16

Artificial Intelligence and the Right to Data Protection

Ralf Poscher

In respect of technological advancement, the law often comes into play merely as an external restriction. That is, lawyers are asked whether a given technology is consistent with existing legal regulations or to evaluate its foreseeable liability risks. As a legal researcher, my interest is the exact opposite: how do new technologies influence our legal framework, concepts, and doctrinal constructions? This contribution shows how Artificial Intelligence (AI) challenges the traditional understanding of the right to data protection and presents an outline of an alternative conception, one that better deals with emerging AI technologies.

I. TRADITIONAL CONCEPT OF THE RIGHT TO DATA PROTECTION

In the early stages of its data protection jurisprudence, the German Federal Constitutional Court took a leading role in establishing the right to data protection, not only in Germany, but also in the European context.[1] In the beginning, it linked the 'right to informational self-determination' to a kind of property rights conception of personal data.[2] The Court explained that every individual has a 'right to determine himself, when and in which boundaries personal data is disseminated'[3] – just as an owner has the right to determine herself when she allows someone to use her property.[4] This idea, which is already illusory in the analog world, has often been ridiculed as naive in our contemporary, technologically interconnected and socially networked reality, in which a vast spectrum of personal data is disseminated and exchanged at all levels almost all of the time.[5] Data simply does not possess the kind of exclusivity to justify parallels

[1] M Albers, 'Realizing the Complexity of Data Protection' in S Gutwirth, R Leenes, and P De Hert (eds), *Reloading Data Protection* (2014) 217 (hereafter Albers, 'Complexity'); K Vogelsang, *Grundrecht auf Informationelle Selbstbestimmung?* (1987) 39–88.

[2] There is a certain parallel between this conceptualization of the right to privacy and its scope under the US Supreme Court's early Fourth Amendment jurisprudence: the Supreme Court, until *Katz v United States* 389 US 347 [1967], applied the Fourth Amendment only to the search and seizure of a citizen's personal property and effects (see, e.g., *Olmstead v United States* 277 US 438 [1928]) and was thus tied in substance to a property right.

[3] BVerfGE 65, 1 (42) (BVerfG *1 BvR 209/83*): ‚Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.'

[4] Albers, 'Complexity' (n 1) 219.

[5] M Albers, 'Information als neue Dimension im Recht' (2002) 33 *Rechtstheorie* 61 (81) (hereafter Albers, 'Information'); K Ladeur, 'Das Recht auf Informationelle Selbstbestimmung: Eine Juristische Fehlkonstruktion?'(2009) 62 *DÖV* 45 (46–47).

https://doi.org/10.1017/9781009207898.022 Published online by Cambridge University Press

with property ownership.[6] The German Constitutional Court seems to have recognized this. And while the Court has not explicitly revoked the property-like formula, it has made decreasing use of it, and in more recent decisions, has not referred to it at all.[7]

Even if everyone can agree that the right to data protection is, in substance, not akin to a property interest in one's personal data, the right to data protection is formally handled as if it were a property right. In the same way that any non-consensual use of one's property by someone else is regarded a property rights infringement, any non-consensual use – gathering, storage, processing, and transmission – of personal data is viewed as an infringement of the right to data protection. This formal conception of data protection is not only still prevalent in the German context, but the European Court of Justice (ECJ) perceives the right to data protection under Article 8 of the Charter of Fundamental Rights of the European Union (CFR) in much the same way. In one of its latest decisions, the ECJ confirmed that data retention as such constitutes an infringement irrespective of substantive inconveniences for the persons concerned:

> It should be made clear, in that regard, that the retention of traffic and location data constitutes, in itself, … an interference with the fundamental rights to respect for private life and the protection of personal data, enshrined in Articles 7 and 8 of the Charter, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference.[8]

According to the traditional perspective, each and every processing of personal data infringes the respective right – just as the use of physical property would be an infringement of the property right.[9] For instance, if my name, license plate, or phone number is registered, this counts as an infringement; if they are stored in a database, this counts as another infringement; and if they are combined with other personal data, such as location data, this counts as yet another infringement.[10] Even though the right to data protection is not regarded as a property right, its formal structure still corresponds with that of a property right.

This conceptual approach is a mixed blessing. On the one hand, it provides a very analytic approach to the data processing in question. On the other hand, the idea of millions of fundamental rights infringements occurring in split seconds by CPUs processing personal data seems a rather exaggerated way of conceptualizing the actual problems at hand. Nevertheless, modern forms of data collection are still conceptualized in this way, including automated license plate recognition, whereby an initial infringement occurs by using scanners to collect license plate information and another infringement by checking this information against stolen car databases,[11] etc.

[6] Cf. J Fairfield and C Engel, 'Privacy as a Public Good' in RA Miller (ed), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (2017).

[7] E.g., BVerfGE 120, 351 (360) (BVerfG *1 BvR 2388/03*); BVerfGE 120, 378 (397–398) (BVerfG *1 BvR 2074/05*).

[8] CJEU, Joined Cases C-511/18, C-512/18, and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* (6 October 2020), para 115 (hereafter CJEU, *La Quadrature du Net*).

[9] Albers, 'Complexity' (n 1) 219.

[10] BVerfGE 100, 313 (366) (BVerfG *1 BvR 2226/94*); BVerfGE 115, 320 (343–344) (BVerfG *1 BvR 518/02*); BVerfGE 125, 260 (310) (BVerfG *1 BvR 256, 263, 586/08*); BVerfGE 130, 151 (184) (BVerfG *1 BvR 1299/05*); BVerfGE 150, 244 (265–266) (BVerfG *1 BvR 142/15*).

[11] BVerfGE 120, 378 (400–401) (BVerfG *1 BvR 1254/05*); BVerfGE 150, 244 (266) (BVerfG *1 BvR 142/15*).

II. THE INTRANSPARENCY CHALLENGE OF AI

AI technology is driven by self-learning mechanisms.[12] These self-learning mechanisms can adapt their programmed algorithms reacting to the data input.[13] Importantly, while the algorithms may be transparent to their designers,[14] after the system has cycled through hundreds, thousands, or even millions of recursive, self-programming patterns, even the system programmers will no longer know which type of data was processed in which way, which inferences were drawn from which data correlations, and how certain data have been weighted.[15]

The self-adaptive 'behavior' of at least certain types of AI technologies leads to a lack of transparency. This phenomenon is often referred to as the black box issue of AI technologies.[16] Why is this a problem for the traditional approach to evaluating data protection?

The analytical approach is based on the justification of each and every processing of personal data. In AI systems, however, we do not know which individual personal data have been used and how many times they have been processed and cross-analyzed with what types of other data.[17] It is thus impossible to apply the analytical approach to determine whether, how many, and what kind of infringements on a thus conceived right to data protection occurred. AI's lack of transparency seems to rule this out. Thus, AI creates problems for the traditional understanding and treatment of the right to data protection due to its lack of transparency.[18] These issues are mirrored in the transparency requirements of the General Data Protection Regulation, which rests very much on the traditional conception of the fundamental right to data protection.[19]

III. THE ALTERNATIVE MODEL: A NO-RIGHT THESIS

The alternative conceptualization of the right to data protection that I would like to suggest consists of two parts.[20] The first part sounds radical, revisionary, and destructive; the second part resolves the tension created by a proposal that is doctrinally mundane but shifts the perspective

[12] H Surden, 'Machine Learning and Law' (2014) 89 *Washington L Rev* 87 (88–90) (hereafter Surden, 'Machine Learning'); W Hoffmann-Riem, 'Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht' (2017) 142 *AöR* 3 (hereafter Hoffmann-Riem, 'Verhaltenssteuerung'); W Hoffmann-Riem, 'Artificial Intelligence as a Challenge for Law and Regulation' in T Wischmeyer and T Rademacher (eds), *Regulating Artificial Intelligence* (2020) 3 (hereafter Hoffmann-Riem, 'Artificial Intelligence').

[13] Surden, 'Machine Learning' (n 12) 93.

[14] Hoffmann-Riem, 'Verhaltenssteuerung' (n 12) 30.

[15] Hoffmann-Riem, 'Artificial Intelligence' (n 12), 17; Hoffmann-Riem, 'Verhaltenssteuerung' (n 12) 29; N Marsch, 'Artificial Intelligence and the Fundamental Right to Data Protection' in T Wischmeyer and T Rademacher (eds), *Regulating Artificial Intelligence* (2020) 36 (hereafter Marsch, 'Artificial Intelligence'); T Wischmeyer, 'Artificial Intelligence and Transparency: Opening the Black Box' in T Wischmeyer and T Rademacher (eds), *Regulating Artificial Intelligence* (2020) 81 (hereafter Wischmeyer, 'Artificial Intelligence').

[16] Hoffmann-Riem, 'Verhaltenssteuerung' (n 12) 29; Marsch, 'Artificial Intelligence' (n 15) 36; Wischmeyer, 'Artificial Intelligence' (n 15) 80.

[17] Cf. Albers, 'Complexity' (n 1) 221: 'The entire approach is guided by the idea that courses of action and decision-making processes could be almost completely foreseen, planned and steered by legal means'; Marsch, 'Artificial Intelligence' (n 15) 39.

[18] Marsch, 'Artificial Intelligence' (n 15) 36.

[19] On the specifics of the transparency requirements generally stated in Articles 5(1)(a) alt. 3 GDPR and the issues the cause for the use of AI-technologies, B Paal, Chapter 17 in this volume.

[20] For a more general discussion of this alternative account, see R Poscher, 'Die Zukunft der Informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen' in H Gander and others (eds), *Resilienz in der offenen Gesellschaft* (2012) 171–179; R Poscher, 'The Right to Data Protection' in RA Miller (ed), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (2017) 129–141.

on data protection rights substantially. Among other advantages, the proposed shift in perspective could render the right to data protection more suitable for handling issues arising from AI.

The first part is a no-right-thesis. It contends that there is no fundamental right to data protection. That is, the right to data protection is not a right of its own standing. This explains why the ongoing quest for a viable candidate as the proper object of the right to data protection has been futile.[21] Article 8 CFR, which seems to guarantee the right to data protection as an independent fundamental right, rests on the misunderstanding that the fundamental rights developments in various jurisdictions, namely also in the jurisdiction of the German Federal Constitutional Court, have created a new, substantive fundamental right with personal data as its object. There is no such new, substantive fundamental right. This, however, does not mean that there is no fundamental rights protection against the collection, storage, processing, and dissemination of personal data. Yet data protection does not take the form of a new fundamental right – property-like or otherwise.

The second part of the thesis reconstructs the 'right' by shifting the focus to already existing fundamental rights. Data protection is provided by all of the existing fundamental rights, which can all be affected by the collection, storage, processing, and dissemination of personal data.[22] In his instructive article 'A Taxonomy of Privacy', *Daniel Solove* developed a whole taxonomy of possible harms that can be caused by data collection.[23] They include the loss of life and liberty, infringements on property interests and the freedom of expression, violations of privacy, and denials of due process guarantees. It is easy to see how the dissemination of personal finance information can lead to the loss of property. He cites tragic cases, which have even led to a loss of life, such as when a stalker was handed the address of his victim by public authorities – data he used to locate and kill her.[24] *Solove's* list suggests that the essence of data protection cannot be pinned down to merely a single liberty or equality interest but instead potentially involves every fundamental right. Understood correctly, the right to data protection consists in the protection that all fundamental rights afford to all the liberty and equality interests that might be affected by the collection, storage, processing, and dissemination of personal data.

The way in which fundamental rights protect against the misuse of personal data relies on doctrinally expanding the concept of rights infringement. Fundamental rights usually protect against actual infringements. For example, the state encroaches upon your right of personal freedom if you are incarcerated, your right to freedom of assembly is infringed when your meeting is prohibited or dispersed by the police, and your freedom of expression is violated when you are prevented from expressing your political views. Usually, however, fundamental rights do not protect against the purely abstract danger that the police might incarcerate you, might disperse your assembly, or might censor your views. You cannot go to the courts claiming that certain police behavioral patterns increase the danger that they might violate your right to assembly. The courts would generally say that you have to wait until they either already do so or are in the concrete process of doing so. In some cases, your fundamental rights might already protect you if there is a concrete danger that such infringements are about to take place, so that

[21] C Gusy, 'Informationelle Selbstbestimmung und Datenschutz: Fortführung oder Neuanfang?' (2000) 83 *KritV* 52, 56–63; K Ladeur, 'Das Recht auf Informationelle Selbstbestimmung: Eine Juristische Fehlkonstruktion?' (2009) 62 *DÖV* 45, 47–50.

[22] N Marsch, *Das Europäische Datenschutzgrundrecht* (2018), 92 (hereafter Marsch, 'Datenschutzgrundrecht').

[23] DJ Solove, 'A Taxonomy of Privacy' (2006) 154 *U Pennsylvania L Rev* 477; see also DJ Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 *San Diego L Rev* 745, 764–772 (hereafter Solove, 'Misunderstandings of Privacy').

[24] Solove, 'Misunderstandings of Privacy' (n 23) 768.

you do not have to suffer the infringement in the first place if it were to violate your rights.[25] These cases, however, are exceptions.

The right to data protection works differently. What is unique about data protection is its generally preemptive character. It already protects against the abstract dangers involved in the collection, storage, and processing of personal data.[26] Data protection preemptively protects against violations of liberty or equality interests that are potentially connected to *using* personal data.[27] The collection, aggregation, and processing of data as such does no harm.[28] This has often been expressed in conjunction with the idea that data needs to become information in certain contexts before it gains relevance.[29] It is only the use of data in certain contexts that might involve a violation of liberty or equality interests. The collection of personal data on political or religious convictions of citizens by the state is generally prohibited, for example, because of the potential that it could be misused to discriminate against political or religious groups. Data protection demands a justification for the collection of personal data, even if such misuse is only an abstract danger.[30] It does not require concrete evidence that such misuse took place, or even that such misuse is about to take place. The right to data protection systematically enhances every other fundamental right already in place to protect against the abstract dangers that accompany collecting and processing personal data.[31]

A closer look at the court practice regarding the right to data protection reveals that, despite appearances, courts neither treat the right to data protection as a right on its own but instead associate it with different fundamental rights, depending on the context and the interest affected.[32] Even at the birth of the right to data protection in Germany, in the famous "Volkszählungs-Urteil" (census decision), the examples the court gave to underline the necessity for a new fundamental right to 'informational self-determination' included a panoply of

[25] See BVerfGE 51, 324 (BVerfG *2 BvR 1060/78*), in which the Court saw it as an infringement of the right to physical integrity to proceed with a criminal trial if the defendant runs the risk of suffering a heart attack during the trial; cf. also BVerfGE 17, 108 (BVerfG *1 BvR 542/62*) (high-risk medical procedure – lumbar puncture – with the aim of determining criminal accountability for a misdemeanor); BVerfGE 52, 214 (220) (BVerfG *1 BvR 614/79*)(eviction of a suicidal tenant) and R Poscher, *Grundrechte als Abwehrrechte* (2003) 388–390 (hereafter Poscher, 'Abwehrrechte').

[26] Cf. Marsch, 'Datenschutzgrundrecht' (n 22) 109, with a focus on the internal peace of mind of deciding on one's exercise of fundamental rights.

[27] E.g., the collection of comprehensive data in the course of a nationwide census is not in itself an imminent threat, but it is dangerous because of the potential (mis-)use of the masses of the gathered mass data, cf. BVerfG 65, 1 (BVerfG *1 BvR 209/8*); the collection of data for an anti-terrorism or anti-Nazi database is problematic because of *potential* negative impacts for those mentioned in it, cf. BVerfGE 133, 277 (331–332) (BVerfG *1 BvR 1215/07*).

[28] Albers, 'Complexity' (n 1) 225.

[29] M Albers, 'Zur Neukonzeption des Grundrechtlichen „Daten"Schutzes' in A Haratsch and others (eds), *Herausforderungen an das Recht der Informationsgesellschaft* (1996) 121–23, 131–33; Albers, 'Information' (n 5) 75; M Albers, *Informationelle Selbstbestimmung* (2005) 87–148; M Albers, 'Umgang mit Personenbezogenen Informationen und Daten' in W Hoffmann-Riem, E Schmidt-Aßmann and A Voßkuhle (eds) *Grundlagen des Verwaltungsrechts* (2nd ed. 2012) 7–28; G Britz, 'Informationelle Selbstbestimmung Zwischen Rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts' in W Hoffmann-Riem (ed), *Offene Rechtswissenschaft* (2010) 566–568 (hereafter Britz, 'Informationelle Selbstbestimmung'); Albers, 'Complexity' (n 1) 222–224.

[30] Cf. the examples mentioned in note 27. This pre-emptive protection against state action is not to be confused with the duties to protect against *unlawful* infringements of liberty interests by *third parties*, cf. Poscher, 'Abwehrrechte' (n 25) 380–387 on the duty to protect under the German Basic Law. As far as such duties to protect are accepted, data protection would also address pre-emptive dimensions of these duties.

[31] Cf. J Masing, 'Datenschutz – ein unterentwickeltes oder überzogenes Grundrecht?' (2014) *RDV* 3 (4); Marsch, 'Datenschutzgrundrecht' (n 22) 109–110; T Rademacher, 'Predictive Policing im Deutschen Polizeirecht' (2017) 142 *AöR* 366 (402); Marsch, 'Artificial Intelligence' (n 15) 40.

[32] Cf. Britz, 'Informationelle Selbstbestimmung' (n 29) 571, 573, who first characterized the German right to informational self-determination as an 'accessory' right.

fundamental rights, such as the right to assembly.[33] In an unusual process of constitutional migration, the court pointed to the 'chilling effects' the collection of data on assembly participation could have for bearers of that right,[34] as they were first discussed by the US Supreme Court.[35] The German Federal Court drew on an idea developed by the US Supreme Court to create a data protection right that was never accepted by the latter. Be that as it may, even in its constitutional birth certificate, data protection is not put forth as a right on its own but associated with various substantive fundamental rights, such as the right to assembly.

Further evidence of the idea that personal data is not the object of a substantive stand-alone right is provided by the fact that data protection does not seem to stand by itself, even in a jurisdiction in which it is explicitly guaranteed. Article 8 CFR explicitly guarantees a right to data protection. In the jurisprudence of the Court of Justice of the European Union, however, it is always cited in conjunction with another right.[36] The right to data protection needs another right in order to provide for a substantive interest – usually the right to privacy,[37] but sometimes also other rights, such as free speech.[38] Thus, even when data protection is codified as an explicit, independent fundamental right, as it is in the Charter, it is nevertheless regarded as an accessory to other more substantive fundamental rights.[39] This is odd if the right to data protection is taken at face value as a substantive right on its own but only natural if taken as a general enhancement of other fundamental rights.

IV. THE IMPLICATION FOR THE LEGAL PERSPECTIVE ON AI

If the right to data protection consists in a general enhancement of, potentially, every fundamental right in order to already confront the abstract dangers to the liberty and equality interests they protect, it becomes clear how personal data processing systems must be evaluated. They have to be evaluated against the background of the question: to what extent does a certain form of data collection and processing system pose an abstract danger for the exercise of what type of fundamental right? Looking at data collection issues in this way has important implications – including for the legal evaluation of AI technologies.

1. *Refocusing on Substantive Liberty and Equality Interests*

First, the alternative conception allows us to rid ourselves of a formalistic and hollow understanding of data protection. It helps us to refocus on the substantive issues at stake. For many people, the purely formal idea that some type of right is always infringed when a piece of personal information has been processed, meaning that they have to sign a consent agreement or

[33] BVerfGE 65, 1 (43) (BVerfG *1 BvR 209/83*).
[34] BVerfGE 65, 1 (43) (BVerfG *1 BvR 209/83*).
[35] *Wieman v Updegraff* 344 US 183 (1952), para 195.
[36] CJEU, Joined Cases C-92/09 and C-93/09 *Schecke and Eifert v Hesse* [2010] ECR I-11063, para 47; CJEU, Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Siochana, Ireland and the Attorney General and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others* (8 April 2014), para 53 (hereafter CJEU, *Digital Rights Ireland*); CJEU, Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (6 October 2015), para 78; CJEU, Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems* (16 July 2020), para 168.
[37] CJEU, *Digital Rights Ireland* (n 36) para 37; CJEU, *La Quadrature du Net* (n 8) para 115.
[38] CJEU, *Digital Rights Ireland* (n 36) para 28; CJEU, *La Quadrature du Net* (n 8) para 118; CJEU, Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (6 October 2020), para 72.
[39] Marsch, 'Datenschutzgrundrecht' (n 22) 132–133.

https://doi.org/10.1017/9781009207898.022 Published online by Cambridge University Press

click a button, has become formalistic and stale in the context of data protection regulation. The connection to the actual issues that are connected with data processing has been lost. For example, during my time as vice dean of our law faculty, I attempted to obtain the addresses of our faculty alumni from the university's alumni network. The request was denied because it would constitute an infringement of the data protection right of the alumni. The alumni network did not have the written consent of its members to justify this infringement. As absurd as this might seem, this line of argument is the only correct one for the traditional, formal approach to data protection. Addresses are personal data and any transfer of this personal data is an infringement of the formal right to data protection, which has to be justified either by consent or by a specific statute – both of which were lacking. This is, however, a purely formal perspective. Our alumni would probably be surprised to know that the faculty at which they studied for years, which handed them their law degrees, and which paved the road to their legal career does not know that it is their alma mater. There is no risk involved for any of their fundamental rights when the faculty receives their address information from the alumni network of the very same university. An approach that discards the idea that there is a formal right to data protection, but asks which substantive fundamental rights positions are at stake, can resubstantialize the right to data protection. This also holds for AI systems: the question would not be what type of data is processed when and how but instead what kind of substantive, fundamental right position is endangered by the AI system.

2. *The Threshold of Everyday Digital Life Risks*

Second, refocusing on the abstract danger for concrete, substantive interests protected by fundamental rights allows for a discussion on thresholds. Also, in the analog world, the law does not react to each and every risk that is associated with modern society. Not every abstract risk exceeds the threshold of a fundamental rights infringement. There are general life risks that are legally moot. In extreme weather, even healthy trees in the city park carry the abstract risk that they might topple, fall, and cause considerable damage to property or even to life and limb. Courts, however, have consistently held that this abstract danger does not allow for public security measures or civil claims to chop down healthy trees.[40] They consider it part of everyday life risks that we all have to live with if we stroll in public parks or use public paths.

The threshold for everyday life risks holds in the analog world and should hold in the digital world, too. In our digital society, we have to come to grips with a – probably dynamic – threshold of everyday digital life risks that do not constitute a fundamental rights infringement, even though personal data have been stored or processed. On one of my last visits to my physician, I was asked to sign a form that would allow his assistants to use my name, which is stored in their digital patient records, in order to call me from the waiting room when the doctor is ready to see me. The form cited the proper articles of the, at the time, newly released General Data Protection Regulation of the European Union (Articles 6(1)(a) and 9(2)(a)). There might be occasions where there is some risk involved in letting other patients know my name. If the physician in question were an oncologist, it might lead to people spreading the rumor that I have a terminal illness. This might find its way to my employer at a time when my contract is up for an extension. So, there can indeed be some risk involved. We have, however, always accepted this risk – also in a purely analog world – as one that comes with the visit of physicians, just as we have accepted the risk of healthy trees being uprooted by a storm and damaging our houses, cars,

[40] VG Minden (11 K 1662/05) [2005], para 32.

https://doi.org/10.1017/9781009207898.022 Published online by Cambridge University Press

or even hurting ourselves. As we have accepted everyday life risks in the analog world, we have to accept everyday digital life risks in the digital world.

For AI technologies, this could mean that they can be designed and implemented in a way that they remain below the everyday digital life risk threshold. When an AI system uses anonymized personal data, there is always a risk that the data will be deanonymized. If sufficient safeguards against deanonymization are installed in the system, however, they may lower the risk to such a degree that it does not surpass the level of our everyday digital life risk. This may be the case if the AI system uses data aggregation for planning purposes or resource management, which do not threaten substantive individual rights positions. An example of a non-AI application is the German Corona-Warn-App, which is designed in such a way as to avoid centralized storage of personal data and thus poses almost no risk of abuse.

3. *A Systemic Perspective*

Third, the alternative approach implies a more systemic perspective on data collection and data processing measures. It allows us to step back from the idea that each and every instance of personal data processing constitutes an infringement of a fundamental right. If data protection is understood as protection against abstract dangers, then we do not have to look at the individual instances of data processing. Instead, we can concentrate on the data processing system and its context in order to evaluate the abstract danger it poses.

Unlike the traditional approach, focusing on abstract dangers for substantive fundamental rights that are connected with AI technologies does not require the full transparency of the AI system. The alternative approach does not require exact knowledge of when and how what kind of data is processed. What it needs, however, is a risk analysis and an evaluation of the risk reduction, management, correction, and compensation measures attuned to the specific context of use.[41] It requires regulation on how false positives and negatives are managed in the interaction between AI and human decision makers. At the time of our conference, the *New York Times* reported on the first AI-based arrest generated by a false positive of facial recognition software.[42] As discussed in the report, to rely solely on AI-based facial recognition software for arrests seems unacceptable given the failure rate of such systems. Legal regulation has to counterbalance the risks stemming from AI by forcing the police to corroborate AI results with additional evidence. A fundamental rights analysis of the facial recognition software should include an evaluation not only of the technology alone but also of the entire sociotechnological arrangement in the light of *habeas corpus* rights and the abstract dangers for the right to personal liberty that come with it. The actual cases, however, are not about some formal right to data protection but about substantive rights, such as the right to liberty or the right against racial discrimination, and the dangers AI technologies pose for these rights.

For AI technologies, the differences between the traditional approach and the suggested approach regarding the right to data protection are similar to differences in the scientific approach to, and the description of, the systems as such. Whereas traditionally the approach to, and the description of, computational systems has been very much dominated by computer sciences, there is a developing trend to approach AI systems – especially because of their lack of informational transparency – with a more holistic intradisciplinary methodology. AI systems are

[41] Cf. Albers, 'Complexity' (n 1) 232, who draws a parallel to risk management in environmental law.

[42] K Hill, 'Wrongfully Accused by an Algorithm' *New York Times* (24 June 2020). nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

studied in their deployment context with behavioral methodologies which are not so much focused on the inner informational workings of the systems but on their output and their effects in a concrete environment.[43] The traditional approach tends toward a more technical, informational analysis of AI systems, which is significantly hampered by the black box phenomenon. The shift to the substantive rights perspective would lean toward a more behavioral approach to AI. The law would not have to delve into the computational intricacies of when and how what type of personal data is processed. It could take a step back and access how an AI system 'behaves' in the concrete sociotechnological setting it is employed in and what type of risks it generates for which substantive fundamental rights.

V. CONCLUSION

From a doctrinal, fundamental rights perspective, AI could have a negative and a positive implication. The negative implication pertains to the traditional conceptualization of data protection as an independent fundamental right on its own. The traditional formal model, which focuses on each and every processing of personal data as a fundamental rights infringement could be on a collision course with AI's technological development. AI systems do not provide the kind of transparency that would be necessary to stay true to the traditional approach. The positive implication pertains to the alternative model I have been suggesting for some time. The difficulties AI may pose for the traditional conceptualization of the right to data protection could generate some wind beneath the wings of the alternative conception, which seems better equipped to handle AI's black box challenge with its more systemic and behavioral approach. The alternative model might seem quite revisionary, but it holds the promise of redirecting data protection toward the substantive fundamental rights issues at stake – also, but not only, with respect to AI technologies.

[43] An overview on this emerging field in I Rahwan and others, 'Machine behaviour' (2019) 568 *Nature* 477 (481–482).

https://doi.org/10.1017/9781009207898.022 Published online by Cambridge University Press