Eireiner, Anna Verena

Article

Imminent dystopia? Media coverage of algorithmic surveillance at Berlin-Südkreuz

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Eireiner, Anna Verena (2020) : Imminent dystopia? Media coverage of algorithmic surveillance at Berlin-Südkreuz, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 9, Iss. 1, pp. 1-19, https://doi.org/10.14763/2020.1.1459

This Version is available at:
https://hdl.handle.net/10419/216224

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 1

Imminent dystopia? Media coverage of algorithmic surveillance at Berlin-Südkreuz

Anna Verena Eireiner
University of Cambridge, United Kingdom, ave23@cam.ac.uk

Published on 30 Mar 2020 | DOI: 10.14763/2020.1.1459

Abstract: Facial-recognition software continues to create heated controversy, as illustrated by a year-long pilot run at the Berlin-Südkreuz train station. The test run at one of Berlin's main arteries was a catalyst for media attention, spurring heated discourse on the efficiency and legitimacy of surveillance technology. Drawing on a critical discourse analysis and (post-)panoptic theory, this paper investigates how the relationship between the public and the state is represented, how automated surveillance technology is linguistically framed and which problematisations were associated with the technology deployed during the 2017 pilot.

Keywords: Science and technology studies (STS), Algorithmic surveillance, Discourse analysis, (Post-)panoptic theory, Facial recognition software

Article information

Received: 11 Aug 2019 **Reviewed:** 21 Jan 2020 **Published:** 30 Mar 2020

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/imminent-dystopia-media-coverage-algorithmic-surveillance-berlin-sudkreuz

Citation: Eireiner, A. V. (2020). Imminent dystopia? Media coverage of algorithmic surveillance at Berlin-Südkreuz. *Internet Policy Review*, *9*(1). DOI: 10.14763/2020.1.1459

INTRODUCTION

Mass-casualty terrorism, migration sparked by raging conflicts and humanitarian crises, and transnational corporate crime give rise to another era of unpredictability. Amid these global challenges, national governments are tasked with providing defence and security of the state, its citizens, institutions, and economy. In a quest to live up to this challenge, recent technological advancements seem to offer promising solutions and are often justified as a means to regain control. One of the most popular tools in this context are surveillance technologies, which are certainly not novel. Yet, the recent strikes towards automation open up unforeseen possibilities. Facial recognition software, for instance, enables the identification of individuals from a picture or video. While 'facial recognition' has become a catch-all term, it should be noted that facial

recognition systems scan a person's face in an attempt to match it against a database, while facial detection systems simply scan for the presence of faces (Roux, 2019).

Surveillance technologies, particularly facial recognition software, get heavily promoted through national and EU funded programmes (Moorstedt, 2017). They are not only promoted as a solution to globalised crime but also as a boost to the growing EU security economy (Möllers & Hälterlein, 2013; OECD, 2004, p. 21). On the hunt for a panacea, it is easy to overlook that the creation and implementation of algorithms is not just the essence of mathematics. It is a social practice. Accordingly, the technological wiring of infrastructure through surveillance technology is a deeply social endeavour. Science and Technology Studies (STS) scholars make important contributions to the exposure of the complex social, political and cultural dimensions that questions of science and technology entail (Jasanoff, 2005; Tiles & Oberdiek, 1995; Verbeek, 2011; Winner, 1980). Technologies are often framed as the answer to security threats but are prone to creating a myriad of other issues. In the light of these complexities, STS offers compelling conceptual lenses, which can help foster comprehensive debates at the intersection of science, technology, and the field of security studies (for a more in-depth discussion on this intersection see Binder, 2016).

Discourse analysis is a valuable entry point to controversies on emerging technologies, as verbal texts provide important insights into the underlying socio-political currents. News reports, feature articles and commentary pieces are accessible sources for analysing the reception of new technologies, as well as the construction of identities, risks, threats and imaginaries of desirable futures.

In line with how STS scholars approach their object of study, this paper discusses the first phase of a pilot project of facial recognition technology at Berlin's railway station Südkreuz, which was carried out from August of 2017 to July 2018. The project was initiated by the Ministry of the Interior, federal and state police and is supported by the incumbent German railway company Deutsche Bahn (Bundesministerium des Inneren, 2017; Horchert, 2017). The pilot project at Südkreuz quickly became a catalyst for media attention, spurring discourse on the efficiency and legitimacy of surveillance technology in the commentary, technology and politics sections of newspapers and online magazines and blogs. The headlines of the coverage of the pilot project in major outlets like Spiegel Online and Süddeutsche Zeitung read "Orwell and Kafka meet at the train station" (Stöcker, 2017) and "they see us"[1] (Moorstedt, 2017). These headlines already hint at implications of structural power, which have a distinct presence throughout this discourse. This paper draws on discourse analysis to point out how the relationship between the public and the state is represented, how automated surveillance technology is linguistically framed and which problematisations were associated with the technology deployed at Berlin-Südkreuz.

First, I will go into the details of my approach to discourse analysis. To enable the sense-making process that is discourse analysis, I will introduce the broader socio-political context by briefly describing the relationship between the state and surveillance technology in Germany. I will also retrace the modalities and challenges that emerged with the pilot project at Berlin-Südkreuz. This is followed by discourse analysis, in which I introduce and interpret the linguistic representation of Berlin-Südkreuz in media discourse. Finally, I will then situate algorithmic surveillance within (post-)panoptic theory and show how the case at hand relates to the work of one of the most important post-panoptic theorists, Shoshana Zuboff (1988).

METHODOLOGY

As mentioned before, understanding (surveillance) technology as a social practice is of utmost importance. This corresponds with STS' interest in the cultural, political and social conditions under which technology, in this case, automated surveillance technology, is developed (Jasanoff, 2005, p. 248). Discourse analysis is most often employed to analyse how written text affects the reader and can help us understand how social reality is produced (Evans, 2013; Phillips & Hardy, 2002, p. 6).

With the rapid development and implementation of increasingly sophisticated surveillance technologies, it is perhaps unsurprising that the social, cultural and political impacts of these technologies have become a topic of lively debate (see Lyon, 2007). From an STS viewpoint, these debates are a cornerstone in the construction of security, threats and new surveillance technologies and, more generally speaking, the co-production of science and social order (Jasanoff, 2004). Media reports, policy briefings, commentary pieces and other verbal texts provide accessible and highly valuable resources for the analysis of sociotechnical imaginaries. Sociotechnical imaginaries can be defined as "collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order, attainable through, and supportive of, advances in science and technology" (Jasanoff, 2015, p. 4). The linguistic framings and symbolic elements in documents and other verbal forms of representation are a crucial element in the (re)production of sociotechnical imaginaries (STS Research Platform, 2018). A close study of the coverage on the trial run at Berlin-Südkreuz gives an insight into how science and technology can spark different associations and responses while invoking and challenging different visions of (un)desirable futures. While this explorative study does not aim to identify specific imaginaries, it provides a first exploration of how this project is linguistically framed and envisioned in and through media discourse. The goal of this paper is to provide some insight into the emerging social, technical and political realities of surveillance technology, complex power relations and their representation through language.

The underlying assumption is that in discourse, objects are not represented but systematically produced. In the sociological terms of SKAD (Sociology of Knowledge Approach to Discourse), discourses are knowledge that form patterns of interpretation and action. Sharing knowledge through discourse shapes interpretations and our everyday practices: some might agree with the application of surveillance technology, others might engage in protest. What is included in and what is excluded from discourse becomes important. Which voices are powerful and can be heard and which cannot? How are truth-claims and discursive identities constructed? (Schneider, 2013a). This paper draws on the analysis of communication around the controversy at hand to illuminate some of these questions. It is compelling to study the quite creative linguistically frames and rhetorical features, carefully filigreed representations of realities. In this regard, newspapers and other media outlets are an important discursive domain, shaping the patterns of interpretation and action (Schneider, 2013b).

This critical discourse analysis follows a text-based approach, drawing on media coverage of the policy discourse around the adaption of algorithmic surveillance technology at Berlin-Südkreuz.[2] All materials are online publications from February 2017 to November 2018 in German language. In this period the pilot was first announced to the public, the year-long project was carried out and finally, in the fall of 2018, the results were published. This analysis codes the linguistic representation of (1) automated surveillance technology, (2) the relationship

between the state and the public and (3) the problematisations associated with both. This exploratory discourse analysis draws on thirty-one news articles, commentary pieces and blog posts from a variety of national, regional and online-only outlets. These sources include more critical stances towards the issue (Süddeutsche Zeitung, Spiegel Online, Netzpolitik.org, Deutsche Welle (DW), Zeit Online), a comparatively moderate position (Berliner Zeitung, Der Tagesspiegel, Morgenpost, Welt) and four with a popular scientific focus (Spektrum, Heise Online, Computer Bild, Wissen.de). Additionally, the analysis included posts on blogs that are more or less loosely centred around the topics of data protection, privacy and security (datenschutz notizen, Datenschutzbeauftragter INFO, digitalcourage.org, IT-Security@Work, law blog, TEXperimenTales) and contributions by online outlets with a focus on digital technologies (tarnkappe.info, Gründerszene). Other articles were published in regional publications (Märkische Allgemeine Zeitung, QIEZ). These sources were selected with the assumption that they each might present the Südkreuz-project in different ways and with different foci. A blog on information security might offer a different perspective than a regional newspaper. Some outlets heavily covered the unfolding of the pilot project and were included in the analysis with more than one text. Although the analysis spans a variety of outlets, the results show that the pilot was generally critically portrayed and represented in a similar fashion. Although the selected sources only represent a small proportion of the many news reports, feature articles, editorials, columns, opinion pieces and blog posts that were published on this topic, they offer an insight into the linguistic framings that characterised the discourse. Thus, this first explorative study offers a baseline for further investigations into the controversy around the Berlin-Südkreuz pilot project.

SURVEILLANCE TECHNOLOGY AND THE STATE

In Germany, as in other countries, the government is the driving force behind the adoption and development of surveillance technologies. The advancements in automated or "smart" surveillance technologies are still recent; thus, no common term has been established. This is partly due to the many new applications, e.g., prediction of criminal behaviour or traffic jams or facial recognition and the move out of local databases into networked systems (Galič et al., 2016; Roßnagel et al., 2011). The terms that are commonly implied in this context include "smart CCTV", "second generation CCTV" and "algorithmic surveillance" (Musik, 2011). I will use the term "algorithmic surveillance". It captures the nature of these systems, which use algorithms to interpret, combine and aggregate data, best.

The Ministry of the Interior, as well as federal and national police, are responsible for the protection of internal security and the provision of policing. Surveillance technologies tend to be justified as resources that enable the state to live up to its responsibility to provide security; as in preventing or reducing harm. In Germany, surveillance tools are increasingly developed and adapted as policing tools. The German Ministry of Education and Research is heavily investing in their development. So are various federal policing institutions across Germany, which run in-house research projects (Möllers & Hälterlein, 2013, p. 60). Additionally, the EU research projects P-REACT and INDECT explore how surveillance systems may be employed to detect criminal activity (European Commission, 2016; European Commission, 2017).

The state is expanding the legal framework to enable algorithmic surveillance. The adoption of biometric databases through the 'e-Pass', is the first strike toward the large-scale acquisition of biometric data (Oepen, 2013). Since May 2017, federal and national security agencies can access the database (Reuter, 2017a). In March 2017, a law

("*Videoüberwachungsverbesserungsgesetz*") was passed to extend the deployment of video surveillance and the possibilities for usage and transmission (Reuter, 2017a).

Nonetheless, the algorithmic surveillance software at Berlin-Südkreuz is most probably, if not certainly, in conflict with the current legal framework (Reinsch, 2017). Under German law, individuals are granted the right to informational self-determination, which refers to "the capacity of the individual to determine in principle the disclosure and use of his/her personal data" (BVerfGE 65, 1). This ruling is the "constitutional anchor for data protection" (Hornung & Schnabel, 2009, p. 4) and internationally unparalleled.

Nonetheless, the infrastructure is expanded for larger-scale public surveillance. In Germany, 900 train stations are already equipped with about 6000 CCTV cameras (Deutscher Bundestag, 2019). The pilot project at Berlin-Südkreuz, which I will outline in the next paragraph, is aimed at exploring the capabilities of the newest technological options (Stöcker, 2017).

A PANACEA? THE PILOT PROJECT AT BERLIN-SÜDKREUZ

Berlin-Südkreuz, located just south of the German capital's city centre, connects the local subway to federal and national trains. During a year-long trial from August 2017 to July 2018, algorithmic surveillance software by three different manufacturers was added to the already employed CCTV (Bundesministerium des Inneren, 2018; Morgenpost, 2017). During this first trial period, each software's facial recognition features were tested to determine if algorithmic surveillance should be adopted permanently. The second stage of the trial commenced in the summer of 2019. Targeted towards additional applications, phase two included the detection of stray objects and dangerous situations, such as acts of violence and individuals in distress (Borchers, 2017; Lobe, 2017, p. 2).

The project was initiated by the Federal Police, the national railway company Deutsche Bahn, the Ministry of the Interior and the Federal Criminal Police Office. Especially Thomas de Maizière, former German Minister of the Interior, has pushed towards the implementation of the project (Käppner, 2017). At Südkreuz three different areas were marked with blue stickers and signs to inform passers-by about the employed software. One camera is pointed at an entranceway, another at an escalator and the third was pointed at an exit (Morgenpost, 2017). With each, a different software application was tested. The Ministry of the Interior first declined to disclose the manufacturers but then announced that the software applications employed are by the multinational corporation Dell, much smaller German security provider ELBEX and another German software company, L-1 Identity Solutions AG (Kurz, 2017).

Figure 1: An area in front of an escalator at the train station Berlin-Südkreuz is separated into two sections: Passers-by on the right hand side are captured by automatic face recognition (blue decal), or can elect to stay on the left and opt out (white decal). (Suthorn, 2017, cc-by-sa-4.0).

Facial recognition applications can identify a person using digital images or video material. Generally, there are two approaches. The first one draws on mapping facial features, or landmarks e.g., jaw, eyes, or nose that are analysed in relation to each other and then compared to images for a match. The second approach calculates the "essence" of a face. The specific value is different for each individual, thus becomes comparable (see Gallbally et al., 2014; Gates, 2011).

Three hundred volunteers were recruited to test different products (Käppner, 2017). A template was extracted from each participant's photograph, building a database (Lobe, 2017). Each volunteer carries a location-tracking transponder which helps to identify if the employed software successfully picked up and matched the individual passing through with the database. For their cooperation, each participant was compensated with a 25 Euro Amazon gift card. The individuals who crossed through most often were incentivised with additional prizes (e.g., Apple watches). The selection of incentives sparked some controversy (Horchert, 2017).

In this context, it is noteworthy that identifying specific individuals within a crowd always implies that there are individuals within a reference group. Thus, the distinction between participants and non-participants is precarious. Essentially every individual that passes through, volunteer or not, is picked up by the cameras and is thus a participant. Moreover, questions of informed consent emerged shortly after the project was rolled out. As it turns out, the volunteers were not informed about the scope of data that the transmitters could collect, which include not only location but other factors, e.g., speed and temperature (Kühl, 2017).

The goal of the project was to test if state-of-the-art algorithmic surveillance software works efficiently. In the long run, the idea is to employ systems that spot people in distress, stray potentially dangerous objects and suspicious behaviour of potential criminals

(Bundesministerium des Inneren, 2017; 2018). As for this specific pilot project, the Ministry of the Interior did not specify beforehand what would constitute "efficiency" and thus a successful pilot project (Reuter, 2017b). In the end, the Ministry of the Interior deemed the 2017 pilot successful (Bundesministerium des Inneren, 2018). According to the official test report, the employed systems identified participants with an accuracy of 80% (Bundesministerium des Inneren, 2018). The Ministry's claim sparked widespread criticism, as the accuracy rate of the various software employed during the trial's first phase ranged between a meagre 65,8% and 12%. Only the combination of the three different systems employed produced higher accuracy rates (Chaos Computer Club, 2018). Despite the controversy, the Ministry of the Interior commenced with the second phase of the Berlin-Südkreuz pilot project in 2019 (Vogt, 2019). In January 2020, the Ministry of the Interior announced that although the results of the pilot project seemed promising, facial recognition software would not immediately be adopted at German train stations and airports. Instead, the Ministry made plans to expand on video surveillance technology (CCTV) at train stations and in other public gathering spaces (Tagesschau, 2020). Although this turn of events does not indicate a significant change of policy agenda, the Ministry's hesitation towards the implementation of facial recognition software might be a response to the widespread public criticism. In this next section, I will give an insight into the media coverage that the controversial trial's first phase sparked.

DISCOURSE ANALYSIS

First, I will show how different authors present the project at Berlin-Südkreuz and point out the linguistic and rhetorical features, taking a close look at how they convey truth-claims and how they present power structures. For a better overview, I structured this section according to coding categories which consist of (1) the relationship between the public and the state, (2) the representation of automated surveillance technology, (3) the problematisations associated with both.

DISCURSIVE IDENTITIES: THE PUBLIC AND THE STATE

First, the identities that are constructed in and through media discourse are quite insightful. A Süddeutsche Zeitung title reads "they see us" (Moorstedt, 2017). A Berliner Zeitung author alludes to the opacity of the algorithmic surveillance employed, calling the project "trials […] in hiding" (Neumann, 2017). Other headlines read suggestively "police seeking volunteers for total surveillance" (Poschmann, 2017) and "go ahead, scan me" (Rabenstein, 2017). One author proclaims that the pilot project marks a "high point of audacity in the relationship between the German state and its citizens" and adds "he [Thomas de Mazière] must not get through with this" (Stöcker, 2017). In Süddeutsche Zeitung Käppner refers to "technology of control" (Käppner, 2017), while many others allude to the "surveillance state" (Reuter, 2017a; Stürzl, 2018) playing along similar lines of the state-citizen relationship.

A distinct boundary is drawn between the protagonists: those under surveillance ("us"), presumably the public or citizens; and those who are in control, the authorities or "they" (e.g., Hermes, 2017; Stürzl, 2018). Although, subtler, "technology of control" implies that there is one party in control and one that is being controlled (Käppner, 2017). These linguistic acts construct two discursive identities. This is referred to as antagonism, constituting an opposing, even hostile, relationship between two subjects. Each subject is attributed to a specific identity, where one is determinately dominating the other (Fontanille, 2006). In critical discourse analysis (CDA), these instances are also referred to as oppositions, as in the creation of opposition

through linguistic frames (Evans, 2013).

Across the articles and blog posts, it is difficult to pinpoint the exact agency of the antagonist(s). It particularly remains unclear, who “they” are, presumably because of the indistinct responsibility distribution across different institutions. Thus, authors sometimes refer to the state, the Ministry of the Interior, the federal criminal police office and/or Deutsche Bahn (Lobe, 2017; Moorstedt, 2017; Morgenpost, 2017; Stöcker, 2017). The opposition will appeal to the readers who will most likely feel drawn to identify with the protagonist “us”, the public, the citizens. The proclamation “he [Thomas de Maizière] must not get through with this” is an appeal for solidarity, a call for collective action (Stöcker, 2017). These antagonisms, as a linguistic twist, imply asymmetrical power-relations and create opposition through language.

THE UNOBSERVABLE OBSERVER

A prominent aspect of linguistic representation is the variety of terms that are used to describe the technology employed at Südkreuz. Therefore, I examined naming, the analysis of nouns as the “units of language that name things in the world” (Evans, 2013). Through naming existence is assumed. If we call something “technology of control” (Käppner, 2017) we presuppose that it exists (Evans, 2013).

Naming varies, often within the same text, from “cameras” (Antonia, 2017; Horchert, 2017; Kühl, 2017; Moorstedt, 2017) to “the system” (Morgenpost, 2017; Stöcker, 2017; Wissen.de, 2018) to “a computer” (Moorstedt, 2017; Morgenpost, 2017), “future technology” (Schmiechen, 2017) or simply “software” (Dr. Datenschutz, 2018; Hummel, 2017; Morgenpost, 2017; Rieblinger, 2017). It is also insightful to consider the attributes that the authors assign to the employed technology. Adjectives range from “magical” (Stöcker, 2017), which mystifies the technology, to "relentless" (Lobe, 2017), "weapon-grade" (Moorstedt, 2017) and “totalitarian” (Schmidt, 2017), which convey that algorithmic surveillance poses a threat. “Staring” (Moorstedt, 2017), “face- and behaviour-scanner” (Reuter, 2017b) “autonomous” (Breyton, 2017), “intimidating” (Law Blog, 2017), “scrutinising” (Simon, 2017) and “all-seeing and always alert” (Stöcker, 2017), convey the Orwellian dystopia of pervasive systems that exercise discipline and control. Käppner reminds the reader that “The Thousand Eyes of Dr. Mabuse” might become a reality (Käppner, 2017). To the reader, this may sound like a warning. “Intelligent” (Borchers, 2017; Conrad, 2017; Horchert, 2017; Kurpjuweit, 2017; Lobe, 2017; Moorstedt, 2017) on the other hand is an adjective that is often employed in this context to communicate the innovative nature of the system. In this case, a system that does not only collect but also interpret, combine and aggregate data. Ultimately, these adjectives do not necessarily draw a positive picture of the employed technology. The ideological potencies of these adjectives are striking, especially considering that the authors seem to struggle to find a suitable term to capture the employed technology.

In fact, a lack of fitting terminology is characteristic of autonomous systems. They can hardly be captured in words, as technology disappears from the front end (cameras, control rooms) into the back end (algorithms) (see Galič et al., 2016; Roßnagel et al., 2011). Presumably, the many different applications and functions of automated surveillance technology add to these difficulties. There are software applications, motion analysis, and facial recognition, object tracking, options for classifications and predictions. Referring to "the system" or "intelligent software" are ways to linguistically capture these facets. There are also attempts to capture the material hardware components into words, referring to what we can observe: "intelligent cameras" (Moorstedt, 2017; Poschmann, 2017; Stürzl, 2018) or “computers” (Moorstedt, 2017; Morgenpost, 2017).

Another linguistic twist in this context are personifications, which are "metaphorical representation, common to literary texts, whereby nonhuman objects are ascribed human attributes or qualities" (Baker & Ellece, 2011, p. 60). Examples include the observation that "systems are not faultless but they can learn at a frightening speed" (Moorstedt, 2013) or that there are now "objects that stare at us" (Moorstedt, 2017) and an "all-seeing, always alert digital guard" (Stöcker, 2017). With the trend towards algorithmic surveillance, their technological focus shifts ways from cameras and human pendants in the control room. What can be grasped under the term algorithmic surveillance describes the move towards autonomous computer-based surveillance, where algorithms take over the formerly human task of analysis and interpretation (see Norris & Armstrong, 1999). The "unobservable observer" is characterised by subtle frontends and black-boxed algorithms. Those who come in touch with the system can hardly make sense of the technology. The diffusion and automation, and with that a sense of mystification and alienation, of surveillance technology, is communicated through language. The employed adjectives and personifications leave the impression that the technology has assumed agency; control over these surveillance systems seems like an illusion, conveying a sense of urgency.

PROBLEMATISATIONS: DISCIPLINE AND CONTROL

The ubiquitous, intangible nature of the surveillance systems in question could be a key point to the speculative nature in which this discourse is held. This discourse is characterised by modalities, which do not necessarily refer to reality, but contingencies or possibilities. They express information "about what could be or must be the case, as opposed to being about what actually is the case" (Swanson, 2008, p. 1193).

One fear is central to the debate and frequently found throughout media coverage, which is assumptions concerning the transfer of discipline and control to an automated process. Most authors did at least touch upon the (in)capabilities of algorithms to classify facial expressions, movements, interactions and to enable authorities to exercise discipline and control based on these interpretations, which is commonly referred to as predictive policing (Perry et al., 2013). Süddeutsche Zeitung author Moorstedt questions the capabilities of a computerised interpretation of our world. The author remarks, "a hug in front of an ICE_3 that is almost leaving the station could look like a brawl to the computer. Those who run on the platform, trying to catch the train, will possibly be marked as on the run" (Moorstedt, 2017). In a blog post, one calls for putting a stop to a trial that turns Berlin-Südkreuz into a "bewilderment train station" (Demuth, 2017). In Spiegel Online, the author speculates about the emergence of "a magic system of artificial intelligence and real-time data collection, which one day will predict who will do evil next" (Stöcker, 2017). The author refers to predictive policing, the algorithmic capabilities to detect and predict potential criminal activity. In the Süddeutsche Zeitung article, the fear of predictive policing through algorithms is expressed through rhetorical questions, which add dramatic quality, emotionally engaging the reader: "What will life look like in times of intelligent cameras, where one is not only always watched but also always evaluated?" (Moorstedt, 2017). The author answers promptly: "One ought to behave as unsuspicious as possible" (Moorstedt, 2017). This rhetorical twist raises the reader's curiosity. The answer is phrased like an ominous wake-up call. Playing along similar lines, the Süddeutsche Zeitung reader is reminded that "everyone is initially suspicious" (Kühl, 2017). Some interpretations go even further: "Algorithmic pattern recognition raises the question of who defines criminality and if police power is impermissibly delegated to machines" (Lobe, 2017). The author suggests that algorithms could define criminality, traditionally a responsibility of the judiciary, which interprets the law, or the legislative that passes them. "Interpretation of criminality" could also refer to a situational interpretation of the legitimacy of acts, an executive task. Interestingly, the

author speaks about delegation of "police power", instead of sheer police work, which would be a more fitting term for mere interpretative algorithmic tasks. Accordingly, the algorithm is not only staged as a computerised process of police supervision. The authors convey that algorithms could not only be used to support law enforcement but ultimately become law enforcement. This is carried to the extreme, evoking dystopian visions about Kafkaesque or Orwellian dystopias and the proclamation that "dystopia threatens to become reality" (Moorstedt, 2017).

Some of the headlines read “Orwell and Kafka meet at the train station” (Stöcker, 2017) and “Big Brother at the train station” (Morgenpost, 2017). Along the same lines, one author asserts "Big Brother is installed at the train station" (Prantl, 2017). In Morgenpost, the totalitarian visions are phrased more subtly. Regarding the recent expansion of surveillance technologies in Germany, the Morgenpost reader is soberly reminded that "facial recognition software already opens up unforeseen opportunities in many dictatorships" (Morgenpost, 2017). These linguistic frames, suggesting dystopian visions, in which those in control use algorithmic surveillance to exercise totalitarian control, privilege one understanding of reality over another. The reader is left with these unsettling speculations about a future of algorithmic discipline and control.

In these articles, the value judgements elicit emotion, while the authors speculate about the possibilities of the technology employed at Berlin-Südkreuz in modalities. The oppositions convey asymmetrical power-relations: there is one party who is controlled and one who exercises control.

The various terms that are applied in this context attempt to capture the pervasive, diffuse nature of algorithmic surveillance. The added adjectives convey associations of autonomous, threatening technology. The employed personifications add to this picture, technology has seemingly assumed agency. The problematisations mainly expressed through modalities point at associated uncertainties about the future. The main themes are speculations about predictive policing and the effectiveness of algorithms to appropriately interpret behaviour and associated worries that it will become necessary to correctly anticipate behaviour to not raise suspicion. This is further escalated, with visions of algorithmic law enforcement and dystopian visions of the future.

This analysis can give us some insight into the arguments, or truth-claims, that are put forward into this context. The critical tone that I found in varying degrees throughout all articles and blog posts does however not imply that there is a societal opposition to the adoption of automated surveillance technology; it just gives us a glimpse into some discursive frames, wider social practices and the negotiation processes that the pilot project spurs. This next section details how (post-)panoptic theory can be utilised to illuminate the topic of algorithmic surveillance technology.

MOVING BEYOND THE PANOPTICON

In the following paragraphs, I want to situate this case, and algorithmic surveillance more generally, within post-panoptic social theory, drawing on the conceptual threads that Shoshana Zuboff (1988) derived from her empirical work. To this end, I will briefly retrace the panoptic journey from its origins to post-panoptic theory.

The headlines suggest how influential different conceptualisations and ideas of surveillance are in this discourse. Kafka and Orwell would certainly be astonished to see recent developments in surveillance technology. In scholarly discourse, two other names, Bentham and Foucault, still impact how scholars think and conceptualise surveillance technology today. Bentham and his ideas on the architectural implementation of surveillance can be regarded as a starting point for surveillance studies. Bentham's younger brother first invented the Panopticon, a circular prison building with a large control tower in the central yard. Stories of prison cells line the rounded walls. Occupants cannot see each other as they are divided by walls. Yet, they can always be watched from within the control tower. The central tower is equipped with lights that hinder the occupants from knowing whether they are being watched or not (Galič et al., 2016, pp. 12-13).

This idea of spatial, passive control was later theoretically refined by Foucault in Discipline and Punish (Foucault, 1995). He used the Panopticon as a metaphor to analyse mechanisms of social control and relations to power and knowledge. Foucault notes how the Panopticon allows for power to become anonymous, as occupants can be efficiently controlled without necessarily being watched. Those "subjected to a field visibility [...] simultaneously play both roles" they become the principle of their subjection (Foucault, 1995, pp. 202-203). With the emergence of the internet, surveillance lost the Panopticon's physical and spatial characteristics. Surveillance is turned into a networked part of the infrastructure. The physical, if hypothetical, prison guard becomes abstract; the metaphor flawed.

Many scholars have made important contributions to the study of contemporary distributed forms of surveillance. Noteworthy theoretical frameworks come from Deleuze, Kallinikos, and Zuboff, among others (Deleuze, 1992; Kallinikos, 2004 & 2007; Zuboff, 1988). These authors, however, all work with different takes on moving beyond the panopticon.

In Smart Machine, Zuboff makes an astonishing empirical and theoretical contribution to surveillance as a means of managerial control. Zuboff (1988) studied the transformation of blue- and white-collar work through the application of information technology within corporations. Surprisingly, her ideas are still relevant today, almost 30 years later. Yet, many of Zuboff's conceptualisations need to be adapted if we want to think about algorithmic surveillance, that in many ways goes way beyond the domains of her studies: Zuboff (1988) considers the rationale behind the adoption of surveillance within an organisation. She remarks that the burden of authority created "the yearning for omniscience in the face of uncertainty, the conformity-inducing power of involuntary display" (Zuboff, 1988: 324). Correspondingly, the narrative of increasing uncertainty in times of globalised threat seems to be a key motivator for the adoption of surveillance technologies like the one deployed at Berlin-Südkreuz. Of course, Zuboff made this observation referring to the exertion of managerial control in times of uncertainty, referring to the uncertainty of process optimisation. The scale and context are different, yet the prospect of regaining control might still appeal to authorities.

She also invokes the panoptic schema, which she describes as "mechanisms or instruments that render visible, record, differentiate and compare [...] whenever one is dealing with a multiplicity of individuals on whom [...] a particular form or behaviour must be imposed (Zuboff, 1988, p. 322). In a corporate setting, employees can assumedly differentiate between (un)desired behaviours and adapt accordingly. One of the goals of the pilot project Berlin-Südkreuz is behaviour modification, deterring unwanted behaviours. Yet, as the media discourse illustrates, anticipating what unwanted behaviour constitutes and how the algorithm would draw these boundaries, raises concern.

The discipline that surveillance imposes upon the individual has, since Zuboff's studies in the 1980s, left factory premises. Algorithmic surveillance is networked and no longer limited to a certain space or specific organisational boundaries. The diffusion of the internet changes spatial dynamics and infrastructures. Even the facial recognition software that is deployed at Südkreuz does not generate and interpret data within clear boundaries. Every passer-by is, if only for a short moment, registered in search for a match with the database. Those who are not content with surveillance in the workplace can, as a last resort, resign. With surveillance technology becoming intertwined in the infrastructure of our everyday lives, simply opting-out is not an option. Algorithmic surveillance pertains to all areas of life with surveillance extending out into the public sphere.

In Zuboff's (1988) study, foremen were watching their workers. Different managerial levels were using the data to check on the lower levels. Zuboff advocated for horizontal visibility as vertical visibility expands, granting data access to those on the same organizational level (Zuboff, 1988, p. 350). Yet, there is no horizontal visibility at the pilot project at Berlin-Südkreuz. Algorithmic surveillance produces the "unobservable observer". Unlike other products of digitalization, e.g., mobile applications, there is no accessible front end, no window into the system that enables the user to make sense of the employed system. In this context, one could take a post-panoptic stance and argue that the diffusion of the internet works both ways: the extensive online media coverage shows that the many [publics] are watching the few [e.g., state authorities] just as much as the few are watching the many. Boyne (2000) makes this point in his piece Post-Panopticism, in which he attempts to redress panopticism. This argument holds some merit. However, the reluctance of those responsible for the pilot project to give out information illustrates that two-way visibility does not necessarily result in an eye-level relationship between the state and the public(s) (Kurz, 2017). Not only could everyone be unknowingly watched, but it is also difficult to draw a boundary between those who are watching — and those who are not. As large interoperable information infrastructures emerge, data is not context-bound anymore. It cannot only be accessed but can leave the context; become aggregated and intertwined (Kallinikos, 2010). The project at Berlin-Südkreuz is the product of a cross-institutional, state-corporate partnership. The construction of the discursive identities, with the citizens as the protagonists and differing ideas about who the antagonist is, are exemplary for the diffuseness and the cross-contextuality that characterise contemporary algorithmic surveillance.

Ideally, managerial control in the relationship between the observer and the observed is mutually beneficial. The data generated through workplace surveillance could be used to assign promotions, bonuses, and if not that, coaching (Zuboff, 1988, p. 324). Algorithmic surveillance in public spaces benefits those who are being observed — but only hypothetically. The ease of moving around anonymously, in relative privacy in a public space, is certainly gone, while it remains questionable how algorithmic surveillance can prevent crime, benefiting those in control and those being controlled by increasing security. London, for instance, has a very tight-knit surveillance infrastructure. Yet, horrible terrorist attacks like the acid attack on 23 September 2017 keep happening (Sharman & Roberts, 2017). How could algorithmic control enable authorities to prevent crime? Zuboff (1988) observes this fundamental challenge as well. She notes that "the panopticon also enabled managers to see more of the processes and behaviours that affected their areas, without necessarily making it any easier to influence or control those events" (Zuboff, 1988, p. 348).

We need to critically question if, and how, the technology-focused, top-down ideas of the Panopticon apply to contemporary surveillance technologies. They are hardly applicable to

diffuse, automated computerised systems. The emergence of plural agency, anticipatory functionalities and obscured spatial boundaries are just some instances that show that the conception of the monolithic Panopticon is not always productive. This case illustrates that post-panoptic theorists such as Zuboff (1988) can still provide us with some helpful conceptual lenses to consider contemporary algorithmic surveillance technology. The next challenge will be to find new ways to approach the emerging social lifeworld of what some already term "surveillance society" (Galič et al., 2016).

CONCLUSION

Despite the heated controversy that the first test run in 2017 sparked, another surveillance pilot commenced at Berlin-Südkreuz in the summer of 2019 (Bundespolizei, 2019). The 2019 trial run specifically tested algorithms that detect suspicious behaviour (Henning, 2019). The new project provoked media coverage similar to the project's first phase (see Henning, 2019; Morgenpost, 2019; Vogt, 2019).

Amidst these developments, it is important to remember that the implementation of surveillance technology is a social practice. It is not only an issue of privacy, but it's also an issue of democracy in itself and pertains to the fundamental right to self-determination. All the social problems that this software ought to solve — transnational corporate crime, violent acts — require social intervention. This discourse exhibits a sombre tone. The safety benefit is hypothetical, the feeling of surveillance is tangible in the discourse. This goes to show that technology does never exist in isolation, it is always embedded in the social world. Social processes, discourses as negotiation, are relevant to technological developments (MacKenzie & Wajcman, 1999, p. 23).

Finally, this small glimpse at the discourse on the pilot-project at Berlin-Südkreuz – and the themes that dominate it – show that valuable insights for future research and exploration can be gained from the study of discourse. This case study also provides a baseline against which future cases could be compared. For instance, it would be compelling to research how media portray change over time and vary across different regions and nations. This discourse also offers a window onto underlying socio-technical imaginaries. To this end, it would be worthwhile to investigate how the media representation of this project compares against expert and policy discourses. A close look at the truth-claims that other actors put forward, e.g., state or manufacturers can offer perspectives onto the social construction and negotiation of the issue. This could give us a valuable insight into the negotiation of the cultural, political and social conditions under which the next generation of surveillance technology is developed.

The technology at hand is one in the making, public discourse is not only important; it's a necessity. Technology must not be developed in the isolation of state research facilities and private corporations. Citizens must be granted an input on questions that concern them so fundamentally. This controversial pilot project illustrates that it is crucial to take a substantive approach to questions of science and technology. A comprehensive participation process that would add new knowledge and improve decision quality.

REFERENCES

Antonia. (2017, August 2). Bahnhof Südkreuz: Start frei für die Erprobung intelligenter Videotechnik zur Gesichtserkennung. *Tarnkappe*. https://tarnkappe.info/bahnhof-suedkreuz-start-frei-fuer-die-erprobung-intelligenter-videotechnik-zur-gesichtserkennung/

Baker, P., & Ellece, S. (2011). *Key Terms in Discourse Analysis*. London: A&C Black.

Binder, C. (2016). Science, Technology and Security: Discovering Intersections between STS and Security Studies. *EASST Review*, *35*(4). https://easst.net/article/science-technology-and-security-discovering-intersections-between-sts-and-security-studies/

Borchers, D. (2017, February 23). Europäischer Polizeikongress: Intelligente Videoanalyse für mehr Sicherheit. *heise online*. https://www.heise.de/newsticker/meldung/Europaeischer-Polizeikongress-Intelligente-Videoanalyse-fuer-mehr-Sicherheit-3633397.html

Boyne, R. (2000). Post-Panopticism. *Economy and Society*, *29*(2), 285–307. https://doi.org/10.1080/030851400360505

Breyton, R. (2017, March 7). Der schmale Grat zwischen Terrorabwehr und Überwachung. *Welt*. https://www.welt.de/politik/deutschland/article162735087/Der-schmale-Grat-zwischen-Terrorabwehr-und-Ueberwachung.html

Bundesministerium des Innern. (2017, August 1). *Sicherheitsbahnhof Berlin Südkreuz* [Press release]. http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2017/08/gesichtserkennungstechnik-bahnhof-suedkreuz.html

Bundesministerium des Innern. (2018, October 11). *Projekt zur Gesichtserkennung erfolgreich* [Press release]. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2018/10/gesichtserkennung-suedkreuz.html

Bundespolizei. (2019, June 7). *Test intelligenter Videoanalyse-Technik*. https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2019/06/190607_videoanalyse.html

BVerfG, Urteil vom 15.12.1983, 1 BvR 209/83 u. a. - Volkszählungsurteil, NJW 1984, 419 http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowInfo&Name=bv065001

Chaos Computer Club. (2018, October 13). *Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg*. https://www.ccc.de/en/updates/2018/debakel-am-suedkreuz

Conrad, C. (2017, August 28). Stopp der Gesichtserkennung am Bahnhof Südkreuz gefordert – wie steht es um das Pilotprojekt?. https://www.datenschutz-notizen.de/stopp-der-gesichtserkennung-am-bahnhof-suedkreuz-gefordert-wie-steht-es-um-das-pilotprojekt-4318928/

Deutscher Bundestag. (2019, October 9). *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Lars Herrmann, Dr. Gottfried Curio, Martin Hess, weiterer Abgeordneter und der Fraktion der AfD, Drucksache 19/13848, 09.10.2019*. http://dip21.bundestag.de/dip21/btd/19/138/1913848.pdf

Deleuze, G. (1992). Postscript on the Societies of Control. *October*, *59*, 3–7. http://www.jstor.org/stable/778828

Demuth, K. (2017, November 30). *Endstation – Bilder vom Protest am Bahnhof Berlin Südkreuz* [Blog post]. https://digitalcourage.de/blog/2017/endstation-protest-suedkreuz

Dr. Datenschutz. (2018, July 23). *Gesichtserkennung am Rande des Zulässigen oder schon darüber hinaus?* [blog post]. https://www.datenschutzbeauftragter-info.de/gesichtserkennung-am-rande-des-zulaessigen-oder-schon-darueber-hinaus/

European Commission. (2016, October 7). *P-REACT Report Summary*. http://cordis.europa.eu/result/rcn/189910_en.html

European Commission. (2017, May 25). INDECT. Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment. http://cordis.europa.eu/project/rcn/89374_en.html

Evans, M. (2013, May 9). *'The Author and the Princess' – An Example of Critical Discourse Analysis*. http://www.languageinconflict.org/component/content/article/90-frontpage/145-the-author-and-the-princess-an-example-of-critical-discourse-analysis.html

Fontanille, J. (2006). *The Semiotics of Discourse*. Peter Lang.

Foucault, M. (1995). *Discipline and punish: the birth of the prison*. Vintage Books.

Galič, M., Timan, T., & Koops, B. J. (2016). Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology*, *30*(1), 9–37. https://doi.org/10.1007/s13347-016-0219-1

Gallbally, J., Marcel, S., & Fierrez, J. (2014). Image Quality Assessment for Fake Biometric Detection. Application to Iris, Fingerprint, and Face Recognition. *IEEE Transactions on Image Processing*, *23*(2), 710–724. https://doi.org/10.1109/TIP.2013.2292332

Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. New York University Press.

Henning, M. (2019, June 19). Überwachung am Südkreuz soll jetzt Situationen und Verhalten scannen. *Netzpolitik*. https://netzpolitik.org/2019/ueberwachung-am-suedkreuz-soll-jetzt-situationen-und-verhalten-scannen

Hermes, J. (2017, December 16). Gesichtserkennung und Wirrungen des BMI. *TEXperimenTales*. https://texperimentales.hypotheses.org/2283

Horchert, J. (2017, August 1). Gesichtserkennung am Berliner Südkreuz. Bitte gehen Sie weiter. Hier werden Sie gesehen. *Der Spiegel*. http://www.spiegel.de/netzwelt/netzpolitik/gesichtserkennung-am-berliner-suedkreuz-ein-test-fuer-unsere-freiheit-a-1160867.html

Hornung, G., & Schnabel, C. (2009). Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination. *Computer Law & Security Review*, *25*(1), 84–88. https://doi.org/10.1016/j.clsr.2008.11.002

Hummel, P. (2017, November 11). Die Tücken der Gesichtserkennung. *Spektrum*. https://www.spektrum.de/news/die-tuecken-der-gesichtserkennung/1521469

Jasanoff, S. (2004). Afterword. In S. Jasanoff (Ed.), *States of Knowledge. The Co-production of Science and Social Order* (pp. 274–282). Routledge.

Jasanoff, S. (2005). *Designs on Nature: Science and Democracy in Europe and the United States*. Princeton University Press.

Jasanoff, S. (2015). Future Imperfect: Science, Technology and the Imagination of Modernity. In S. Jasanoff & Kim, S. H. (Eds.), *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power* (pp. 1–33). University of Chicago Press.

Kallinikos, J. (2004). Deconstructing Information Packages: Organizational and Behavioural Implications of ERP Systems. *Information Technology & People*, *17*(1), 8–30. https://doi.org/10.1108/09593840410522152

Kallinikos, J. (2007). *The Consequences of Information: Institutional Implications of Technological Change*. Edward Elgar Publishing.

Kallinikos, J. (2010). The "Age of Smart Machine": A 21st Century View. In P. A. Laplante (Ed.), *Encyclopedia of Software Engineering* (Vol. 1, pp. 1097–1103). Auerbach Publications. https://www.taylorfrancis.com/books/e/9781351249270/chapters/10.1081/E-ESE-120044162

Käppner, J. (2017, September 15). Videoüberwachung. *Süddeutsche Zeitung*. http://www.sueddeutsche.de/leben/v-videoueberwachung-1.3656960

Kühl, E. (2017, August 24). Datenschützer fordern Abbruch des Pilotprojekts. *Zeit*. http://www.zeit.de/digital/datenschutz/2017-08/gesichtserkennung-berlin-suedkreuz-daten-transponder

Kurpjuweit, K. (2017, February 20). Bahn testet intelligente Videoüberwachung am Südkreuz. *Tagesspiegel*. https://www.tagesspiegel.de/berlin/berliner-bahnhof-bahn-testet-intelligente-videoueberwachung-am-suedkreuz/19413266.html

Kurz, C. (2017, August 1). Ortstermin am Südkreuz: Die Automatische Gesichtserkennung beginnt. *Netzpolitik*. https://netzpolitik.org/2017/ortstermin-am-suedkreuz-die-automatische-gesichtserkennung-beginnt/

Law Blog. (2017, August 1). *Nicht hinnehmbares Gefühl des Überwachtwerdens* [Blog post]. https://www.lawblog.de/index.php/archives/2017/08/01/nicht-hinnehmbares-gefuehl-des-ueberwachtwerdens/

Lobe, A. (2017, May 9). Lobes Digitalfabrik. Wir merken uns schon mal Ihr Gesicht. *Spektrum*. http://www.spektrum.de/kolumne/wir-merken-uns-schon-mal-ihr-gesicht/1456847

Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press.

MacKenzie, D. A., & Wajcman, J. (1999). Introductory Essay: The Social Shaping of Technology. In: A. MacKenzie & J. Wajcam. (Eds.), *The Social Shaping of Technology* (pp. 3–27). Open University Press.

Möllers, N., & Hälterlein, J. (2013). Privacy Issues in Public Discourse: The Case of "smart"

CCTV in Germany. *Innovation: The European Journal of Social Science Research*, *26*(1-2), 57–70. https://doi.org/10.1080/13511610.2013.723396

Moorstedt, M. (2017, April 7). Sie Sehen Uns. *Süddeutsche Zeitung*. http://www.sueddeutsche.de/kultur/kuenstliche-intelligenz-sie-sehen-uns-1.3455674

Morgenpost. (2017, July 28). Gesichtserkennung: Big Brother im Bahnhof Berlin Südkreuz. https://www.morgenpost.de/bezirke/tempelhof-schoeneberg/article211395129/Im-Bahnhof-Suedkreuz-startet-Test-zur-Gesichtserkennung.html

Morgenpost. (2019, June 6). Videoüberwachung am Südkreuz startet wieder. https://www.morgenpost.de/berlin/article226216631/Videoueberwachung-am-Suedkreuz-startet-wieder.html

Musik, C. (2011). The thinking eye is only half the story: High-level semantic video surveillance. *Information Polity*, *16*(4): 339–353. https://doi.org/10.3233/IP-2011-0252

Neumann, P. (2017, April 4). Testlauf Ab Herbst wird am Südkreuz Gesichtserkennung erprobt. https://archiv.berliner-zeitung.de/berlin/testlauf-ab-herbst-wird-am-suedkreuz-gesichtserkennung-erprobt-26247956

Norris, C. & Armstrong, G. (1999). *The Maximum Surveillance Society: The Rise of CCTV*. Berg Publishers.

OECD. (2004). *The Security Economy*. OECD Publishing.

Oepen, D. (2013, August). Transparenz und Datensparsamkeit von Elektronischen Ausweisdokumenten in Deutschland. In Arbeitsgruppe Informatik in Bildung und Gesellschaft (Ed.), *Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen. Tagung, 30.11/1.12.2012* (pp. 37–60). Humboldt-Universität zu Berlin.

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Rand Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf

Phillips, N., & Hardy C. (2002). *Discourse Analysis - Investigating Processes of Social Construction*. *Qualitative Research Methods*. SAGE Publications.

Poschmann, A. (2017, June 20). Polizei sucht Freiwillige für Totalüberwachung. *Computer Bild*. https://www.computerbild.de/artikel/cb-News-Sicherheit-Polizei-sucht-Freiwillige-Totalueberwachung-18383625.html

Prantl, H. (2017, August 24). De Maizière hebt das Recht auf Anonymität auf. *Süddeutsche Zeitung*. https://www.sueddeutsche.de/digital/gesichtserkennung-de-maiziere-hebt-das-recht-auf-anonymitaet-auf-1.3639958

Rabenstein, A. (2017, June 23). Berlin-Südkreuz: Los, scanne mich. *Märikische Allgemeine*. https://www.maz-online.de/Brandenburg/Berlin-Suedkreuz-Los-scanne-mich

Reinsch, M. (2017, August 22). Gesichtserkennung am Südkreuz: Opposition befürchtet

endgültiges Ende der Anonymität. *Berliner Zeitung*. https://archiv.berliner-

zeitung.de/berlin/gesichtserkennung-am-suedkreuz-opposition-befuerchtet-endgueltiges-ende-der-anonymitaet-28208738

Reuter, M. (2017a, June 21). Dauerfeuer gegen das Grundgesetz – so treibt die große Koalition das Land in den Überwachungsstaat. *Netzpolitik*. https://netzpolitik.org/2017/dauerfeuer-gegen-das-grundgesetz-so-treibt-die-grosse-koalition-das-land-in-den-ueberwachungsstaat/

Reuter, M. (2017b, August 24). Bundesregierung: Test am Südkreuz wird auf jeden Fall ein Erfolg. *Netzpolitik*. https://netzpolitik.org/2017/bundesregierung-test-am-suedkreuz-wird-auf-jeden-fall-ein-erfolg/

Rieblinger, P. (2017, August 25). Überwachung: Der Pilotversuch Berlin Südkreuz. *IT-Security@Work*. https://www.isw-online.de/ueberwachung-der-pilotversuch-berlin-suedkreuz-2/

Roßnagel, A., Desoi, M., & Hornung, G. (2011). Gestufte Kontrolle bei Videoüberwachungsanlagen. *Datenschutz und Datensicherheit-DuD*, *35*(10). https://doi.org/10.1007/s11623-011-0166-z

Roux, M. (2019, March 20). Face Recognition vs Face Detection: What's the difference? https://sightcorp.com/blog/face-recognition-vs-face-detection-whats-the-difference/

Schmidt, F. (2017, August 24). Biometrische Gesichtserkennung macht Totalüberwachung möglich. *DW*. https://p.dw.com/p/2igNt

Schmiechen, F. (2017, August 28). Berliner Bahnhof Südkreuz: Ist Gesichtserkennung der Beginn der totalen Überwachung? *Gründerszene*. https://www.gruenderszene.de/allgemein/berlin-gesichtserkennung-kommentar

Schneider, F. (May 6, 2013a). Introduction to Discourse Analysis [video file]. https://www.youtube.com/watch?v=NpJhICZczUQ

Schneider, F. (May 13, 2013b). How to Do a Discourse Analysis. *PoliticsEastAsia*. http://www.politicseastasia.com/studying/how-to-do-a-discourse-analysis/

Sharman, J. & Roberts, R. (2017, September 23). Stratford 'Acid Attack': Six People injured near Shopping Centre in East London. *Independent*. http://www.independent.co.uk/news/uk/crime/stratford-acid-attack-latest-updates-bus-station-incident-injured-police-a7963831.html

Simon, L. (2017, June 22). #SelfieStattAnalyse: Masken gegen Überwachung. *Digitalcourage*, https://digitalcourage.de/blog/2017/selfiestattanalyse-masken-gegen-ueberwachunung

Stöcker, C. (2017, August 25). Videoüberwachung am Südkreuz. Treffen sich Orwell und Kafka am Bahnhof. *Der Spiegel*. http://www.spiegel.de/netzwelt/netzpolitik/gesichtserkennung-am-suedkreuz-treffen-sich-orwell-und-kafka-am-bahnhof-a-1164578.html

STS Research Platform. (2018). *Sociotechnical Imaginaries: Methodological Pointers*. http://sts.hks.harvard.edu/research/platforms/imaginaries/ii.methods/methodological-pointers/

Stürzl, J. (2018, October 12). Mehr Sicherheit durch mehr Überwachung? *Qiez*.

https://www.qiez.de/suedkreuz-ueberwachung-gesichtserkennung/

Suthorn, C. (2017, August 1). *Face Recognition Field Test at Südkreuz 14* [Photograph]. Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Face_Recognition_Field_Test_at_S%C3%BCdkreuz_14.jpg

Swanson, E. (2008). Modality in Language. *Philosophy Compass*, *3*(6), 1193–1207. https://doi.org/10.1111/j.1747-9991.2008.00177.x

Tagesschau. (2020, January 24). Gesichtserkennung. Kameras ja, Software nein. https://www.tagesschau.de/inland/gesichtserkennung-bundespolizei-101.html

Tiles, M., & Oberdiek, H. (1995). *Living in a Technological Culture: Human Tools and Human Values*. Routledge. https://doi.org/10.4324/9780203980927

Verbeek, P.-P. (2011). *Moralizing Technology: Understanding and Designing the Morality of Things*. University of Chicago Press.

Vogt, S. (2019, June 9). Das Südkreuz wird wieder zum Drehort. *Tagesspiegel*. https://www.tagesspiegel.de/berlin/videoueberwachung-in-berlin-das-suedkreuz-wird-wieder-zum-drehort/24439112.html

Winner, L. (1980). Do Artifacts have Politics?. *Daedalus*, *109*(1), 121–136. http://www.jstor.org/stable/20024652

Wissen.de. (2018, November 2). Hinterfragt: Wie gut funktioniert die Gesichtserkennung? *wissen.de*. https://www.wissen.de/hinterfragt-wie-gut-funktioniert-die-gesichtserkennung

Zuboff, S. (1988). *In the Age of the Smart Machine: The Future of Work and Power*. Basic Books.

FOOTNOTES

1. All coverage analysed and referenced in this paper was published in German. Citations are the author's translations.

2. For a full compilation of all articles, see Appendix A.

3. German high-speed train.