Johanna Möllentin / Francesca Schmidt

Surveillance, Artificial Intelligence and Power

Artificial intelligence (AI) creates new possibilities for the algorithmic use of data and its automated analysis; thus, the public discourse on AI automatically leads to a discourse on algorithms. Increased and accelerated linking of data sets offer new surveillance images—of individuals, (marginalized) populations, and even entire societies. These new quantitative and qualitative changes in technical surveillance systems not only bring old, never sufficiently resolved decisions to the surface, but also give rise to entirely new and highly urgent questions—of a legal, social, and ethical nature. They concern the private sphere (mutual surveillance) and the relationship between the state and its citizens.

Also, these questions bring with them a severity by breaching issues such as the many encroachments on (fundamental) rights, such as informational self-determination, and human dignity. As we are currently experiencing during the Corona pandemic, times of crisis reinforce this spiral due to newly grown insecurities and fears; sometimes, used deliberately as a pretext. This shows itself in the often-misused data protection as an excuse for ineffective or faulty Corona protection measures in the past few months.

The (populist) call for security, order, and control is continuously getting louder. All these intensified calls, which make use of a paralyzing fear spiral, ultimately make the world seem more insecure by the day. Consequently, the increasing endowment of state authorities with legal and technical competencies for surveillance is justified and thus increases the acceptance of senseless and ineffective measures of surveillance, which mostly miss or even counteract an actual increase in security.[1]

At the same time, our fundamental democratic freedoms and values are facing increasing pressure. Above all, the private sphere, protected by fundamental rights, is constantly experiencing further restrictions—at times rapidly and with enforced media coverage, at times successively and quietly.

The networking of different technologies and data sets also reinforces that new technologies are increasingly being used categorically rather than just purposefully. Data taps and stockpiles are growing immeasurably; using artificial intelligence, or algorithms, these can be sifted through, clustered,

1 Neumann, Linus: Untersuchung: Vorratsdatenspeicherung ist ineffektiv. In: netzpolitik, January 27, 2011, https://netzpolitik.org/2011/untersuchung-vorratsdatenspeicherung-ist-ineffektiv/ (May 24, 2021).; henning: Trügerische Sicherheit: Der elektronische Personalausweis. In: Chaos Computer Club, September 15, 2013, https://www.ccc.de/de/updates/2013/epa-mit-virenschutzprogramm (May 24, 2021).

merged, and entire societal graphs can be created.[2] Today, entire contexts are often surveilled rather than targeted individuals. In the state-citizen relationship, this development particularly effects state measures. For example, countless video cameras are demanded in public places in Berlin to prevent crimes.[3]

When these technologies are connected with artificial intelligence, a panopticon emerges wherein its dimensions go far beyond those imagined by Foucault.[4] One of the fundamental ideas of the panopticon is centrality. The panoptic prison is a circular building with a surveillance tower in its center, separating guards and prisoners into those who see and those who are to be seen. The guards can observe all prisoners from the surveillance tower without them seeing the guards. Because the prisoner cannot be sure who is watching him or her from the top of the tower, he or she lives in the idea that he or she is always being watched. Surveillance thus takes place permanently, regardless of whether the guards are present or not. Especially in the course of digitalization, this model has been criticized, as it does not allow to respond to the wealth of data and technological interconnections. Kevin Haggerty and Richard Ericson, both Canadian sociologists, consider the principle of assemblage to be more appropriate for digital surveillance.[5] They understand assemblages, following Gilles Deleuze and Felix Guattari, as a multiplicity of heterogeneous objects whose connection arises solely from their functionality. Those assemblages make it possible to think surveillance in differently interlinked spheres (social, financial, labor, health, gender/body), even though they initially appear unconnected.

In the 21st century, unprovoked mass surveillance is becoming more of a reality than ever before due to the use and development algorithms. A reality that is becoming more and more intense, and more and more expansive every day. More noticeable to some, and less noticeable to others. Visible? To

2 See also boyd, danah; Crawford, Kate: CRITICAL QUESTIONS FOR BIG DATA: Provocations for a cultural, technological, and scholarly phenomenon, Information, Communication & Society, xv/5 2012, pp. 662–679.

3 Biselli, Anna: Berlin: Keine rationalen Argumente für Videoüberwachung an S-Bahnhof. In: netzpolitik, March 1, 2019, https://netzpolitik.org/2019/berlin-keine-rationalen-argumente-fuer-videoueberwachung-an-s-bahnhof/ (May 24, 2021).

4 Foucault, Michel: Überwachen und Strafen: Die Geburt des Gefängnisses, Frankfurt am Main 1977.

5 Haggerty, Kevin D. and Ericson, Richard V.: The surveillant assemblage, The British Journal of Sociology, li/4 2000, pp. 605–622.

whom? To what extent, exactly? At what point in time? What information is stored, for how long, and for what purpose? This often remains non-transparent and invisible.

Necessary Change of Perspective

Although we are all affected by surveillance, it has different consequences for those who deviate from the culturally and historically implanted masculine white norm in its different forms. To change this, we need to address many aspects, but it takes two things above all: awareness/knowledge (of the difference in consequences) and will (to dissolve existing power structures). This includes the feminist, especially intersectional, view of the complexity of surveillance, even beyond the question of privacy.

Looking back, we can see that the surveillance of all of those who do not appeal to the patriarchally shaped male heteronormative norm, has a long tradition. Simone Browne, Professor of African and African Diaspora Studies at the University of Austin, Texas, emphasized that surveillance and its technologies are racialized and serve to restore the white norm and re-enforce who belongs and who does not. Many practices of surveillance used in the transatlantic slave trade, both discursive and real, continue to operate today.[6] This is the case, for example, with practices of bodily measurement used primarily to determine the age of young refugees. The biometric collection of fingerprints also follows this pattern.

From that very patriarchal surveillance, historically, women's bodies have also been shaped—to this day, dramatic forms of surveillance of the female or trans* body exist, which can take on different dimensions depending on the cultural and political context.

It becomes clear: Surveillance does not result in the same regulatory (fundamental rights) interventions for all people, and there are complex and severe differences, especially in the area of justification and, in particular, proportionality. Surveillance thus does not affect everyone equally. Within the white patriarchal norm, the freedom of some means the surveillance of others, i.e., of all those who are denied belonging or who choose not to be part of this norm.

6 Browne, Simone: Dark matters: on the surveillance of blackness, Durham 2015.

Nevertheless, We are All Surveilled...

The prominent sentence "I have nothing to hide"—expressing not having a problem with mass or unprovoked surveillance—falls short, as shown by the explanations above.

On the one hand, it reflects the opposite of self-determined, autonomous decision making; on the other hand, it is dangerous not to be aware of prospective risks and, above all, refusing to be knowledgeable about them. The awareness of what should be "hidden" is missing at this very point. What will be done with and extracted from the surveillance data and its results? Which data will be used for or against us in the future? We do not know at the time of this statement. Nor do we know how they will be linked and re-evaluated.

Nevertheless, quite fundamentally, as a society, we should fight back against a form of surveillance that is increasingly automated by algorithms. After all, maintaining privacy does not necessarily mean keeping secrets. Instead, such a sentence, which can only be in relation to a counterpart, suggests that surveillance seems to be well-founded in the case of this other. The others (beyond the norm), therefore, have something to hide.

Privacy: For Whom?

Surveillance is very often discussed in terms of privacy. However, in a first evaluation, we should distinguish here who invades privacy: the state, private companies, or other people (often again with the help of private companies, like Facebook & Co).

When we talk about state intrusions into privacy, we see that the intensity of these intrusions increases with the degree of dependence on the state. For example, people who receive state social benefits, people with disabilities, refugees, or asylum seekers have to reckon with much more numerous and more profound interventions than people who do not belong to any of these or other marginalized, stigmatized groups. Transparency becomes an essential requirement for social government services. Practices such as home visits, monitoring of activities on social networks[7], and disclosure of bank account

7 Wermter, Benedict: Schnüffeln auf Facebook. In: Correctiv. Recherche für die Gesellschaft, June 22, 2015, https://correctiv.org/aktuelles/auskunftsrechte/2015/06/22/schnueffeln-auf-facebook/ (July 26, 2019).

transactions are used to surveil and spy on people who belong to low-income or less prosperous groups, ostensibly in the public interest.

People, however, exposed to the right education, technical knowledge, time, and money, can protect their data from the state or private companies to a greater extent, and, if such a possibility arises, can make their data available in a self-determined manner, protecting their privacy to a greater extent. A de facto privilege, as legally, it is equally available to all.

When we discuss surveillance under the dictum of privacy, it becomes clear that we have to think about societal structures of power and domination because the freedom that a few receive through the protection of privacy is at the same time the lack of freedom for others. Parallel to this, there are many forms of surveillance from which a few gain additional value, for example, financially or in the form of knowledge and superiority, whereas others face disadvantages without any additional value. In this respect, discussions around privacy versus security are once again deceptive because they distract from the more essential questions of privacy versus control and the central power structures that accompany and permeate these questions.

Big Data, Algorithms, and AI for Social Compartmentalization

The enormous amount of data that we as a society accumulate and store daily is the basis for increased surveillance, including state surveillance. At the very least, these data collections, which are also constantly improving in "quality," make it possible to establish (new) correlations and relationships of facts. In some countries this is already taking effect by being used for predictive policing.

The data collected at different points in time and from different locations, as well as by different systems are brought into new correlations by automated processes. To put it simply; these are algorithms that calculate probabilities based on an analysis of case data and make statements about who, when and where a possible crime might be committed. This technology is used to control the deployment of police forces, now also by some police authorities in German states. However, in the USA, it is already part of everyday life that potential offenders receive a visit from the police, as a result

of an indication and warning for possible future criminal offenses.[8] A procedure that neither fits into our legal system nor should fit into our social value system and yet is increasingly applied.

Apart from the indiscriminate blanket suspicion and its severe (e.g., psychological, social, or financial) consequences, which emanate from such messages (and possibly making them public)[9] we should ask ourselves: What happens if the people concerned are only turned into potential offenders by new data correlations produced by algorithms? They are assigned to a risk cluster based on personal habits, past acquaintances, relatives, or their birthplace. From the outset, judgments are made that often reinforce existing discrimination. It is difficult for those affected to defend themselves against this bias. This is because they have to defend themselves against a suspicion that has only arisen based on a data correlation or what Algorithms has made of it.[10] The situation is further complicated because technology is often ascribed to objectivity and neutrality and is frequently said to be free of errors. Nevertheless, feminist research established years ago that technology is not neutral.[11] With all their discriminatory structures, ideas of society flow into and materialize in the developments of new technologies. Consequently, we must ensure that technologies, especially automatic decision-making systems, are developed according to transparent criteria and remain verifiable. As for now, it is the case that the police rarely know how the probabilities of possible future crimes are calculated. However, how are we supposed to trust these systems if we do not even know how they work?[12] Especially when they are accompanied by opacity and lack of verifiability? How does a person

8 Gorner, Jeremy: Chicago Police Use Heat List as Strategy to Prevent Violence. In: Chicago Tribune, 2013, http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list (November 1, 2021); Merz, Christina: Predictive Policing—Polizeiliche Strafverfolgung in Zeiten von Big Data, Karlsruher Institut für Technologie (KIT), 2016, https://publikationen.bibliothek.kit.edu/1000054372 (November 1, 2021).

9 Steinschaden, Jakob: Der "Chilling Effect": Massenüberwachung zeigt soziale Folgen—Netzpiloten.de. In: Netzpiloten Magazin, April 7, 2014, https://www.netzpiloten.de/der-chilling-effect-massenueberwachung-zeigt-soziale-folgen/ (May 24, 2021).

10 Gless, Sabine: Predictive policing und operative Verbrechensbekämpfung. In: Herzog, Felix and Schlothauer, Reinhold and Wohlers, Wolfgang (eds), Rechtsstaatlicher Strafprozess und Bürgerrechte, Gedächtnisschrift für Edda Weßlau, Berlin 2016.

11 See, for example Wajcman, Judy: TechnoFeminism, Cambridge UK 2004.

12 Fry, Hannah: Hello World: How to be Human in the Age of the Machine, London New York Toronto Sidney Auckland 2018.

defend himself/herself against the accusation of a crime if there is no open and comprehensible decision-making process, and how can one even argue against a "future" crime that has not been completed, let alone prepared or planned? Isn't the surveillance, evaluation or assessment already criminal itself? Is the algorithmically calculated probability of crime already an accusatory situation made in the Blackbox? For good reason and with German history in sight the German constitutional state, despite all of its transparency, once decided against a too broad advance of criminal liability and thus against the Gesinnungsstrafrecht[13]. However, this decision seems to be continuously mellowed throughout the discourse and within law making. This can be seen in implementations such as the conceptualization of a "dangerous person" into criminal law—with the aid of verbal turns of phrase embedded in novel discourses on criminal law by individual instances of power[14]. These being more in favor of surveillance itself than of the (de facto hardly existing) alleged successes and advantages.

Thus, we are divided into potential perpetrators and victims; other clusters are also formed with the help of the data. This, in turn, determines our creditworthiness, the number of insurance premiums, job offers, or, in case of doubt, the cost of our health insurance (which is fortunately not yet the case in Germany). The specialist literature uses the term social sorting[15] for this clustering, i.e., the sorting into certain social classes and thus their location in the prevailing power structure.

This power structure (e.g., Europe) also becomes evident, by the process of it sealing itself off from the outside world with the help of artificial intelligence. Border controls are being automated and the electronic passport is supposed to save time but poses a challenge to people or places who cannot provide this document, or in case of any doubt can never receive it in the first place, elevating those who do have it to even more transparency. Furthermore, what happens to the existing state surveillance systems and hoarded

13 A term that basically means a kind of criminal law oriented primordially to punish attitudes or belief systems of offenders instead of the act itself, respectively, the traditional elements of mens rea.

14 See Böhm, María Laura: Der Gefährder und das Gefährdungsrecht: eine rechtssoziologische Analyse am Beispiel der Urteile des Bundesverfassungsgerichts über die nachträgliche Sicherungsverwahrung und die akustische Wohnraumüberwachung, Göttingen 2011.

15 Lyon, David: Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination, London 2003.

data volumes beyond these factors if the current political system ever changes? A look at countries with other government structures, such as China, India, or Russia, gives insight on this.

The deadly point of compartmentalization is geofencing, when artificial intelligence is used to arm "digital fences". Video surveillance, motion sensors, and thermal imaging are used to track down border crossers daily, as practiced along the Turkish-Syrian border for example. With the help of integrated automated self-firing systems, such surveillance zones can kill people without manual labour. The debate over armed drone operations or computer game deliriums seems to have been resolved. The use of technology for surveillance is being expanded to the point where, ultimately, even the "dirty work" almost no longer requires direct human interaction. The accompanying questions of responsibility are becoming less and less tangible, moving away from the counterpart as a legal subject and thus also giving new meaning to the decisions to be made about social guidelines and responsibilities. Whereas usually, the core of surveillance is often secrecy, here surveillance and consequences seem shrill, neon flashing, and impossible to miss, almost like a statement. The use of surveillance is as complex and diverse as the expression of power behind it. The result of surveillance, in this case, is unmistakably, an expression of power over freedom of movement and even human life. Yet people choose to look the other way. In fact, technology is used precisely for this purpose: to be able to observe others more efficiently. In those cases unsolved ethical questions, or unfound answers, related to society as a whole, are easier to ignore than to solve. As a result many answers were often decided due to the implementation of a few and without the acquiescence of many.

Even if we, as a Western European society, oppose the use of lethal AI, the moral boundaries seem permeable: A conflation of migration policy, economic policy, and the arms industry lead to the conclusion that "digital fences" are provided by Germany and Europe as well, such as the one in Morocco. The fence delivered to Saudi Arabia in 2009, that was co-financed by EADS (now Airbus), was also, among others, enabled by the German Gesellschaft für Internationale Zusammenarbeit.[16]

16 Grieger, Fabian and Schlindwein, Simone: Migrationspolitik und Rüstungsindustrie: Das Geschäft mit Hightech-Grenzen. In: taz.de, die tageszeitung 2016.

Critical Review Versus Perpetuation of Existing Discrimination?

That algorithms perpetuate discrimination because they produce discriminatory results in many cases is well known and widely documented.[17] Automated facial recognition designed not only to match people to "official" identities but in some cases even to look for possible affects and emotions such as anger, aggression, and propensity for violence, in order to preempt possible terrorist attacks, is considered highly error-prone. Concerning affective computing[18], we know from previous research that on the one hand emotions and affects are coded differently in various cultures. On the other hand, however, emotions continue to be stereotyped and gendered in a binary understanding: Herein anger, for example, is often classified as something masculine and hysteria as rather feminine trait.

How does this impact facial recognition? Often, programs fail to identify faces correctly, or even fail in recognizing them as human[19], especially concerning Black people. Joy Buolamwini of the MIT Media Lab found that facial recognition only works well for white men. Black women and Black men often fail to be recognized entirely. In the case of Black women, nearly one-third of all matches are simply wrong[20].In 2018 The American Civil Liberties Union (ACLU), found that Amazon's facial recognition system incorrectly matched 28 members of the US Congress to mugshots. These false matches disproportionately involved people of color. These included six members of the Congressional Black Caucus, an association of African-American members of Congress. The recently deceased Congressman and icon of the Black

17 Benjamin, Ruha: Race after technology: abolitionist tools for the new Jim code, Medford, MA 2019; Buolamwini, Joy and Gebru, Timnit: Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research. In: Proceedings of Machine Learning Research, 2018, lxxxi 2018, pp. 77–91; Eubanks, Virginia: Automating inequality: how high-tech tools profile, police, and punish the poor, New York, NY 2017; Noble, Safiya Umoja: Algorithms of Oppression: How Search Engines Reinforce Racism, New York 2018; O'Neil, Cathy: Weapons of math destruction: how big data increases inequality and threatens democracy, New York 2016.

18 Picard, Rosalind W.: Affective computing, Cambridge, Mass 2000.

19 Barr, Alistair: Google Mistakenly Tags Black People as "Gorillas," Showing Limits of Algorithms. In: The Wall Street Journal, July 1,2015, http://blogs.wsj.com/digits/2015/07/01/google-mistakenly-tags-black-people-as-gorillas-showing-limits-of-algorithms/ (November 1, 2021).

20 Buolamwini; Gebru 2018.

American Civil Rights Movement, John Lewis, was also misattributed.[21] All of these members of Congress are public figures, represented broadly with a variety of imagery within various databases. Nevertheless, facial recognition failed in their correct identification. Used as a tool for (governmental) surveillance, it thus promotes discrimination, in that, police measures tend to be predominantly directed against Black people, as they are repeatedly associated with crime in this way. If state security authorities use such faulty systems, this has particularly severe consequences. Due to the power relationships at hand, and the state's duty to protect—discrepancies become evident in the disparity between the aim of security for all, that effectively cannot be applied to each individual due to the biases explained above.

Powerful algorithms, such as those used in facial recognition and speech recognition technologies, work with learning systems instead of simple rule-based conditional chains. This means that the database with which the system is fed directly impacts the system's subsequent decision making. If the unadjusted baseline databases already contain imbalances or discrimination, the algorithm will perpetuate it, leading to and further reinforcing inequality. To continue within the congressional example: If the database contains a majority of imagery linking Black people to criminal offences, the algorithm will automatically assign the images of Black people accordingly. This discrimination does not have to be intentional. However, it clearly shows a lack of intersectional problem awareness regarding power and hierarchical structures, and it also shows how institutionalized forms of discrimination such as racism and sexism are perpetuated in our society.

Flexible or Clear Boundaries?

Now we could—as is often done—ultimately state that it is simply a matter of cleaning up the technology's data set and its (training) data set, in order to make it socially and legally acceptable, i.e., to put an end to discrimination.

The use of technology and software could lead to diminishing existing patterns of discrimination and counteracting its perpetuation. Although in

21 Snow, Jacob: Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots. In: American Civil Liberties Union, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 (August 11, 2019).

the case of Algorithms, this is highly complex and never fully guaranteed, we as a society should be paying attention to and proactively driving such a development forward. There are many inspiring and progressive ideas and models for this that need to be discussed elsewhere. However, even if, in some cases, it is possible to minimize existing discrimination through the use of Algorithms and to present this in an open and factual manner, the real struggle remains within the acknowledgement that neutral technology will never be the product of neutral people, as these simply do not exist.

Thus, critical awareness leads us to question: How much and what kind of discrimination and/or surveillance should be "allowed"? To what extent must the assessment be different when the state acts with surveillance measures? The Basic Law provides the guidelines for this answer. Nevertheless, if legal measures were to be equated, there would probably be no mentioning of problems, as well as no need for any of the executive and judicial branches.

One thing becomes clear: Surveillance often results in a large number of encroachments and violations to our fundamental rights. It affects our fundamental democratic freedoms and values, such as our privacy protected by these fundamental rights, the right to sexual and reproductive self-determination, freedom of assembly and movement, and freedom from discrimination. Last but not least, it is also about human dignity, Article 1 of the German Basic Law. Concerning artificial intelligence, which increases the severity of the interference many times over, entirely new questions arise. The old questions, to which the answers are still lacking, not only remain topical, but they also partly arise anew with unprecedented urgency. With the amount of data collected and stored, it is possible to search for suspicious patterns and correlations on a microscopic scale. By linking data sets, it is even possible—especially with the help of metadata—to create entire population profiles. Even if artificial intelligence is still less relevant in German surveillance measures, a look at the Chinese social scoring program shows us where this journey can lead. Mass and profound surveillance powers and data retention not only harms democracy in many ways.

The relationship between citizens and the state is always linked to accompanying questions of power distribution, including the tension between duty and protection. In recent years, the latter has often been used to justify an increasing number of measures that are supposed to implement security. However, these can at times not only lead to opposing results, but also, because of their effects, show a substantial imbalance in the proportionality of their assessment. A long chain of shrill flashing warning lights becomes un-

avoidable. A warning expressed in the publications of Edward Snowden about the global surveillance system.

For example, a German parliamentary Committee of Inquiry have shed light, and its impact has been documented in scientific reports. Who surveils the overseers when the warning lights are not perceived equally by everyone, and the internet is not infrequently declared a lawless space?

For a long time, the expansion of state surveillance measures, which is growing into an almost unwieldy, opaque patchwork of authorization bases, was hardly considered in its entirety from a legal point of view. In Germany it has now been flanked by a clear edge on the part of the judiciary. In addition to the need to specify the differentiation of intrusion powers according to the weight of the intrusion in the decision of the German Federal Constitutional Court on inventory data disclosure II,[22] a lawsuit filed by civil society organizations recently led the judges in Karlsruhe to examine the right to intelligence services concerning the permissibility of warrantless surveillance of global internet traffic by the Federal Intelligence Service. The result of which should not be surprising: The human rights illegality and incompatibility of warrantless mass surveillance with the German constitution was established.[23] The actual novelty was associated with the former: a clarification regarding the previous unequal treatment of citizens and "foreigners abroad".

However, in addition to this milestone for the legal protection of millions of people, the question remains as to whether the constitutional corrective also leads to the setting of limits or the preservation of rights. Instead of addressing the issue of independent monitoring as a whole, which was already required by constitutional law in 2010[24] (to the question of how the existing surveillance practice of German security authorities is structured as a whole and what consequences current surveillance entails) we look at a continuous development of surveillance systems in terms of the constant expansion of measures—despite countless clear decisions by the highest courts on data retention, preventive telecommunications surveillance and online searches.

Not long ago, in Germany a "successful" attempt was made to finally defer expiring surveillance measures,[25] which were initially limited in time in the so-called Schily-catalogs and subject to the obligation of constant in-

22 BVerfG, 27.05.2020, 1 BvR 1873/13, 1 BvR 2618/13.

23 BVerfG, 19.05.2020, 1 BvR 2835/17.

24 BVerfG, 02.03.2010, 1 BvR 256/08.

25 BT-Drs 19/23706, https://www.bundestag.de/dokumente/textarchiv/2020/w45-de-terrorismusbekaempfung-802464 (May 24, 2021).

dependent evaluations, after numerous interim deferrals. Independent full evaluations are nonexistent up to date. The legislative package contains legal bases for surveillance measures that the Constitutional Court has long since overturned. Thus, to date, there is no overall account of surveillance, not even a list of criteria for an urgently needed scientific evaluation of all surveillance laws.[26] There is simply too little known about the technologies used by security authorities and the suitability or necessity of the far-reaching encroachments on fundamental rights that accompany them. Moreover, without technology assessment, the effects on individuals and society remain in the dark.

The argument that is always put forward in opposition to these concerns is security. However, without wanting to use this misleading security-liberty dichotomy: There is no security without freedom, without equality.

This is why, as early as 1983, the Constitutional Court, in its still highly topical decision on the census ruling, urged that the effects of surveillance on individuals and society as a whole ought to be reviewed: "Those who are uncertain whether deviant behavior will be noted at any time and permanently stored, used, or passed on as information will try not to be conspicuous by such behavior. Anyone who expects that, for example, participation in a meeting or a citizens' initiative will be recorded by the authorities and that risks may arise for him as a result will possibly refrain from exercising his corresponding fundamental rights (Articles 8, 9 of the Basic Law)."[27]

In its way of pointing out and admonishing uncertainties, a theoretical rationale focuses on the (subconsciously) action-changing component of surveillance measures (chilling effects). From a legal perspective, the chilling effect describes the deterrent effect of an intervention in fundamental rights. Surveillance can lead to citizens no longer exercising their fundamental rights due to this intervention.[28]

This also restricts the opportunity for self-determined individual development. Due to the power relations of the surveillance measures and exist-

26 Dolderer, Dr. Winfried: Deutscher Bundestag—Bedenken gegen Entfristung von Vorschriften zur Terrorismusbekämpfung. In: Bundestag, November 2, 2020, https://www.bundestag.de/dokumente/textarchiv/2020/kw45-pa-innen-antiterrorgesetze-799842 (November 8, 2020).

27 BVerfG, 15.12.1983, 1 BvR 209/83: 146.

28 See also Assion, Simon: Chilling Effects und Überwachung. In: Telemedicus: Recht der Infomationsgesellschaft, November 26, 2014, https://www.telemedicus.info/article/2866-Chilling-Effects-und-UEberwachung.html (March 19, 2018).

ing discrimination, the impairment is less intense for some and more intense for others. The social effects on our free democratic social structure are noticeable when action and participation are restricted. If the restrictions are of different kinds and affect us differently as a society, this fundamentally changes us, affecting the understanding of us as a diverse and varied society and ultimately altering democratic processes such as political opinion-forming. Such so-called chilling effects are difficult to present in court in individual cases, and a legal review faces numerous obstacles.[29] It is, therefore, also of fundamental value to question how we can approach the solution of this associated social task. How do we want to shape the way we live together and upon which measures to be base this? Under which and whose order and control do we want this to happen? Who is the "we," and who decides these questions? For a long time, not taking these questions into account, seemed to be an option. But it has proven to not be a good one. The use of Algorithms forces us to address these pressing questions, to deal with them and take action.

Without fulfilling the state's duty to accompany this decision-making process openly and transparently, without conducting and deciding in respect of interdisciplinary perspectives rather than isolated and elitist mannerisms, we will never be able to close the gap between the demands of society as a whole and our existing Basic Law. We will never be able to implement the factual situation of likewise existing violations of fundamental rights due to surveillance, and in any case, never be able to uncover them in the first place.

The logic problem inherent in any surveillance measures is the lack of transparency anchored within them. While a small part of society accumulates more and more information and thus power, most of the population simply knows too little about these processes. This is exacerbated by the use of computer technologies, if those are built with lack of transparency, filled with unchecked data, deployed, and ultimately unevaluated results.

So, in conclusion is digital self-defense the only option left as a last resort for self-protection? A situation that would certainly not contribute to equal participation.

This is cynical, mainly because of the power relationship between citizens and the state, as even the state has not yet clarified its relationship to

29 Sass, Ineke: Wie Überwachung die Meinungsfreiheit gefährdet. In: Amnesty International, May 9, 2016, https://www.amnesty.de/informieren/blog/deutschland-wie-ueberwachung-die-meinungsfreiheit-gefaehrdet (May 24, 2021).
Staben, Julian: Der Abschreckungseffekt auf die Grundrechtsausübung, Tübingen 2016.

encryption. It is increasingly taking or giving itself the right to state intervention, for example, with the help of state Trojans. While civil society organizations, in turn, have to demand a stop to surveillance through judicial clarification30, the attempt at expansion is being continued by the state, even going so far as to oblige companies to support surveillance by distributing malware and thus hacking their customers.[31]

Human or Algorithms—Who or What Needs to be Surveilled?

Furthermore, who should be given the responsibility to answer these questions? When it comes to warrantless mass surveillance, fundamental decisions can probably only be made by society as a whole. What kind of world do we want to live in, in what proportion, how should power be distributed, who belongs to society and who is left outside? In mass surveillance, we cannot decipher who is affected by the surveillance and to what extent. Or do we? As for now, we simply surveil everyone by general suspicion in order to define the individual object of surveillance afterwards. It is easy to say "no" to this in principle, but it is probably impossible to draw the boundaries in practice.

In the case of individual surveillance, surveillance in the private sphere or commercial enterprises, the question of which forms of surveillance we want and which we do not want seems easier to answer. Not only legally but also factually. However, already, the proactive approach shows its faultiness.

Is it not a matter of feeling? Or is it? To do justice to the responsibility of using technology, we need to move away from the perhaps unconscious decision that it is sufficient to use feelings to legitimize social decisions up to and including legal bases. Neither concerning the decision for more robust and extensive surveillance measures to cover feelings of fear nor concerning an unreflective trust in technology. This is especially true for the increasing use of artificial intelligence, which can often lead to wrong decisions and increase discrimination, as we have shown. Black boxes, i.e., non-transparent,

30 Mattes, Anna Livia: Pressemitteilung: Verfassungsbeschwerde gegen Staatstrojaner eingelegt—GFF—Gesellschaft für Freiheitsrechte e.V.. In: Gesellschaft für Freiheitsrechte, August 24, 2018, https://freiheitsrechte.org/pm-vb-trojaner/ (November 8, 2020).

31 Meister, Andre and Biselli, Anna: Wir veröffentlichen den Gesetzentwurf—Seehofer will Staatstrojaner für den VerfassungsschutzIn: netzpolitik, March 28, 2019, https://netzpolitik.org/2019/wir-veroeffentlichen-den-gesetzentwurf-seehofer-will-staatstrojaner-fuer-den-verfassungsschutz/ (November 8, 2020).

self-contained systems whose structure and inner workings can only be inferred—if at all—from reactions to input signals, used in surveillance pose a double threat.

That Means we Have to Surveil the Right One: Algorithms

To ensure that existing discrimination and systemic biases are minimized rather than exacerbated by AI systems, there needs to be fundamental transparency in their design. Starting with the open labeling of such systems, they must be developed and designed to be as comprehensible and verifiable as possible. Explainable AI is the keyword here.

A documentation and logging obligation seems unavoidable in order to be able to detect and correct errors and wrong decisions. When using AI, not only must unintended conclusions about individual persons be prevented, but counterfactual explanations such as claims for information for affected persons about which factors led to an unfavorable decision are also imperative.

The higher the potential for harm, the higher the requirements to be applied to the criteria of AI systems. Nevertheless, what is the point of open standards, data quality, robustness, or data protection rules if an AI system is used for surreptitious surveillance? What is the point of data subjects having rights with respect to automated algorithmic decisions if they cannot enforce them due to lack of knowledge on surveillance? Does this mean that when surveillance is used, the use of AI systems should be banned altogether? It seems clear that in the case of facial recognition technology in public spaces, for example, we must speak of an unacceptable risk of harm. In view of the sensitivity of most of the areas affected, the intensity of the intervention, the number of people affected, or the irreversibility of decisions, will be affirmative for many areas. At this point, it must be said that there are certain areas of applied surveillance, for example, in the medical field, where the balance expresses itself differently.

However, who takes responsibility for deciding what technology should or should not accompany us in the future, what data it should work with, and to what extent it must be verifiable? Who decides which switches are the right ones and where they should lead, and who is ultimately responsible for them? Who develops, certifies, or standardizes them? Furthermore, what are the social and private implications of these answers? This requires a fundamental decision—personally and for society as a whole, in Germany, Europe, and

worldwide. Surveillance concerns us all. Opting out of the discourse has implications, usually on a larger scale for all those who are particularly affected by surveillance bias and its restrictions. We need to frame and conduct this debate in an intersectional feminist way, i.e., including power and domination structures, to view the different forms of discrimination and their effects. Otherwise, we cannot justly answer the questions on surveillance measures with or without AI systems—to how and with which result and to which extent concerning our future.

Literature

Assion, Simon: Chilling Effects und Überwachung. In: Telemedicus: Recht der Infomationsgesellschaft, November 26, 2014, https://www.telemedicus.info/article/2866-Chilling-Effects-und-UEberwachung.html (March 19, 2018).

Barr, Alistair: Google Mistakenly Tags Black People as "Gorillas," Showing Limits of Algorithms. In: The Wall Street Journal, July 1, 2015, http://blogs.wsj.com/digits/2015/07/01/google-mistakenly-tags-black-people-as-gorillas-showing-limits-of-algorithms/ (November 1, 2021).

Benjamin, Ruha: Race after technology: abolitionist tools for the new Jim code, Medford, MA 2019.

Biselli, Anna: Berlin: Keine rationalen Argumente für Videoüberwachung an S-Bahnhof. In: netzpolitik, March 1,2019, https://netzpolitik.org/2019/berlin-keine-rationalen-argumente-fuer-videoueberwachung-an-s-bahnhof/ (May 24, 2021).

Böhm, María Laura: Der Gefährder und das Gefährdungsrecht: eine rechtssoziologische Analyse am Beispiel der Urteile des Bundesverfassungsgerichts über die nachträgliche Sicherungsverwahrung und die akustische Wohnraumüberwachung, Göttingen 2011.

boyd, danah; Crawford, Kate: CRITICAL QUESTIONS FOR BIG DATA: Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society, xv/5 2012, pp. 662–679.

Browne, Simone: Dark matters: on the surveillance of blackness, Durham 2015.

Buolamwini, Joy; Gebru, Timnit: Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, (Proceedings of Machine Learning Research, 2018), lxxxi 2018, pp. 77–91.

Dolderer, Dr. Winfried: Deutscher Bundestag—Bedenken gegen Entfristung von Vorschriften zur Terrorismusbekämpfung. In: Bundestag, November 2, 2020, https://www.bundestag.de/dokumente/textarchiv/2020/kw45-pa-innen-antiterrorgesetze-799842 (November 8, 2020).

Eubanks, Virginia: Automating inequality: how high-tech tools profile, police, and punish the poor, New York, NY 2017.

Foucault, Michel: Überwachen und Strafen: Die Geburt des Gefängnisses, Frankfurt am Main 1977.

Fry, Hannah: Hello World: How to be Human in the Age of the Machine, London, New York, Toronto, Sidney, Auckland 2018.

Gless, Sabine: Predictive policing und operative Verbrechensbekämpfung. In: Felix Herzog, Reinhold Schlothauer, and Wolfgang Wohlers (eds), Rechtsstaatlicher Strafprozess und Bürgerrechte, Gedächtnisschrift für Edda Weßlau, Berlin 2016.

Gorner, Jeremy: Chicago Police Use Heat List as Strategy to Prevent Violence. In: Chicago Tribune, 2013, http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list (November 1, 2021).

Grieger, Fabian; Schlindwein, Simone: Migrationspolitik und Rüstungsindustrie: Das Geschäft mit Hightech-Grenzen. In: taz.de, die tageszeitung 2016.

Haggerty, Kevin D.; Ericson, Richard V.: The surveillant assemblage. In: The British Journal of Sociology, li/4 2000, pp. 605–622.

henning: Trügerische Sicherheit: Der elektronische Personalausweis. In: Chaos Computer Club, September 15, 2013, https://www.ccc.de/de/updates/2013/epa-mit-virenschutzprogramm (May 24, 2021).

Lyon, David (Ed.): Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination, London 2003.

Mattes, Anna Livia: Pressemitteilung: Verfassungsbeschwerde gegen Staatstrojaner eingelegt—GFF—Gesellschaft für Freiheitsrechte e.V. In: Gesellschaft für Freiheitsrechte, August 24, 2018, https://freiheitsrechte.org/pm-vb-trojaner/ (November 8, 2020).

Meister, Andre; Biselli, Anna: Wir veröffentlichen den Gesetzentwurf—Seehofer will Staatstrojaner für den Verfassungsschutz. In: netzpolitik, March 28, 2019, https://netzpolitik.org/2019/wir-veroeffentlichen-den-gesetzentwurf-seehofer-will-staatstrojaner-fuer-den-verfassungsschutz/ (November 8, 2020).

Merz, Christina: Predictive Policing—Polizeiliche Strafverfolgung in Zeiten von Big Data, Karlsruher Institut für Technologie (KIT), 2016, https://publikationen.bibliothek.kit.edu/1000054372 (November 1, 2021).

Neumann, Linus: Untersuchung: Vorratsdatenspeicherung ist ineffektiv. In: netzpolitik, January 27, 2011, https://netzpolitik.org/2011/untersuchung-vorratsdatenspeicherung-ist-ineffektiv/ (May 24, 2021).

Noble, Safiya Umoja: Algorithms of Oppression: How Search Engines Reinforce Racism, New York 2018.

O'Neil, Cathy: Weapons of math destruction: how big data increases inequality and threatens democracy, New York 2016.

Picard, Rosalind W.: Affective computing, Cambridge, Mass 2000.

Sass, Ineke: Wie Überwachung die Meinungsfreiheit gefährdet. In: Amnesty International, May 9, 2016, https://www.amnesty.de/informieren/blog/deutschland-wie-ueberwachung-die-meinungsfreiheit-gefaehrdet (May 24, 2021).

Snow, Jacob: Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots. In: American Civil Liberties Union, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 (August 11, 2019).

Staben, Julian: Der Abschreckungseffekt auf die Grundrechtsausübung, Tübingen 2016.

Steinschaden, Jakob: Der "Chilling Effect": Massenüberwachung zeigt soziale Folgen—Netzpiloten.de. In: Netzpiloten Magazin, April 7, 2014, https://www.netzpiloten.de/der-chilling-effect-massenueberwachung-zeigt-soziale-folgen/ (May 24, 2021).

Wajcman, Judy: TechnoFeminism, Cambridge UK 2004.
Wermter, Benedict: Schnüffeln auf Facebook. In: Correctiv. Recherche für die Gesellschaft, June 22, 2015, https://correctiv.org/aktuelles/auskunftsrechte/2015/06/22/schnueffeln-auf-facebook/ (July 26, 2019).