intermediaries.

Benefits of a platform perspective

If we look at hessenDATA not just as a public security project but as a digital platform entrusted with the task of integrating data and making it analyzable, we can gain new perspectives for empirical analysis and new ideas for regulation (see Table 1). Platforms are inherently data

Table 1. HessenDATA and its regulation from a platform perspective.

platform aspect	HessenDATA	themes of regulatory conflict	options for regulation
datafication	data bank integration, automated data analysis, search engine, visualization	data protection and data sovereignty	automated reporting, accountability, and regulatory monitoring
modularity	modular structure with different opt-in functions	public transparency, costs	modular data and rights protection
multilaterality	connection between data banks and between police forces	invasive surveillance, data-driven policing, civil rights	intermediary responsibility: reporting and flagging systems for users and citizens, notice-and-takedown protocols, sanctions

Source: authors

driven, they connect different sides, and they are scalable and modular. This platform perspective enables us to not look solely at the police and its security practices but at the sum of the linkages of data and actors that Palantir Gotham created. In doing so, we can more comprehensively capture the impact of Palantir Gotham and the involvement of third parties.

For the public, it is still not sufficiently clear who has access to what kind of data and what decisions are taken based on hessenDATA. While this is the case for many other digital technologies as well, it is especially typical for data integration and analysis platforms, since these are flexible and customizable by nature, making it even harder for outsiders—including relevant oversight bodies—to determine their functions and hence their possible encroachments on civil rights. Whereas social media platforms are visible to end users, generate direct user experiences, and increasingly provide transparency and redress procedures for users, public security data integration and analysis platforms are entirely outside of direct citizen control. While low regulatory standards are still too common in digital technology markets, the uncertainty we observed regarding regulatory compliance in the case of hessenDATA is rather unsettling—considering that the platform directly influences the fulfillment of public (security) functions and may thus encroach on numerous civil rights. Technology companies and their state clients should not benefit from loose digital-technology-market rules when executing public functions—quite the contrary.

Accountability and platform liability

It is clear that Palantir's self-portrayal as an agnostic infrastructure has to be challenged. If Palantir were to be seen as an intermediary, it could be held liable for the activities on its platform—either by invoking already existing norms or by creating new regulations similar to those created by the EU's Digital Services Act. Such regulations could include procedures of transparency towards data subjects, such as reporting and flagging systems for users and citizens, and the establishment of publicly accessible, reliable, and fast procedures in cases of harm (notice-and-takedown protocols).[11] In addition, the monitoring of regulatory implementation and relevant reporting could be automated. State agencies and their contractors could be required to undertake reporting duties and establish oversight boards, and they could face sanctions for noncompliance. Another possibility would be to create an interface for citizens seeking to access whether and how information that concerns them —for example, about themselves or their neighborhood— has been processed in the platform, and with what consequences. While the above-mentioned culture of secrecy and opacity in public security agencies are serious obstacles to these regulatory propositions, there are examples where citizens already have basic rights concerning their personal information in police data banks, for example, rights to access and redress. In addition, various regions in Germany have experience with independent oversight organizations that partly control police activities and serve as an access point for citizen concerns and complaints.

Relevance beyond the case

While additional empirical studies of platform regulation in practice are necessary, the present study's findings are relevant beyond hessenDATA, as Palantir products are spreading to other German regions and even other European states. The question of whether and how the services of US-based technology platforms can be implemented in the field of public security—in line with the existing legal norms in data protection, data security, and public procurement—is being closely observed by other governments. If successful, the strategies used in Hesse could be applied elsewhere. Our study underlines the great uncertainty about the nature and extent of regulatory compliance regarding digital security technologies generally and data integration and analysis platforms specifically. In principle, the hessenDATA case can be seen as an expression of the implementation of the GDPR, the European Data Protection Law Enforcement Directive, and national data protection laws. These legal norms provide rules but leave margins for interpretation. The question of how

public agencies and regulatory oversight authorities define what data-related practices are acceptable and how this will be assessed thus ultimately points to how laws materialize. The German Constitutional Court has, for example, established rather strict standards for data mining by law enforcement agencies, while the data protection authority of Hesse has decided to abstain from establishing strict implementation monitoring and from supporting public accountability.

Democratic implications of the platform control deficit

Platform regulation is not only a matter of regulatory agencies controlling companies, but also of state agencies controlling other state agencies. Here, it is evident that traditional mechanisms of democratic control—such as the separation of powers, checks and balances, party competition, and public scrutiny—are part of platform regulation. Consequently, good functioning of democracies is as important to platform regulation as technology-specific regulation. Or, on a more critical note, we could say that the weakness of the parliamentary opposition, the weakness of civil society, and the weakness of the data protection authority are hurdles for effective platform regulation. In addition, it is noteworthy that data protection and data sovereignty did not play an important role in public debates or election campaigns; this is in line with the more general pattern that digital surveillance very rarely leads to massive citizen protest.[12] Platform regulation is not only about finding the right incentives and mechanisms to avoid social harm through technology. Instead, it is clear that platform regulation in practice depends upon political factors, such as the specific interests, resources, and power relations of the involved actors. Platform regulation is a political process and it depends upon healthy democracies—and in the same way, healthy democracies depend on functioning platform regulation.

Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Bundesministerium für Bildung und Forschung (Weizenbaum Institute for the Networked Society) and the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (Grant agreement No. 833749). We also acknowledge support for the publication costs by the Open Access Publication Fund of Bielefeld University and the Deutsche Forschungsgemeinschaft (DFG).

ORCID iDs

Lena Ulbricht https://orcid.org/0000-0002-6259-0144
Simon Egbert https://orcid.org/0000-0002-3729-0393

Supplemental material

Supplemental material for this article is available online.

Notes

1. We are grateful for the cooperation of Jana Pannier, David Prinz and Ole Fechner. We also thank the organizers and participants of the workshop "The Role of Data Integration and Analysis Platforms in Contemporary Society", at IT-University of Copenhagen for their comments on an earlier version of this paper. We also thank the anonymous reviewer and Rocco Bellanova from Big Data and Society for their valuable feedback.
2. One obstacle is, for example, the high complexity of digital data and analysis algorithms, which makes it difficult to externally verify the legality of the practices; another is the difficulty of controlling private technology companies that are often opaque, that distribute complex technology, and that may have a "move fast and break things" approach to regulation.
3. In this study we zoom in on public security, as it is one of the sectors with the highest number of technology projects.
4. Examples of recent European platform regulation include the Digital Services Act, the Digital Markets Act, the Artificial Intelligence Act, the Data Governance Act, the General Data Protection Regulation, and many other related legislative initiatives.
5. Examples of recent legal actions are the many court cases of the European Commission against Google, Amazon, and Facebook.
6. There are a few recent exceptions, such as the Facebook Oversight Board and the dispute settlement processes of the DSA [Art. 21 DSA], but the actual power of civil society actors is not yet clear.
7 The public image of Peter Thiel has not only been shaped by his various business enterprises (as a co-founder of PayPal and an early investor in Facebook) but also by his support for Donald Trump and his plans to create a radical libertarian society on an artificial island.
8 §25a Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG). While the data protection law allows for the collection and use of personal citizen data by state agencies in public interest, the government followed the suggestion of the independent data protection authority and created a specific authorization procedure for automated data integration and analysis, which was integrated into the public security law (Hessischer Landtag, 2019b: 5–6, 86–87.)
9 The European Data Protection Law Enforcement Directive does not explicitly prohibit data mining by law enforcement authorities. It does, however, establishes rules and safeguards to govern the processing of personal data for law enforcement purposes: Data processing must be lawful, fair, and transparent; and data collection has to follow specified, explicit, and legitimate purposes and should not be processed further in a manner incompatible with those purposes.

10 It is important to note that the empirical analysis concentrates on the time period during which hessenDATA was framed as a project, and regulatory challenges were identified and addressed. Whether these conflicts will persist over time, depends upon various factors such as litigation and political trends.

11 At the same time, there are respects in which Palantir Gotham differs from social media platforms: There is no massive user-created content, as in social media, as the users (police officers) are less numerous and are also extensively certified and trained. Dealing with unwanted user-generated content is therefore not the central problem here.

12 The "Fuck-the-algorithm" protests in the UK in 2020 were a more recent example; the "Freiheit-statt-Angst" [freedom instead of fear] demonstrations in German cities from 2006 to 2015 were an older example.

References

Aguilera T, Artioli F and Colomb C (2021) Explaining the diversity of policy responses to platform-mediated short-term rentals in European cities: A comparison of Barcelona, Paris and Milan. *Environment and Planning A: Economy and Space* 53(7): 1689–1712.

Amoore L (2013) *The Politics of Possibility: Risk and Security beyond Probability*. Durham: Duke University Press.

Andersson Schwarz J (2017) Platform logic: An interdisciplinary approach to the platform-based economy. *Policy & Internet* 9(4): 374–394.

Anstis S (2021) Government procurement law and hacking technology: The role of public contracting in regulating an invisible market. *Computer Law & Security Review* 41: 105536.

Aradau C and Blanke T (2015) The (big) data-security assemblage: Knowledge and critique. *Big Data & Society* 2(2): 1–12.

Bayerisches Landeskriminalamt (2022) *Noch erfolgreichere Polizeiarbeit - Zuschlag für neues Recherche- und Analysesystem der Bayerischen Polizei: Höchste Ansprüche an Datensicherheit und Datenschutz*. 7 March. Available at: https://www.polizei.bayern.de/aktuelles/pressemitteilungen/025971/index.html (accessed 24 February 2022).

Bellanova R and De Goede M (2022) The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance* 16(1): 102–118.

Beverungen A (2021) Kybernetischer kapitalismus? Amazon, algorithmisches management und aneignung. In: Daum T and Nuss S (eds) *Die Unsichtbare Hand des Plans: Koordination und Kalkül im Digitalen Kapitalismus*, 1st ed. Berlin: Dietz Vlg Bln, 95–109.

Bigo D (2020) Interoperability: A political technology for the datafication of the field of EU internal security? In: Bigo D, Diez T, Fanoulis E, et al. (eds) *The Routledge Handbook of Critical European Studies*, 1st ed. Abingdon, Oxon; New York, NY: Routledge, 400–417. Available at: https://www.taylorfrancis.com/books/9780429957505 (accessed 22 September 2023).

Bigo D, Carrera S, Gonzáles Fuster G, et al. (2011) Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament. Brussels.

Bloch-Wehba H (2021) Visible policing: Technology, transparency, & democratic control. *California Law Review* 109(3): 917–978.

Bloch-Wehba H (2022) Algorithmic governance from the bottom up. *Brigham Young University Law Review* 49(1): 69–136.

Borges G (2023) Liability for AI systems under current and future law: An overview of the key changes envisioned by the proposal of an EU-directive on liability for AI. *Computer Law Review International* 24(1): 1–8. Verlag Dr. Otto Schmidt.

Bossong R and Wagner B (2017) A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change* 67(3): 265–288.

Bovaird T (2004) Public–private partnerships: From contested concepts to prevalent practice. *International Review of Administrative Sciences* 70(2): 199–215.

boyd d and Crawford K (2012) Critical questions for big data. *Information, Communication & Society* 15(5): 662–667.

Brayne S (2017) Big data surveillance: The case of policing. *American Sociological Review* 82(5): 977–1008.

Brayne S (2021) *Predict and Surveil: Data, Discretion, and the Future of Policing*. New York, NY: Oxford University Press.

Brigham K (2020) Palantir is going public after 17 years — here's what it does and why it's been controversial. Available at: https://www.cnbc.com/2020/09/20/palantir-secretive-data-mining-firm-goes-public.html (accessed 31 January 2023).

Brühl J (2018) Palantir in Deutschland: Wo die Polizei alles sieht. *Süddeutsche Zeitung*, 18 October. Frankfurt ; München. Available at: https://www.sueddeutsche.de/digital/palantir-in-deutschland-wo-die-polizei-alles-sieht-1.4173809 (accessed 24 February 2022).

Bundesverfassungsgericht (2023) Legislation in Hesse and Hamburg regarding automated data analysis for the prevention of criminal acts is unconstitutional. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2023/bvg23-018.html.

Chafkin M (2021) *The Contrarian: Peter Thiel and Silicon Valley's Pursuit of Power*. New York: Penguin Press, an imprint of Penguin Random House LLC.

Chan NK and Kwok C (2022) The politics of platform power in surveillance capitalism: A comparative case study of ride-hailing platforms in China and the United States. *Global Media and China* 7(2): 131–150.

Christensen KK and Petersen KL (2017) Public–private partnerships on cyber security: A practice of loyalty. *International Affairs* 93(6): 1435–1452.

Colangelo G and Maggiolino M (2018) Data accumulation and the privacy–antitrust interface: Insights from the Facebook case. *International Data Privacy Law* 8(3): 224–239.

Colomb C and Moreira de Souza T (2023) Illegal short-term rentals, regulatory enforcement and informal practices in the age of digital platforms. *European Urban and Regional Studies*: 09697764231155386. DOI: 10.1177/096977642311553.

Dencik L, Hintz A, Redden J, et al. (2018) *Data Scores as Governance: Investigating uses of Citizen Scoring in Public Services. [Project Report]*. Cardiff University, UK: Open Society Foundations. Available at: http://orca.cf.ac.uk/117517/ (accessed 30 March 2019).

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (2022) Analyse-Software der Hessischen Polizei vor dem Bundesverfassungsgericht. Available at: https://datenschutz.hessen.de/presse/analyse-software-der-hessischen-polizei-vor-dem-bundesverfassungsgericht.

Dourish P (2016) Algorithms and their others: Algorithmic culture in context. *Big Data & Society* 3(2): 1–11.

Egbert S (2019) Predictive policing and the platformization of police work. *Surveillance & Society* 17(1/2): 83–88.

European Commission (n.d.) The Digital Services Act package. Shaping Europe's digital future. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (accessed 26 April 2021).

Ferguson AG (2017) *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: NYU Press.

Gates K (2019) Policing as digital platform. *Surveillance & Society* 17(1/2): 63–68.

Gillespie T (2010) The politics of 'platforms'. *New Media & Society* 12(3): 347–364. SAGE Publications.

Gillett R, Stardust Z and Burgess J (2022) Safety for whom? Investigating how platforms frame and perform safety and harm interventions. *Social Media + Society* 8(4): 20563051 221144315. SAGE Publications Ltd.

Gorwa R (2019) What is platform governance? *Information, Communication & Society* 22(6): 854–871.

Gorwa R (2021) Elections, institutions, and the regulatory politics of platform governance: The case of the German NetzDG. *Telecommunications Policy* 45(6). DOI: 10.1016/j.telpol.2021.102145.

Gorwa R, Binns R and Katzenbach C (2020) Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society* 7(1): 2053951719897945. SAGE Publications Ltd.

Große-Bley J and Kostka G (2021) Big data dreams and reality in Shenzhen: An investigation of smart city implementation in China. *Big Data & Society* 8(2): 20539517211045171. SAGE Publications Ltd.

Helberger N (2020) The political power of platforms: How current attempts to regulate misinformation amplify opinion power. *Digital Journalism* 8(6): 842–854. Routledge.

Hessischer Landtag (2019a) Kleine Anfrage Torsten Felstehausen (Die Linke) Teil 1 und Antwort Minister des Innern und für Sport. Drucksache 20/660. Available at: https://starweb.hessen.de/cache/DRS/20/0/00660.pdf.

Hessischer Landtag (2019b) Zwischenbericht des Untersuchungsausschusses und Abweichende Berichte. Drucksache 19/6864. Available at: https://starweb.hessen.de/cache/DRS/19/4/06864.pdf.

Hessisches Ministerium für Inneres und Sport (2018) *Jahresbilanz* 2018. Jahresbericht, December. Wiesbaden: Hessisches Ministerium des Innern und für Sport. Available at: www.innen.hessen.de (accessed 17 March 2023).

Hildebrandt M (2020) *Law for Computer Scientists and Other Folk*. Oxford, New York: Oxford University Press.

Iliadis A and Acker A (2022) The seer and the seen: Surveying Palantir's surveillance platform. *The Information Society* 38(5): 334–363.

Jori A (2015) Shaping vs applying data protection law: Two core functions of data protection authorities. *International Data Privacy Law* 5(2): 133–143.

Koop C and Lodge M (2017) What is regulation? An interdisciplinary concept analysis. *Regulation & Governance* 11(1): 95–108.

Kuckartz U and Rädiker S (2023) *Qualitative Content Analysis: Methods, Practice and Software. Second*. Thousand Oaks: Sage Publications.

Landeskriminalamt Nordrhein-Westfalen (2020) LKA-NRW: Polizei NRW setzt bei Verbrechensbekämpfung und Gefahrenabwehr zukünftig neue Analysetechniken ein. Available at: https://www.presseportal.de/blaulicht/pm/58451/4490593.

Landtag Nordrhein-Westfalen (2021) Sitzung des Innenausschusses am 15.04.2021 Antrag der Fraktion Bündnis 90/Die Grünen vom 01.04.2021 „Aktueller Sachstand zur Soft are Gotham-Palantir - Vorlage 17/5078. Available at: https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-5078.pdf.

Laurer M and Seidl T (2021) Regulating the European data-driven economy: A case study on the general data protection regulation. *Policy & Internet* 13(2): 257–277.

Mazur J and Serafin M (2023) Stalling the state: How digital platforms contribute to and profit from delays in the enforcement and adoption of regulations. *Comparative Political Studies* 56(1): 101–130.

Medzini R (2022) Enhanced self-regulation: The case of Facebook's content governance. *New Media & Society* 24(10): 2227–2251. SAGE Publications.

Möllers N (2021) Making digital territory: Cybersecurity, technonationalism, and the moral boundaries of the state. *Science, Technology, & Human Values* 46(1): 112–138.

Munn L (2018) *Ferocious Logics: Unmaking the Algorithm*. DE: meson press. Available at: https://doi.org/10.14619/1402 (accessed 1 December 2022).

Palantir (2020a) Data protection in Palantir Foundry. Available at: https://medium.com/palantir/data-protection-in-palantir-foundry-5ab9f346195 (accessed 24 February 2022).

Palantir (2020b) Palantir is not a data company (Palantir Explained, #1). In: *Palantir Blog*. Available at: https://medium.com/palantir/palantir-is-not-a-data-company-palantir-explained-1-a6fcf8b3e4cb (accessed 24 February 2022).

Pasquale F (2015) *The Black Box Society. The Secret Algorithms That Control Money and Information*. Berlin, Boston: Harvard University Press. Available at: https://www.degruyter.com/view/product/430038 (accessed 26 April 2018).

Rieder B and Hofmann J (2020) Towards platform observability. *Internet Policy Review* 9(4). DOI: 10.14763/2020.4.1535.

Siapera E and Viejo-Otero P (2021) Governing hate: Facebook and digital racism. *Television & New Media* 22(2): 112–130. SAGE Publications.

Siefken ST (2018) *Parlamentarische Kontrolle Im Wandel: Theorie Und Praxis Des Deutschen Bundestages. 1. Auflage. Studien zum Parlamentarismus 31*. Baden-Baden: Nomos.

Srnicek N (2016) *Platform Capitalism*. Cambridge Malden, MA: Polity.

Taylor L, Sharma G, Martin A, et al. (eds) (2020) *Data Justice and Covid-19: Global Perspectives*. London: Meatspace Press.

Ulbricht L (2018) When big data meet securitization. Algorithmic regulation with passenger name records. *European Journal for Security Research* 3(2): 139–161.

Ulbricht L (2020) Scraping the demos. Digitalization, web scraping and the democratic project. *Democratization, Special Issue Democratization Beyond the Post-Democratic Turn. Political Participation Between Empowerment and Abuse* 27(3): 426–442.

Vallas S and Schor JB (2020) What do platforms do? Understanding the gig economy. *Annual Review of Sociology* 46(1): 273–294.

van Dijck J (2013) *The Culture of Connectivity: A Critical History Of Social Media*. Oxford ; New York: Oxford University Press.

van Dijck J, Poell T and Waal Md (2018) *The Platform Society: Public Values in a Connective World*. New York: Oxford University Press Inc.

van Dijk N, Tanas A, Rommetveit K, et al. (2018) Right engineering? The redesign of privacy and personal data protection. *International Review of Law, Computers & Technology* 32(2–3): 230–256.

Voigts H (2023) Hessen: Eine Gesetzesreform für die Weiternutzung von „Palantir". *Frankfurter Rundschau*, 21 February. Available at: https://www.fr.de/rhein-main/landespolitik/hessen-eine-gesetzesreform-fuer-die-weiternutzung-von-palantir-92101651.html.

Wilson D (2017) Algorithmic patrol. The futures of predictive policing. In: Završnik A (ed) *Big Data, Crime and Social Control. 1st ed*. Cham, Switzerland: Routledge, 108–127. Available at: https://www.taylorfrancis.com/books/9781315395777 (accessed 9 May 2020).

Wilson D (2021) The new platform policing. In: Završnik A and Badalič V (eds) *Automating Crime Prevention, Surveillance, and Military Operations*. Cham, Switzerland: Springer International Publishing, 47–68. Available at: https://link.springer.com/10.1007/978-3-030-73276-9_3 (accessed 18 November 2022).

Yates L (2023) How platform businesses mobilize their users and allies: Corporate grassroots lobbying and the airbnb 'movement' for deregulation. *Socio-Economic Review* 21(4): 1917–1943.

Zierer M, Kartheuser B, Schöffel R, et al. (2023) Bund rückt von Software Palantir ab. *tagesschau.de*. Available at: https://www.tagesschau.de/investigativ/br-recherche/palantir-software-analyse-polizei-100.html.

Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.