Prof. Dr. Mario Martini

Chair of Public Administration, Public Law, Administrative Law and European Law, German University of Administrative Sciences Speyer,
Director of the program area "Transformation of the state in the digital age" at the German Research Institute for Public Administration,
Member of the Data Ethics Commission appointed by the German Federal Government

FUNDAMENTALS OF A REGULATORY SYSTEM FOR ALGORITHM-BASED PROCESSES

– Expert opinion prepared on behalf of the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband)* –

1/5/19

Gefördert durch:

aufgrund eines Beschlusses
des Deutschen Bundestages

Recommended citation:

Martini, Fundamentals of a Regulatory System for Algorithm-based Processes, Speyer, 2019.

A. Out of control? Algorithms as navigators in the digital world

Higher processor speeds, cheaper and larger storage capacities, ubiquitous access to the internet and increasing use of media throughout the population make it possible: artificial intelligence and algorithms have advanced to central keystones in digital societies.[1] They affect our lives in a multitude of ways with lasting effects.[2] Algorithms help consumers to choose the best product, employers to select the best employee and support universities in their admission processes. They take independent financial transaction decisions[3], predict which patient is likely to suffer from a heart attack, compose music, create comics and perfumes, and can even autonomously devise scientific publications.[4]

Artificial intelligence is more than just another toy in the sandbox of digital technology. It profoundly impacts our social interaction and its rules. Machine learning software influences important decisions of society and can sometimes outperform people in their cognitive performance. Thus, the cybernetic vision of a future in which man and machine fuse takes shape.

However, algorithmic decision processes can emulate black boxes. Firstly, they use machine learning processes (including so-called *deep learning* of artificial neuronal networks) in a dynamic manner that is hardly comprehensible from the outside. Secondly, proprietary software applications do not allow for any insights into the source code (for legal reasons by virtue of the protection of trade secrets).[5]

---

* This expert opinion is, especially in part B (p. 8 ff.), based on the author's publications "Algorithmen als Herausforderung für die Rechtsordnung", JZ 2017, 1017 ff. as wells as the monograph "Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz" (Berlin et al., 2019) and integrates the views expressed in these publications in its argumentation. In order to restrict this text to the most essential aspects, it includes only a limited number of references. Extensive references to literature can be found in the monograph. Online sources were last accessed on 14/4/2019. The author thanks *Jonathan Hain, Matthias Hohmann, Michael Kolain, Anna Ludin*, *Jan Mysegades* and *David Nink* for their valuable support. Originally, this expert opinion was published in German titled "Grundlinien eines Kontrollsystems für algorithmenbasierte Entscheidungsprozesse". It was translated into English by *Alice Regina Bertram* and *Stefanie Zenzen*.

[1] Regarding the growing importance of algorithms cf., for example, *Coglianese/Lehr,* Georgetown Law Journal 105 (2017), 1147 (1149 ff.); *Hoffmann-Riem*, AöR 142 (2017), 1 (4 f.); *Tutt,* Administrative Law Review 69 (2017), 83 (84 ff.).

[2] *Martini,* JZ 2017, 1017 (1017).

[3] See *Martini*, Blackbox Algorithmus, 2019, p. 146 ff. on the differentiated regulatory control concept of algorithmic trading.

[4] *Pluta*, Algorithmus schreibt wissenschaftliches Buch, golem.de, 16/4/2019.

[5] These applications are distinct from so-called open-source software: source code of open-source-software is publicly accessible (e. g. via GitHub.com). While open-source applications provide transparency regarding the underlying data processing algorithms, the number of people who can put software applications through its

Algorithms have the air of objectivity and truth. However, they are by no means impartial, but reflect the (subliminal) values of their creators in their specific operation.[6] In an opaque decision-making structure, users cannot reliably detect risks of discrimination. An incorrect data basis, an erroneous code or an improper configuration of a decision-making system can yet have lasting effects on both, the rights of the data subjects and the chances of the controllers to prevail in competition.[7]

In order to mitigate the risks of automated decision-making and the preliminary stages of the computer-aided assistance of a human decision (in combination referred to as: algorithm-based decision-making processes[8]) in areas sensitive to fundamental rights, a *one-size-fits-all*-approach is comparably easy to implement legally and therefore seems appealing. However, a simplified approach would fail to do justice to the complex reality of the matter subject to regulation. The methods and areas of life and economic sectors in which algorithm-based procedures are used are simply too diverse. Instead, a well-balanced, finely-tailored system of protection[9] is needed, consisting of a diversified set of regulation instruments.[10]

---

paces (because they understand the software's complexities) is relatively small. Furthermore, each software application allows for personal configurations of specific program parts. The average consumer is in his interaction with digitalised applications therefore ultimately dependent on an intermediate and on testing even when using open-source software.

[6] *Martini,* Blackbox Algorithmus, 2019, p. 48 ff.

[7] The risks of opacity, discrimination and the monopolisation of both market power and power over opinion are more widely discussed in *Martini*, JZ 2017, 1017 (1017 ff.) and *Martini,* Blackbox Algorithmus, 2019, p. 27 ff.

[8] Also commonly used is the term "ADM" – algorithmic decision-making.

[9] For a detailed discussion see *Busch*, Algorithmic Accountability, 2018; *Ernst,* JZ 2017, 1026 (1026, 1031 ff.); *Herberger,* NJW 2018, 2825 (2826 ff.); *Hoffmann-Riem,* AöR 142 (2017), 1 (20 ff.); *Schweighofer/Sorge et al*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, October 2018, p. 132 ff.*; Schwintowski*, NJOZ 2018, 1601 (1606 ff.); *Wischmeyer*, AöR 143 (2018), 1 (18 ff.). For international discussions cf. *Citron/Pasquale*, Washington Law Review 89 (2014), 1 ff.; *Edwards/Veale*, Duke Law & Technology Review 16 (2017), 18 (18 ff.) with further notes (above all fn. 4); these authors compare the political discussion with the invisible force of the market in the 19th century (19 f.); *Pasquale*, The Black Box Society, 2015; *Tene/ Polonetsky*, Northwestern Journal of Technology and Intellectual Property 11 (2013), 239 (239 ff.); *Tufekci*, Colorado Technology Law Journal 13 (2015), 203 (203 ff.). With regard to the "autonomous driving" case, cf. *Gasser*, Fundamental and Special Legal Questions for Autonomous Vehicles, in: Maurer/Gerdes/Lenz et al. (ed.), Autonomous Driving: Technical, Legal and Social Aspects, 2015, p. 523 (534 ff.); with regard to the autocomplete function in *Google Search* see *Kastl*, GRUR 2015, 136 (136 ff.); *Müller-Hengstenberg/Kirn*, MMR 2014, 307 (307 ff.). With regard to employment law and discrimination arising from data-based recruitment wizards cf. *von Lewinksi/de Barros Fritz*, NZA 2018, 620 (620 ff.); regarding the sub-domain of robotics cf. *Beck*, JR 2009, 225 (225 ff.); *Spranger/Wegmann*, Öffentlich-rechtliche Dimensionen der Robotik, in: Beck (ed.), Jenseits von Mensch und Maschine, 2012, p. 105 (105 ff.).

[10] This does not mean a cumulative implementation of all conceivable regulatory instruments, but rather supports the idea of a toolbox of conceivable, feasible reform approaches, to the extent that these are appropriate based on a case-by-case basis.

Thus, the legislator is called upon to develop a regulatory approach for a consumer policy dedicated to delivering adequate protection to data subjects in individual cases without losing sight of economic opportunities provided by new technologies. Any additional regulation should thereby always anticipate and minimise the (bureaucratic) costs for small and medium-sized enterprises and non-profit associations. How possible regulatory frameworks can be combined into an overall concept and which actors should be addressed by these frameworks to ethically and legally limit the risks that algorithms and artificial intelligence pose to consumers' daily life is essentially a question of social and political understanding. This expert opinion sets out to enrich the ongoing debate by contributing to a variety of aspects from the perspective of EU and German Law.

B. Regulatory instruments

I. Transparency requirements

Users are disarmed due to the lack of insight into the arsenal of software applications: Whether an algorithm-based decision is correct, can only be verified by those who know and understand the data basis, sequence of actions and weighing of the decision criteria.[11] For this reason, the European Union's General Data Protection Regulation (GDPR) explicitly establishes the requirement of transparency as one of its central principles ("processed […] in a transparent manner in relation to the data subject", Art. 5 (1) lit. a GDPR).

Transparency is a necessary prerequisite for building trust in information technology systems and being able to make an informed decision. To establish confidence in algorithm-based processes and to prevent individuals from being left completely unaware of the content of their complex procedures, the GDPR imposes particularly extensive information and disclosure obligations on those responsible for data protection in Art. 12 ff. GDPR.[12] Overall, however, the requirements set out in the GDPR lag behind the standards a desirable legal policy includes.

[11] *Martini*, JZ 2017, 1017 (1018).
[12] For an overview over the system of data subjects' rights, see *Franck*, RDV 2016, 111 (111 ff.).

1. Ex-ante obligations to mark and inform

a) Status quo under existing legislation

For (fully) automated decision-making procedures, Art. 13 (2) lit. f and Art. 14 (2) lit. g GDPR establish a special obligation for data controllers to provide information.[13] These provisions not only require data controllers to inform data subjects about "the existence of automated decision-making", i. e. to make the use of such procedures *clearly visible*.[14] Additionally, they require them to provide data subjects with meaningful information on the modalities of processing – at least in the cases of profiling.[15] This obligation extends to both, the *logic involved* and the *significance and envisaged consequences of fully automated processing* (cf. recital 60 p. 1–2 GDPR).

However, the GDPR reins in consumers' extensive expectations: The information and labelling obligations do not apply *unconditionally*. They consistently refer to Art. 22 GDPR. This substantially restricts the obligations' scope of applicability: They are only binding for data controllers to the extent that personal data is processed through *fully automated decision-making*.[16] Consequently, only decisions void of *any substantial (decisive) human intervention* are

[13] It is opposed by an identical right to information of the data subject with regard to content (Art. 15 (1) lit. h GDPR); see also *Martini*, Blackbox Algorithmus, 2019, p. 177 f. and p. 14 f. below.
[14] The law on high-frequency and algorithmic trading already provides for a similar labelling obligation to ensure greater information transparency in algorithm-based trading in financial instruments, simplify supervision and increase compliance, cf. sec. 16 (2) no. 3 Stock Exchange Act (*Börsengesetz/*BörsG*)* and sec. 72 (1) no. 10 Securities Trading Act (*Wertpapierhandelsgesetz/*WpHG*)*; more details in *Martini*, Blackbox Algorithmus, 2019, p. 151.
[15] The exact meaning of the clause "at least in those cases" is not clear (in detail see *Martini*, Blackbox Algorithmus, 2019, p. 182 ff.). From recital 63 p. 3 GDPR, it can be concluded that the EU legislator only wanted to include an absolute obligation to provide information on logic and scope in cases of processing "of the existence of profiling and the consequences of such profiling" (see also recital 60 p. 3 GDPR). However, a somewhat broader interpretation can also be considered, according to which the duty to provide information applies not only in the case of profiling, but in *all* (fully) automated procedures. The wording of the provisions leaves room for both interpretative approaches.
[16] *Martini*, JZ 2017, 1017 (1020).

subject to extended information obligations[17] – the provisions do not apply to human decisions supported by algorithms.[18] The GDPR therefore lacks an effective regulatory regime for scenarios in which software applications *merely prepare or support* human decision-making.[19]

b) Recommendation for future legislation

In the future, the legal system should extend its catalogue of information obligations: labelling obligations and the obligation to inform data subjects about logic and scope of algorithm-based processes should apply in principle[20] to *all software applications processing data sensitive to fundamental rights*[21] –, in the granting of loans on the basis of a score value or in profiling procedures, for example, when a social network assigns users to different categories based on an assessment of their personality.[22] This in particular applies to situations in which individuals are subjected to computerised evaluations against their will – for example where the government uses scoring software to decide on vocational support measures for unemployed persons.[23]

In order for the (obligatory) labels to create an actual impact, consumers need to be able to easily comprehend their meaning. Hence, labels have to be more than annoying or unhelpful notices in a privacy statement, which consumers would easily disregard. It is therefore advisable to demand *visually easily comprehensible icons* as obligatory labelling elements.[24] Although the GDPR allows for standardised picture symbols (Art. 12 (7) s. 1 GDPR), it leaves the

[17] Purely formal human decisions that do not affect substantive decisions, i.e. mere "signing off", invoke Art. 22 (1) GDPR, cf. *Martini*, in: Paal/Pauly (ed.), DS-GVO/BDSG, 2nd ed., 2018, Art. 22 GDPR, marginal no. 17.
[18] *Martini*, in: Paal/Pauly (ed.), DS-GVO/BDSG, 2nd ed., 2018, Art. 22 GDPR, marginal no. 16 ff.; *Martini*, JZ 2017, 1017 (1020).
[19] The situation is different with regard to the regulation of algorithm-based trading of financial instruments. Here, the legislator subjects the financial services companies to the algorithm-specific obligations even if their algorithm-specific software trading systems merely determine that a person should continue to process the order to a limited extent, Art. 4 (1) no. 39 Directive 2014/65/EU of 15 May 2014, OJ No. L 173 of 12 June 2014, p. 349 in conjunction with Art. 18 Delegate Regulation (EU) No. 2017/565 of 25 April 2016, OJ No. L 87, 31 March 2017, p. 1.
[20] See also *Martini*, JZ 2017, 1017 (1020); *Busch*, Algorithmic Accountability, 2018, p. 58 ff. and *Schweighofer/Sorge et al.,* Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, October 2018, p. 161. *Tene/Polonetsky, Northwestern* Journal of Technology and Intellectual Property 11 (2013), 239 (271), see the marking obligation as a duty of "fairness and justice".
[21] See p. 44 ff. below for a suggestion on how to specify fundamental rights sensitivities in individual cases.
[22] On content requirements to the permissibility of profiling see p. 19 below.
[23] A similar approach is planned in Austria: *Fanta*, Österreichs Jobcenter richten künftig mit Hilfe von Software über Arbeitslose, netzpolitik.org 13/10/2018.
[24] *Martini*, JZ 2017, 1017 (1020); assenting *Busch*, Algorithmic Accountability, 2018, p. 59; for critical comments regarding the substantive design of labelling obligations cf. *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, October 2018, p. 162.

decision to make use of such to the responsible person's discretion. In the future, it would also be conceivable to categorise different algorithm-based systems in a traffic light system based on different levels of fundamental rights sensitivities, with results (such as "highly sensitive") being displayed to consumers in an easily comprehensible manner – similar to the energy efficiency classification or the hygiene "traffic light" for catering establishments. Art. 13 (2) or Art. 14 (2) GDPR could then be subjected to reform in line with the following guiding principle:

(2) In addition to the information referred to in paragraph 1, the data controller shall provide the data subject with the following information necessary to ensure fair and transparent processing with respect to the data subject: […]

g) [respectively h)] in the case of software applications sensitive to fundamental rights[25]: an indication that an algorithm-based evaluation is being carried out, as well as meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject..

2. Ex-post information

a) Obligation to state reasons

Users typically cannot comprehend software applications' decision results based solely on an *ex ante* knowledge of abstract decision parameters. They will acquire a better understanding of algorithm-based decisions relevant to them when provided with information on the reasons why the system decided in a specific manner in their individual situation – especially when a specific request (e. g. a loan) is rejected. In order to meet this objective, the legislator could oblige the data controller to explain the specific decision results to those affected. In contrast to an information obligation within the meaning of Art. 13 (2) lit. f or Art. 14 (2) lit. g GDPR which, in principle, applies *prior to processing*, the data controller would then not only have to describe the functioning of the algorithm-based process *in general*. Rather, he would have to make the specific result comprehensible, *after* the decision has been taken.

[25] This constituent element of "sensitivity to fundamental rights" would then certainly require a (legal) definition and specification by means of delegated legislation (see p. 44 ff. below).

aa) Legal status quo

As of now, the GDPR does not include a general requirement to provide case-by-case justifications for algorithm-based processes; such an obligation neither directly arises from Art. 22 (3) GDPR (as part of the obligation to take protective measures for fully automated decisions) nor can it be derived from recital 71 subpara. 1 s. 4 GDPR[26], nor is it set forth as an element of the information and access obligations in Art. 12 ff. GDPR.[27]

bb) Recommendation for future legislation

Not only when software applications make their own fully automated decisions, but also when algorithms are integrated into a (human) decision-making process – for example as an assistance system – an obligation to state reasons can provide helpful transparency incentives.[28] A justification would give data subjects adequate and appropriate insight into the software's black box as is necessary and appropriate in order to better understand the basis of the decision and to be able to challenge it if needed.[29]

cc) Limitations of obligatory justifications

It is not merely a profound technical challenge to obtain justifications from machine learning software. It would also initiate a paradigm shift: In legal transactions under private law, contracting parties (in contrast to the state, sec. 39 Administrative Procedure Act [*Verwaltungsverfahrensgesetz*/VwVfG]) are generally not forced to disclose the considerations leading them to act – also in case of decisions which are based on a complex combination of motives.[30]

---

[26] The recital refers to a right "an explanation of the decision reached after such assessment". However, this topos is not recalled in the enacting terms of this regulation (which alone consitute legally binding obligations). There is a deeper reason for this: The GDPR does not generally require the data controllers to provide explanations, but only, if the data subject has made use of its right to state its own position. The phrase "reached after such an assessment" indicates this, referring grammatically to the presentation of one's own position, thus relating to a small range of conceivable cases. If the controller has given data subjects the opportunity to object and obtain an explanation as to whether and how these have been taken into account, the EU legislator regards their interests as sufficiently taken into account. See also *Martini*, Blackbox Algorithmus, 2019, p. 191.

[27] For more details see *Martini*, Blackbox Algorithmus, 2019, p. 190 ff.

[28] Especially machine learning software often involves non-transparent decision-making processes because artificial neuronal networks – similar to the human brain – rely on highly complex interactions between large numbers of nodes (so-called *hidden layers*).

[29] Cf. also *Mittelstadt/Allo et al.*, Big Data & Society 2016, 1 (7); *Tutt*, Administrative Law Review 69 (2017), 83 (110) stating the need for mandatory justifications in relation to supervisory authorities.

[30] *Martini*, Blackbox Algorithmus, 2019, p. 192 f.

Even the German General Act on Equal Treatment (*Allgemeines Gleichbehandlungsgesetz*/AGG) does not require private law subjects to justify their decisions in contexts susceptible to discrimination.

Just as in the analogue world, private individuals should not be subject to a *general* justification obligation in the cyberspace. A duty to explain the reasons of private legal actions can only be legitimised by the *structural peculiarity of algorithm-based processes:*[31] In comparison to humans, they make other, sometimes surprising mistakes.[32] Algorithms operate on a quantitative basis of phenotypic similarities and stochastic conclusions: They recognize correlation, but not causation. An obligation to justify is appropriate where the risk of false conclusions due to fictitious causality unfolds (or other structural risks of algorithm-based procedures are realised) and fundamental rights trigger a special need for protection due to sensitive effects of an algorithm-based process.[33]

The requirement to justify algorithm-based decisions has to be limited when business secrets, in particular the source code of a decision-making system, are threatened to be disclosed[34] or when interests of third parties relevant to fundamental rights override the interest in a justification (for example, if a justification discloses information on indirectly concerned persons, e.g. personal data of a reference group).[35]

b) Right of access to underlying data and the decision basis

aa) Status quo under existing legislation

Data subjects have a right to access underlying data (free of charge): In addition to information on the processing (Art. 15 (1) GDPR), the data controller must also provide data subjects with

[31] *Martini*, Blackbox Algorithmus, 2019, p. 195 ff.; *Hoeren/Niehoff*, RW 9 (2018), 47 (57 ff.).
[32] An overview of error sources in algorithmic decision-making processes gives *Zweig*, Wo Maschinen irren können, February 2018, p. 21 ff.
[33] This is especially, but not only, true if the decision touches subject matter which is personality sensitive. For further detail see p. 44 ff. below.
[34] The situation is different if there are sufficient safeguards for the protection of secrets – such as an official review while maintaining secrecy. Cf. *Whittaker/Crowford et al.*, AI Now Report 2018, December 2018, p. 22, further demand that companies should refrain from protecting their trade secrets using algorithm-based systems in order to enable effective external control. On the *status quo* under copyright law, patent law and secrecy protection law, cf. *Martini*, Blackbox Algorithmus, 2019, p. 33 ff.
[35] *Martini*, Blackbox Algorithmus, 2019, p. 197; assenting *Busch*, Algorithmic Accountability, 2018, p. 60.

a copy of their personal data subject to the processing (Art. 15 (3) GDPR).[36] This allows data subjects to verify that all data used in the decision are correct, complete and up-to-date.[37]

However, the GDPR does not readily grant insight into the classifications made by profiling instruments about a person ("resilient", "conservative", "with a probability of 70 % homosexual") on a case-by-case basis. The right of access extends, in principle, only to the data relied on during the processing and not its full result.[38] According to the will of the EU legislator, Art. 15 (1) GDPR is limited, by "the rights or freedoms of others, including trade secrets or intellectual property" and by freedom of expression and the freedom to choose and obtain an occupation (recital 63 s. 5 GDPR).

Also, Art. 16 s. 1 GDPR does not grant data subjects a right to gain insight into a profile assessment or to demand its correction.[39] The right in Art. 16 s. 1 GDPR is in essence directed at the underlying database, which is subjected to a check based on intersubjectively verifiable criteria ("accurate personal data"). This provision in the GDPR does not silently establish any right to demand of others to disclose the opinion formed about others as a result of a process.[40]

bb) Right to appropriate algorithmic conclusions as a recommendation for future legislation?

A in-depth regulatory approach aimed at improving the transparency of algorithmic patterns can (other than provided in Art. 15 and 16 GDPR) extend beyond the decision basis of the

[36] On the basis of Art. 15 (3) GDPR, the Higher Labour Court of Baden-Württemberg (*Landesarbeitsgericht /LAG Baden-Württemberg*) recently obliged an employer to provide an employee with a copy of all "performance and behaviour data" relating to him (judgment of 20/12/2018, ref. 17 Sa 11/18, marginal no. 203 ff.).
[37] Cf. also *sub specie* fully automated decisions within the meaning of Art. 22 GDPR: recital 71 subpara. (2) s. 1 GDPR, which requires controllers to "implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected"; for the more stringent French regulations cf. *Martini,* Blackbox Algorithmus, 2019, p. 186.
[38] See in detail, *Martini*, Blackbox Algorithmus, 2019, p. 199 ff.
[39] On the other hand, the right to deletion pursuant to Art. 17 (1) GDPR may also include the results of a data processing (e. g. the results of profiling); cf. also *Kamann/Braun*, in: Ehmann/Selmayr (ed.), DS-GVO, 2nd ed., 2018, Art. 17, marginal no. 36. However, Art. 17 (1) GDPR is mostly only useful to the addressee of algorithm-based decisions in cases where the data controller has not yet made a decision and the data subject therefore has the opportunity to request the deletion of the data. If there is a reason for deletion (Art. 17 (1) lit. a to lit. f GDPR), the data controller may then no longer base his decision on this data basis. Art. 17 (1) GDPR, on the other hand, does not stipulate a right to inspect algorithm-based profile results or to demand that the responsible person subsequently corrects an algorithm-based decision made on the basis of personal data.
[40] Nor does anything else apply to the right of objection under Art. 21 (1) s. 1 GDPR. It does not provide the data subject with the possibility to influence the content of the result of the data processing, but rather concerns *whether* data processing is carried out on the basis of Art. 6 GDPR.

process: The legal system should consider not only the *processing of personal data*, but especially the *consequences* resulting from the processing of particular data.[41] This is particularly indicated where software applications that predict user preferences may have a damaging effect on a data subject's reputation without being subject to scrutiny.[42] The legal protection is then no longer directed solely at the data input. Instead the normative scope would extend also to the data output, i.e. the processing results, in particular algorithmic conclusions (so-called inferences) and reference data sets.[43] If, for example, an algorithm inferences low customer satisfaction from the fact that a user moves the cursor slowly, this hypothesis may be open to factual challenge (as the user may simply be tired, or his hardware may be slow), and it may, in a worst-case scenario, even infringe on individual rights. It is therefore conceivable that the GDPR should give individuals the ability to take control of algorithmic classifications relating to them: This would enable them to challenge controllers in cases of unverifiable or highly error-prone inferences.

For data subjects to exercise such a right effectively, providers will not only need to explain why data are necessary for a particular conclusion and why the conclusion in turn is relevant for the decision-making process, but also whether the data collection and conclusion methods are reliable.[44] In legal terms, the legislator could construe this requirement by expanding the scope of existing substantive *information obligations* applicable to providers of algorithmic applications.[45]

However, such a subjective right of access to profiling tools is, just like any right to obtain certain decision results, ultimately prone to overreach. Established in the legal system is the right to individual self-portrayal as part of the individual's general right to privacy[46], however

[41] *Tene/Polonetsky*, Northwestern Journal of Technology and Intellectual Property 11 (2013), 239 (270 f.); *Wachter/Mittelstadt*, Columbia Business Law Review 2019, 1 (1 ff.) of the type script.
[42] *Wachter/Mittelstadt*, Columbia Business Law Review 2019, 1 (3) of the type script.
[43] With regard to the problem of statistical inferences and reference datasets cf. *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, October 2018, p. 35; about this and the following see also *Martini*, Blackbox Algorithmus, 2019, p. 205 f.
[44] *Wachter/Mittelstadt*, Columbia Business Law Review 2019, 1 (57 f.) of the type script; similarly, with regard to the introduction of positive lists of objectively justified attributes relevant to the decision-making process, see *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, October 2018, p. 91.
[45] *Wachter/Mittelstadt*, Columbia Business Law Review 2019, 1 (57 f.) of the type script; they also support the regulatory substance of sec. 28 of the German Federal Data Protection Act (*Bundesdatenschutzgesetz*/BDSG), old version, but additionally propose an obligation to provide information; *ibid*, p. 60 f.
[46] This includes in particular the right to one's own image, one's own word and one's own name as well as the right of reply; cf. e. g. *Martini*, JA 2009, 839 (841).

not a right to be regarded in a particular way by third parties. Neither in the analogue nor in the digital world such a right is generally necessary for an effective protection of an individual's personality – even if the risk to privacy is elevated in times of in-depth Big Data analysis. Much more relevant is that the assumptions fed into algorithm-based processes are valid. The supervision regarding this point is best placed in the hands of a supervisory authority – and not of each data subject: Only a supervisory body usually possesses the crucial expertise to assess reliably and more extensively than a case-by-case approach which data must not be used and under which circumstances specific conclusions are permissible and justified. An individually enforceable right to appropriate conclusions collides in particular with the software user's legitimate privacy interests and fundamental autonomy to make decisions freely (as an expression of their economic freedom), without being essential for effective protection of privacy. It is only of limited use if private persons affected try to enter into a discussion with a provider about whether the classifications the provider has made are in line with their own assessment. Valuations cannot be verified on an intersubjective level and are therefore, in principle, not legally enforceable.[47] The crucial point is, rather, that the assumptions on which the evaluations are based are valid and subject to a supervised accuracy check. More expedient than a right to know what someone or a computer "thinks" about another person, and more effective than to include a right to proper conclusions as a legal measure is on a closer examination therefore another measure: The law should objectively and legally ensure the legality of the processing model and its basic assumptions by means of appropriate normative guidelines and state supervision.

3. Expansion and publication of the data protection impact assessment

Data protection law is under suspicion to follow an oversimplified black-and-white pattern as it employs a general prohibition with an option of retroactive permission, thus placing all processing operations under the presumption of being dangerous.[48] The approach of *risk-adjusted regulation* is the right attempt at aligning the regulatory regime with the actual risks

[47] The legal system does not grant the individual any legally enforceable right to revocation of reputation-damaging opinions by third parties. The individual can only demand that they refrain from taking such action in the future. See for example *Martini/Kühl*, Jura 2014, 1221 (1227).
[48] Cf. more detailed, for example, *Martini*, Blackbox Algorithmus, 2019, p. 159 ff.

posed by processing operations and, thus, to deal with data protection conflicts in the digital age more adequately.[49]

As part of a risk-based regulatory approach, Art. 35 (1) GDPR requires data controllers to subject their own data processing operations to comprehensive testing. However, this impact assessment does not constitute an *encompassing* risk analysis. It merely addresses impacts on the *protection of personal data* (and thus primarily "traditional" data protection concerns).[50] Other objects of protection, such as assets, property or physical integrity, do not necessarily need to be included in a controller's scope of assessment ("assessment of the impact […] on the protection of personal data" – Art. 35 (1) s. 1 GDPR). They are merely of importance to the question *whether* an impact assessment should be conducted at all ("for the rights and freedoms of natural persons"), but not for the scope of the content of the audit ("assessment of the impact of the processing operations envisaged on the protection of personal data").[51]

As a result, the regulatory approach of the GDPR falls short. For data controllers using algorithms sensitive to or potentially endangering fundamental rights, it is appropriate to request a *thematically encompassing* impact assessment[52] before they deploy their software application.[53]

The law should link the requirement to conduct an impact assessment to the obligation to make the results of such an assessment available to the *public*.[54] In order to increase the efficiency of such a regulatory approach, a public register[55] could be established to collect and provide access to impact assessments of risk-prone algorithmic processes (within the limitations set by legitimate interests in protection of intellectual property). Comparable registers already exist, for example for public assessments and risk analyses that companies have to prepare as part of the process to approve pharmaceuticals.

---

[49] See also *Böhning*, ZD 2013, 421 (422); *Härting/Schneider*, CR 2015, 819 (822 ff.); *Veil*, ZD 2015, 347 (348 ff.).
[50] *Martini*, Blackbox Algorithmus, 2019, p. 209 f.
[51] See in detail *Martini*, Blackbox Algorithmus, 2019, p. 209 f.
[52] The legal system may entrust the provider of a software application to identify previously unidentified risks for all affected legal interests. Cf., for example, the corresponding regulations in the law of hazardous substances: Art. 5 ff. EU regulation No. 1272/2008.
[53] *Martini*, Blackbox Algorithmus, 2019, p. 209 f.; with a similar approach ("Algorithmic Impact Assessments") for US law: *Reisman/Schultz et al*., Algorithmic Impact Assessments, April 2018, p. 7 ff.
[54] In addition already *Martini*, JZ 2017, 1017 (1022); in detail *Martini*, Blackbox Algorithmus, 2019, p. 210 ff.
[55] *Kolain*, Data Protection Impact Assessment (Art. 35 GDPR) as a Tool of Privacy Regulation, 2018, p. 22.

II. Content control

To ensure that the use of algorithm-based systems is in line with legal provisions, it is essential to implement regulations responding to the operational risks. Thus, not only viable standards have to be devised and implemented into law (1.), but also powerful institutions need to be established which ensure compliance with said regulations in practice (2.).

1. Regulation mechanisms

a) Approval procedure in sensitive areas of application

In order to effectively protect data subjects using particularly high-risk applications, a state-imposed *ex ante* permit system is a conceivable solution.[56] Software applications must then undergo a specific approval procedure prior to their deployment.

At the same time, a permit regime burdens companies with bureaucratic expenses and may slow down economic growth. Typically, permit requirements overreach in the sector of algorithm-based processes. Preventive admission procedures may be appropriate for specific algorithm-based procedures – for instance for applications which can seriously impair fundamental rights,[57] in particular health (e.g. care robots)[58] or software which the administration uses to assess and allocate benefits (e.g. university admissions, granting social benefits and subsidies). Preventive admission procedures can also be appropriate for applications used by private individuals who potentially have a significant impact on areas of systemic importance for a liberal democracy (such as elections or the creation of public opinion).[59]

[56] In this context and with regard to the substantive aspects of relevant control procedures cf. *Martini*, JZ 2017, 1017 (1021); cf. assenting *Busch*, Algorithmic Accountability, 2018, p. 59 ff.
[57] Private individuals, software operators are not directly bound by fundamental rights. However, fundamental rights indirectly influence private legal relationships, especially where opportunities for personal development are at stake. The regime of the GDPR also unspokenly builds in many parts on the idea of an indirect binding effect of the fundamental right to privacy.
[58] Some software applications are already subject to such approval requirements due to sector-specific regulations, for example the Medical Products Law.
[59] With regard to potential regulatory thresholds, see p. 40 ff. below.

b) Specifying regulations for the legitimacy of profiling, in particular the requirement of mathematical-statistical validity of algorithm-based decisions

Art. 22 (1) GDPR sets forth an important element for a preventive regulation of algorithms. It grants data subjects a legal defense against automated decisions.

The scope of the provision, however, is relatively cryptic. On the one hand, only decisions "solely" based on automated processing are covered. On the other hand, it is sufficient that the decision is "based on" automated processing. This insinuates that intermediate steps, e.g. human interventions, can lie between the automated processing and its result. Art. 22 (1) GDPR does in fact not preclude this. But the wording “based solely on automated processing” does not allow for significant intermediate steps between the automated processing and its results, i.e. any human intervention within this interpretation has to be a strictly formalistic confirmation of a computer-based decision, void of any substantial examination.[60]

As a result, Art. 22 (1) GDPR is limited in scope: Only decisions made without decisive human involvement are subject to the provision (such as fully automated tax assessments, cf. sec. 155 (4) tax code [*Abgabenordnung*/AO]).[61] Art. 22 GDPR thus – for the majority of algorithmic decision-making processes – does not provide a comprehensive solution to the regulatory challenge.

With regard to consumer protection, it is *prima facie* tempting to *extend*[62] the scope of Art. 22 (1) GDPR *to semi-automated decisions*, or more specifically to "decision[s] based predominantly or solely on automated processing, including profiling".[63] However, extending the

[60] In the field of algorithm-based trading of financial instruments, the legislator subjects the financial services companies to algorithm-specific obligations as early as when their algorithm-specific software trading systems merely determine that a person is to process the order in a restricted way, Art. 4 (1) no. 39 Directive 2014/65/EU of 15 May 2014, OJ No. L 173 of 12 June 2014, p. 349 in conjunction with Art. 18 Delegate Regulation (EU) No. 2017/565 of 25 April 2016, OJ No. L 87, 31 March 2017, p. 1.

[61] *Buchner*, in: Kühling/Buchner (ed.), DS-GVO/BDSG, 2nd ed., 2018, Art. 22, marginal no. 15 f.; *Hoeren/Niehoff*, RW 9 (2018), 47 (63).

[62] However, the legislator would do well to specify the ambiguous scope of the standard by sublegally specifying it, in particular, by specifying more clearly where the limits for exclusively automated decisions ("decisions based solely on automated processing") lie.

[63] Automated decisions in manufacturing processes of industry, robotics etc. would not be affected by this, as far as data processing has no personal reference and the GDPR therefore does not apply; Art. 2 (1) GDPR , Art. 2 (2) order (EU) 2018/1807; cf. also *Reisman/Schultz et al.*, Algorithmic Impact Assessments, April 2018, p. 13.

black-and-white scheme of prohibition employed in Art. 22 (1) GDPR does not adequately fulfill the challenges posed by the digital world; a general prohibition of profiling overreaches.[64] It is rather necessary to specify quality-related standards for profiling to sensitively confine the prohibition. Such standards include in particular protection mechanisms that reduce errors and risks in algorithm-based profiling. Thus, an algorithm-based decision is only correct if the information on which the subsequent decision is based is relevant in a mathematical-statistical sense.[65] The legal system should provide[66] data controllers with qualitative normative guidelines regulating which data, underlying assumptions and mathematical methods and evaluation mechanisms may be used for a decision.[67]

Consumers must be able to rely on the algorithmic systems to operate on the basis of robust assumptions and models (see also recital 71 subpara. 2 GDPR[68]).[69] In this respect, sec. 31 (1) no. 2 German Federal Data Protection Act (*Bundesdatenschutzgesetz*/BDSG) is a model for a provision with respect to scoring.[70] In addition, the law should formulate requirements for valid mathematical-statistical procedures also for the – much broader – field of algorithm-based profiling evaluation instruments (e. g. social networks).[71]

What constitutes a valid mathematical-statistical procedure on an individual basis needs to be specified further. In the German Federal Data Protection Act, the legislator has left this question unanswered. The law should provide specific guidelines on methodological requirements for individual algorithm-based procedures – be it in form of a parliamentary act (which – under

[64] This does not mean that the need for protection of the persons concerned cannot justify the prohibition of profiling analyses in specific subject areas under specific circumstances. Art. 6 (2a) subpara. 2 of the draft E-Privacy regulation of 19 October 2018, for example, intends that the provider of electronic communications networks or services may not use the metadata of communications (e. g. whereabouts of the sender of an electronic message) for profiling analyses. However, this absolute limit to profiling does not apply if the processing of metadata is carried out with the consent of the user or on the basis of a law which serves to secure a public objective within the meaning of Art. 23 (1) lit. c to lit. e, lit. i or lit. j GDPR , see Art. 11 (1) of the draft E-Privacy Regulation of 19 October 2018.

[65] *Martini*, Blackbox Algorithmus, 2019, p. 257.

[66] Similarly, *Wachter/Mittelstadt*, Columbia Business Law Review 2019, 1 (61) of the type script.

[67] *Martini,* Blackbox Algorithmus, 2019, p. 257 ff. The opposite question also arises, namely whether statistically relevant data must be included in the decision-making process under certain circumstances, see *Domurath/Neubeck,* Verbraucher-Scoring aus Sicht des Datenschutzrechts, October 2018, p. 23.

[68] Recitals are not binding, but an aid of interpretation of the legal act under Union law.

[69] In addition to the fact that the legal system should shape the control objectively and not subjectively, and especially should not implement the right to an appropriate conclusion, p. 14 ff. above.

[70] Sec. 31 (1) no. 2 Federal Data Protection Act (*Bundesdatenschutzgesetz*/BDSG) is incompatible with the primacy of application of the GDPR. See e. g. *Martini*, in: Paal/Pauly (ed.), DS-GVO/BDSG, 2nd ed., 2018, Art. 22 GDPR, marginal no. 44.

[71] *Martini*, Blackbox Algorithmus, 2019, p. 257.

German constitutional law – is necessary if it substantively touches fundamental rights – cf. *Wesentlichkeitslehre*) or in form of a regulation on the administrative level.[72] In addition, the legislator should create more precise guidelines to define which models of profile allocation ("conservative", "homosexual", "unreliable", etc.) data controllers may no longer use because they have been proven to be insufficiently substantiated, offensive or for any other reason violating the rights of the data subject. These requirements should also specify qualitative operational aspects of the relationship between the underlying data and the result of the algorithmic data processing.[73] They should outline minimum requirements which assumptions and mathematical calculation methods (such as the weighing of individual calculation factors) on which the algorithmic calculation is based must meet. Those who use processing models making personality-sensitive decisions must then be able to ensure and (in the case of judicial proceedings) prove the existence of a statistically valid relationship between the underlying data and the expected evaluation result: Only those criteria, proven to be relevant and legitimate for the decision, may be included in the decision model.[74]

To balance the competing fundamental rights of the controller and the data subject, the requirements for the validity of the mathematical models and the relevance of the underlying data should correspond to the scope of the decision and the potential damage of an algorithm-based procedure.[75]

c) Anti-discrimination guardianship: Obligation to ensure lawful and, in particular, non-discriminatory decision results

Those who employ machine learning software in areas sensitive to fundamental rights should be obligated to carry out routine audits of their systems. It is particularly advisable – similar to the regulatory scheme in environmental law regarding immissions – to impose *dynamic obligations* on the controller making him responsible for the decision results and the correct

[72] In detail on delegated legislation below p. 53 ff.
[73] On the following *Martini*, Blackbox Algorithmus, 2019, p. 257 ff.
[74] *Martini*, Blackbox Algorithmus, 2019, p. 257 ff.
[75] Its capacity to identify uncertainties and differentiate degrees of uncertainty determining a decision, is, in particular, signifying a good quality of the model; *Martini*, Blackbox Algorithmus, 2019, p. 259.

processing of the system:[76] Operators should be obliged not only to test[77] and analyse a software's decision results before it is deployed, but also to subsequently audit the software's compliance with the principles set forth by the law.[78]

Such operator obligations should be coordinated with effective external supervision to ensure that the systems in fact comply with the legal requirements.

aa) Operator obligations under discrimination law

One of the central risks arising from algorithm-based processes are discriminatory results. Machine learning software applications reflect the prejudices and social imbalances engraved in their code and training data. Thus, they reproduce prejudices and unequal treatment found in social reality. Socially or legally unwanted unequal treatment can hereby go unnoticed and be incorporated into the results. If, for example, a company defines the category "outstanding" in the performance assessment of its employees by the number of working hours, it will generally discriminate indirectly against women: Women work part-time significantly more often than men in order to take care of family responsibilities. If an algorithm uses machine learning in order to identify students with high performance potential for a scholarship program, it may also take into account linguistic peculiarities of their social milieu or their home address because previous students with similar factors were, on average, less successful.[79]

In an algorithm-based environment capable of screening the individual according to various categories on the basis of in-depth analysis tools, the data subject is, in case of doubt, more and more frequently exposed to grids and differentiations that are not due to his personal characteristics but to certain group characteristics that he fulfills.

(1) Extension of the General Equal Treatment Act (AGG)

In Germany, the General Equal Treatment Act (*Allgemeines Gleichbehandlungsgesetz*/AGG) ensures the protection of those at risk of discrimination from unjustified unequal treatment.

[76] In detail *Martini*, Blackbox Algorithmus, 2019, p. 256 ff.
[77] In detail *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, October 2018, p. 146. *Schmid*, CR 2019, 141 ff. derives a control obligation of the operator for "integrated product monitoring" for automated and networked systems from the insurance obligations of tort law.
[78] To include social and economic consequences as well (beyond antitrust or other competition law limits) would quickly overburden the examination programme.
[79] *Whittaker/Crawford et al.*, AI Now Report 2018, December 2018, p. 21 f.

To date, the AGG – as well as it's European "parent" guidelines – is fragmentary: Neither are all conceivable forms of discrimination covered (e. g. different financial capabilities are not included) nor all areas of life where discrimination may occur. It therefore does not cover all manifestations of algorithm-based decision-making systems capable of penetrating an individuals' legal sphere.[80] It focuses on the areas of work, education, social affairs and mass transactions.

In order to expand the legal framework of the AGG into an anti-discrimination law for algorithm-based procedures encompassing all areas of life, the legislator could add a new no. 9 to sec. 2 AGG (or alternatively the provision sec. 19 (1) AGG), extending the scope of application of the AGG to all unequal treatment "*based on an algorithm-based data evaluation or an automated decision process*".

However, a large number of legally abusive compensation proceedings have been based on the AGG (so-called "AGG hoppers").[81] Hence any political efforts to extend the AGG's scope of application must be cautiously evaluated. As part of a cautious regulatory approach, it may therefore alternatively be advisable not to extend the scope of the AGG generally to algorithm-based processes (possibly with extensive counter-exceptions), but rather to add few specific areas which are particularly sensitive to fundamental rights and potentially impact a person´s life planning (e.g. "consumer contracts entered into on the basis of a scoring") or integrate clearly defined high-risk processes relating to present AGG areas of protection (such as facial recognition methods).[82]

(2) Technical measures of protection against indirect discrimination

Regulation responding to algorithmic potential for discrimination is challenged by having to address indirect discrimination caused by discriminatory training data.[83] To fight indirect discrimination, the legislator should focus on the "selection and design of training data". Operators of learning systems should be obliged to take protective technical measures to counteract

[80] In detail *Martini,* Blackbox Algorithmus, 2019, p. 231 ff.
[81] In detail *Martini,* Blackbox Algorithmus, 2019, p. 237 f. A classification summary of this topic can be found at *Bauer/Krieger*, NZA 2016, 1041 (1041 f.) with further notes. On the criminal law assessment of the "AGG-Hopping" cf. *Brand/Rahimi-Azar*, NJW 2015, 2993 (2993 ff.).
[82] In detail *Martini*, Blackbox Algorithmus, 2019, p. 236 ff., 337 ff.
[83] In detail *Martini,* Blackbox Algorithmus, 2019, p. 239 ff.

discrimination through an appropriate configuration and control of their sets of training data. In particular, it is conceivable to use standardised data sets and test methods or to restrict certain data to be used only in specific contexts.[84]

bb) Quality requirements for procedural justice

In order to counter the risk of unlawful decision results, qualitative requirements for decision algorithms are useful. The legislator should oblige operators to provide a minimum of technical and mathematical guarantees of procedural quality which safeguard the legality of the algorithm-based results using a specific procedure. The operators have to ensure that the software reaches its decisions in a lawful procedure. This can particularly include security mechanisms guaranteeing the quality of the processed data, the decision model and the configuration.

cc) Obligation to implement a risk management system and name a responsible person

Anyone implementing (learning) algorithms in software applications sensitive to fundamental rights[85] should not only have to provide a risk prognosis, as prescribed by Art. 35 (1) s. 1 GDPR. Instead, he should generally be obliged to implement a *risk management* system in data processing.[86] The GDPR does not yet require data controllers to implement such systems. Herein lies a regulatory gap. The EU legislator could, for example, extend the data controller's general obligations in Art. 25 (1) GDPR to introduce and operate an effective risk management system if and when software sensitive to fundamental rights is used.[87]

A risk management system complements the already existing data protection impact assessment: it requires the data controllers to assess the extent to which risks have materialised and to react to them when necessary. In case of error indications in the running software, the risk management system can trigger a (human) review of the algorithm-based decision. Thus, it

[84] In detail *Martini,* Blackbox Algorithmus, 2019, p. 239 ff.
[85] For a more detailed description of the regulatory thresholds see p. 44 ff. below.
[86] In addition already *Martini*, JZ 2017, 1017 (1022). Specific obligations (regarding organisation) already exist in the area of algorithmic trading with financial instruments, sec. 80 (2-5) Securities Trading Act (*Wertpapierhandelsgesetz*/WpHG) in conjunction with the delegated regulation (EU) 2017/589: in detail *Martini*, Blackbox Algorithmus, 2019, p. 148 ff.
[87] See p. 37 below for a more detailed definition of who belongs to this group. Below a critical sensitivity threshold, the legislator could transfer the responsibility for appointing a risk manager to the operator, thus granting a preferential treatment in terms of supervision if the risk manager is able to demonstrate the controller's compliance.

can help to prevent unforeseen, and in particular discriminatory, decisions in algorithm-based processes.

For the risk management system, operators (above a certain size and sensitivity threshold) should have to appoint a *responsible person*. She should not only be able to assess the risks of systems based on specific knowledge of statistics, mathematics and computer science; the person should also be liable. Comparable to actuaries (sec. 141 (5) of the German Insurance Supervision Act [*Versicherungsaufsichtsgesetz*/VAG], risk managers are responsible for identifying errors impacting decisions of algorithm-based systems, for communicating identified errors within the company and working towards solutions. Furthermore, general *obligations to report or inform* are appropriate for especially sensitive algorithm-based processes; they would have to inform the public about its risk development.

Comparably in data protection law, Art. 34 (1) GDPR stipulates that in the event of a "*personal data breach*" (e. g. in case of a data leak) the data controller must communicate the breach to the data subjects when it "*is likely to result in a high risk to the rights and freedoms*" of the data subjects. An obligation to inform below this infringement threshold, in particular on risks that have arisen or have been averted, can strengthen risk awareness and consumer confidence and, in the ideal case, incentivise suppliers to use suitable risk reduction strategies.

d) Supervision by the authorities during operation of algorithm-based systems

As individuals have very limited insight into the lawfulness of algorithm-based processes and the systems' decision patterns change dynamically, supervision by public authorities is of utmost importance. A sovereign supervisory procedure puts software systems under scrutiny to determine that the conditions for lawful use are continuously met.[88] In addition to audit algorithms, rights of access and inspection (bb) can be important components of this supervision.

aa) Control of decision results, specifically through audit algorithms

Audit algorithms systematically search for anomalies and in particular for discriminatory tendencies in software applications' decision results.[89] They determine which factors are

[88] *Martini,* Blackbox Algorithmus, 2019, p. 249 f.
[89] In addition already *Martini*, JZ 2017, 1017 (1022); assenting *Busch*, Algorithmic Accountability, 2018, p. 66.

weighted particularly strongly by the implemented algorithm and whether the alleged correlation between fact and result corresponds to the algorithm's actual decision behaviour.[90]

Supervision by authorities should not be limited to the use of audit algorithms. An effective external inspection as to whether the service meets the legal requirements can only be regularly conducted if authorities are granted access not only to the source code but also to the *learning mechanisms*, the *underlying data* and the *processing results*.[91]

bb) Authorities' rights of access and inspection, in particular access rights/interfaces for tests and external controls

In order for supervisory authorities to be able to check whether software applications comply with legal requirements, the legislator should grant them rights of access and inspection corresponding to the operators' legal obligations.[92] Art. 58 (1) GDPR could serve as a baseline and blueprint: It defines a (comprehensive) catalogue of investigative powers ("to provide any information", "to carry out investigations", "to obtain […] access to all personal data and to all information") and thereby enables data protection supervisory authorities to extensively investigate and uncover facts relevant to legal and factual data protection.[93]

Another normative model is provided in sec. 32e (5), (6) German Act against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen*/GWB). The provision authorises the *German Federal Cartel Office* to conduct sector enquiries under consumer law.[94] Analogous provisions exist in the area of algorithmic trading with financial instruments (sec. 6 (4) Securities Trading Act [*Wertpapierhandelsgesetz*/WpHG], sec. 3 (4) no. 5 Stock Exchange Act [*Börsengesetz*/BörsG] in conjunction with sec. 7 (3) s. 1 BörsG).[95]

[90] *Martini,* Blackbox Algorithmus, 2019, p. 250 f.
[91] *Martini*, JZ 2017, 1017 (1022).
[92] In addition already *Martini*, Blackbox Algorithmus, 2019, p. 262; also similarly *Whittaker/Crawford et al*., AI Now Report 2018, December 2018, p. 22.
[93] Regarding the regulatory content cf. *Selmayr*, in: Ehmann/Selmayr (ed.), DS-GVO, 2nd ed., 2018, Art. 58, marginal no. 11 ff.; *Boehm*, in: Kühling/Buchner (ed.), DS-GVO/BDSG, 2nd ed., 2018, Art. 58, marginal no. 13 ff.
[94] *Busch*, Algorithmic Accountability, 2018, p. 66 f.
[95] These provisions implement the requirements of Art. 17 of Directive 2014/65/EU into German national law; in detail *Martini*, Blackbox Algorithmus, 2019, p. 153 f.

The affected service providers' legitimate confidentiality interests[96] can be adequately protected by employing instruments designed to protect confidentiality, such as the in-camera procedure (cf. sec. 99 (1) s. 2 of the Administrative Procedure Code [*Verwaltungsgerichtsordnung*/VwGO]; cf. also sec. 30 VwVfG).[97]

(1) Interface for tests and external controls

Algorithm-based systems are only accessible to external auditors if the operators of the respective system provide real-time technical access to the system while it is operating. An effective audit of algorithm-based systems therefore depends on the technical capability to test and examine the system while in use in its most up-to-date version.[98] This requires an interface provided by the operator enabling external access at any time.[99] The right to access such interfaces should be granted to authorities by law. Likewise, operators should be obliged to use adequate and interoperable IT solutions when implementing interfaces to enable official introspection. Supervision by public authorities is particularly important regarding scoring-software used in credit allocation, particularly by credit agencies. If, for example, the suspicion arises that a particular scoring system systematically puts women at a disadvantage, it will be very difficult for a single customer to confirm and substantiate this suspicion from the outside. Even the large-scale data collection initiative #OpenSCHUFA had to be terminated due to its inability to supply sufficient and diverse data.[100]

It is also conceivable to grant interface access to other institutions committed to protecting data subjects' rights – for instance to organisations entitled to file reprensentative action or organisations serving dispute settlement in arbitration bodies.[101] However, if private third par-

[96] On issues of patent law, copyright and fundamental rights relating to the protection of trade secrets, cf. *Martini*, Blackbox Algorithmus, 2019, p. 33 ff.
[97] *Martini*, Blackbox Algorithmus, 2019, p. 253 ff.
[98] For an instructive approach from a technical point of view, see *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, October 2018, p. 44 ff.
[99] It would also be conceivable to have automated real-time monitoring by the supervisory authorities in particularly sensitive areas. Since 15 November 2018, for example, a consolidated monitoring system called CAT (Consolidated Audit Trails) has been monitoring the US capital markets, see in detail *Martini*, Blackbox Algorithmus, 2019, p. 155.
[100] Cf. intermediate report on the initiative, available at https://algorithmwatch.org/de/zwischenbilanz-der-openschufa-datenspende/; cf. also *Busch*, Algorithmic Accountability, 2018, p. 69.
[101] See p. 37 below for potential association rights of action and arbitration.

ties gain access to the systems, this creates lasting risks for operators' professional and personal freedom, in particular with regard to their trade secrets: In-depth system testing via an interface can be equated to, figuratively speaking, selling the company's "family silver" and thus disproportionately infringe operators' rights. In extreme cases, tests may also impair systems, in particular compromising the systems' stability and performance.[102] Furthermore, it is by no means always clear whether an individual test result actually reveals a system error or rather a phantom and whether tests therefore can be considered evidence.[103] To date, no common regulatory and technical framework for testing has been developed: Both, the quality of tests as well as adequate test procedures, need to be safeguarded by law.[104]

In view of the numerous risks, it is advisable not to grant direct access to interfaces to third parties but to confer the enforceable right to request an official test conducted by the authorities (comparable to the right to enforce action in criminal law [„Klageerzwingungsverfahren"] or the procedural right to submit motions) to authorised consumer associations and protection organisations. The private institutions would have to submit facts indicating an unlawful algorithmic practice and demonstrate that without an official test they cannot adequately exercise their right to file representative action (respectively their rights of participation or property rights for the benefit of the group of people for whom they have been appointed, cf. sec. 27 f. AGG).

(2) Obligation of service providers to keep records

If it is not possible to prove infringements of an algorithm-based system with suitable instruments *ex post*, this would leave a "blind spot" in the regulation of algorithm-based systems. An effective and adequate regulation therefore includes a duty to record software program operations which might cause lasting harm, e. g. result in significant liability for damages.[105]

---

[102] It may be appropriate to limit the number of permitted accesses for this purpose, for example.

[103] See *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, October 2018, p. 150 f.

[104] *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, October 2018, p. 158 f.

[105] The legislator has already imposed an obligation to keep records (sec. 80 (3) s. 1, 2 Securities Trading Act [*Wertpapierhandelsgesetz*/WpHG]) and to provide information (sec. 80 (3) s.3 WpHG; sec. 6 (4) WpHG, sec. 3 (4) no. 5 Stock Exchange Act [*Börsengesetz*/BörsG] in conjunction with sec. 7 (3) s. 1 BörsG) on algorithm-based processes for algorithmic trading on the financial markets. The procedural obligations are intended to prevent or detect in particular market manipulation. However, they only exist vis-à-vis the competent supervisory authorities. See also *Martini*, Blackbox Algorithmus, 2019, p. 148 ff., 153 f.

Art. 30 GDPR already requires a list of processing activities. But its obligations are limited to elementary data, in particular the name of the controller, the purposes of the processing, etc.[106] The procedural list of Art. 30 GDPR thus lags behind reasonable requirements for active logging of the program sequences. Art. 5 (2) and Art. 24 (1) s. 1 GDPR do neither formulate logging of the processing steps of algorithm-based systems as a mandatory duty – at least not sufficiently clearly. The European Union legislator should establish such a logging duty and define its scope precisely.

However, a rigorous obligation to keep records is not the only conceivable regulatory approach. In future legislation, the decision on the extent of the recording could (in areas which are not highly sensitive to fundamental rights) be placed in the hands of the data controller – while reversing the burden of proof in case of lacking or incomplete records:[107] Should action be brought against an operator of an algorithm-based decision system and should indications of unlawful processing be presented, the operator would have to prove on the basis of its records that the system was in compliance with all legal requirements at the point in time when the algorithm-based decision was taken. Should the operator not succeed in presenting exculpatory evidence, this will bear the risk of uncertainty. Likely, such a construction will induce companies to keep records in areas in which they must expect significant claims for damages or injunctive relief.

2. Institutional design

If the legislator decides to establish an official audit and supervisory regime for software applications sensitive to fundamental rights, it has to decide in whose hands the responsibility shall lie.[108] Conceivable options include (a) a general supervisory authority responsible for regulating algorithmic systems, (b) a supporting institution designed to assist various already existing supervisory authorities by contributing expertise, as well as (c) the inclusion of extra-official audit mechanisms into the total concept.

[106] *Hartung*, in: Kühling/Buchner (ed.), DS-GVO, BDSG, 2nd ed., 2018, Art. 30 GDPR, marginal no. 16 ff.; *Martini* (Fn. 89), Art. 30 GDPR, marginal no. 5 ff.
[107] See already *Martini*, JZ 2017, 1017 (1022).
[108] With regard to the following, cf. *Martini*, Blackbox Algorithmus, 2019, p. 268 ff.

a) General supervisory authority?

In Germany, government supervision of sensitive software applications currently resembles a patchwork: It is distributed across a number of authorities – starting with State and Federal Data Protection Authorities ranging over the Federal Competition Authority[109] (*Bundeskartellamt*) and the State Media Authorities (*Landesmedienanstalten*) to the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungen*/BaFin), the State Exchange Supervisory Authority (*Börsenaufsicht*, in charge of algorithmic trading with financial instruments), the Federal Anti-discrimination Board (*Antidiskriminierungsstelle des Bundes,* sec. 25 AGG) to federal and state supervisory authorities under data protection law (*Landes-/Bundesbeauftragte für den Datenschutz)*.

Pooling these disparate resources in a single federal enforcement body certainly seems rather attractive:[110] A central body could (promptly) build up and concentrate the technical expertise necessary to perform the manifold tasks related to algorithm regulation. It would also be conceivable to establish an entirely new authority for this purpose, perspectively possibly even at the level of the European Union[111].[112]

However, the regulation of algorithm-based processes is highly interdisciplinary: It requires specialised expertise in various fields of supervision, from competition law to data protection and anti-discrimination laws. Correspondingly, any enforcement authority dedicated to regulating algorithmic systems is reliant on expertise in the various areas of its regulatory scope.[113] Data protection authorities, for instance, lack specialist knowledge in anti-discrimination matters, while the anti-discrimination office does not possess in-depth data protection expertise.

[109] *Council of Experts on Consumer Issues at the German Federal Ministry of Justice and Consumer Protection*, Verbraucherrecht 2.0, Dec. 2016, p. 8, 69 ff.; cf. also the demands raised by the federal parliamentarians *Marcus Held* and *Matthias Heider* in *Ludwig*, Mehr Arbeit fürs Kartellamt, Süddeutsche Zeitung Online of 21/11/2016; cf. also *Kieck*, PinG 2017, 67 (67 ff.) and *Körber*, WuW 2018, 173 (173).
[110] *Martini*, Blackbox Algorithmus, 2019, p. 268 f.
[111] *Wachter/Mittelstadt et al.*, International Data Privacy Law 7 (2017), 76 (98).
[112] *Martini*, Blackbox Algorithmus, 2019, p. 270.
[113] *Whittaker/Crawford et al.*, AI Now Report 2018, December 2018, p. 4 therefore propose (in the US-American context) a sector-specific regulatory approach.

BaFin in turn may have the broadest expertise in dealing with official supervision for algorithmic processes, given its supervisory powers for algorithmic securities trading[114], but is not mandated with the task of protecting personality rights.

Most importantly, the complex regulatory framework of federal competence structures hampers the objective of establishing a single federal enforcement authority for algorithm-based processes: The *Länder* (states) are generally in charge of enforcing federal laws (Art. 83 ff. German constitution [*Grundgesetz*/GG]), whereas only few competences to enforce laws and authorities lie at the federal level (Art. 86 f. GG).[115] Under European data protection law Member States are in addition required to maintain data protection supervisory authorities as separate, *independent* supervisory bodies focusing exclusively on data protection and fund them adequately (cf. specifically Art. 52 (1) and (4) GDPR).[116] Consequently, the tasks of algorithm regulation will (have to) remain in the hands of the specialised authorities for the foreseeable future.[117]

b) Supporting service unit

The fact that several authorities share the duty to enforce legal requirements for software applications does not preclude establishing a technically experienced support unit: Such a unit could support the supervisory authorities in preparing enforcement measures.[118] Similar to the German National Metrology Institute (*Physikalisch-Technische Bundesanstalt*/PTB)[119] or the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*/BSI), a *federal, research based service unit* could accumulate technical expertise in controlling algorithm-based processes as a higher federal authority and support the existing law

[114] With regard to the reference area of "algorithmic high-frequency trading": risk management approaches from an administrative law perspective under the German Banking Act (*Kreditwesengesetz*/KWG), Securities Trading Act (*Wertpapierhandelsgesetz*/WpHG) and Stock Exchange Act (*Börsengesetz*/BörsG)" see *Martini*, Blackbox Algorithmus, 2019, p. 142 ff.
[115] With regard to the above see *Martini*, Blackbox Algorithmus, 2019, p. 268 f.
[116] Due to its competence to regulate the economy, however, the Federation would not be constitutionally prevented from placing the competence for the supervision of non-public bodies in the hands of the Federal Commissioner for Data Protection and Freedom of Information.
[117] *Martini*, Blackbox Algorithmus, 2019, p. 270.
[118] *Martini*, Blackbox Algorithmus, 2019, p. 271 f.; similarly *Council of Experts on Consumer Issues at the German Federal Ministry of Justice and Consumer Protection,* Verbraucherrecht 2.0, Dec. 2016 p. 75 and *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, October 2018, p. 172 ff. with suggestions concerning a „digital agency" or rather „agency for ADM-systems".
[119] The PTB is a senior federal scientific and technical agency under the authority of the *Federal Ministry for Economic Affairs and Energy* (*Bundesministerium für Wirtschaft und Energie*).

enforcement authorities as technical investigator by making obtained findings available to them.

The specialised supervisory authorities could then enforce their sovereign powers on the basis of a shared knowledge base. This new institution could, in addition, contribute to the development of methods and tools for converting legal requirements into technical standards or even support it with highly specialised testing teams for individual measures. The constitutional competence to create such a federal service unit lies with the federal government (Art. 87 (3) s. 1 GG).

c) Additional non-authority control mechanisms

In addition to executing its duties through public agencies, the state can, in principle, include private institutions as *administrative assistants* in enforcing the regulatory framework for (learning) software applications. An administrative assistant (*Verwaltungshelfer*) assists in performing public tasks on behalf of and according to directions by the supervising authority. An administrative assistant serves as an extension of the administration comparable to a human tool. The administration retains its supervision and decision-making power (*Werkzeugtheorie* - "tool theory").[120] The supervising authority is responsible for the administrative assistant's actions.[121] However, relying on administrative assistants is only permissible as long as they do not autonomously exercise public competences.

The German Unity Motorway Planning and Construction Company (*Deutsche Einheit Fernstraßenplanungs- und -bau-Gesellschaft GmbH*/DEGES), which supports the planning and construction of federal highways[122], for example, holds a function of an administrative assistant that is to some extent conceptually comparable with the function of technical validation and evaluation of algorithm-based procedures. Another case for reference is the Institute for Quality and Efficiency in Health Care (*Institut für Qualität und Wirtschaftlichkeit im Gesundheitswesen*/IQWiG): It seeks to master the complexity and diversity of medical interdependencies by analysing the current state of medical knowledge on the basis of evidence-based evaluations. Legislation assigns IQWiG a key role in the cost-benefit analysis of pharmaceutical

[120] With regard to tool theory and its development cf. *Kiefer*, NVwZ 2011, 1300 (1302).
[121] See e. g. *Reimer*, in: Posser/Wolff (ed.), BeckOK VwGO, 47th ed. (status: 1/11/2018), sec. 40, marginal no. 80.
[122] See *Martini*, WiVerw 2009, 195 (203 ff.).

products (sec. 35b (1) s. 1 Social Security Statute Book V [*Sozialgesetzbuch V*/SGB V]). In addition, the IQWiG compiles health information on diagnostic and therapeutic procedures and makes them available to the public. The IQWiG merely operates as a body organised under private law (sec. 139a (1) s. 2 SGB V) providing services to the state assisting in the fulfilment of its duties.[123] It has no sovereign decision-making power of its own but is involved in the preparation of administrative decisions.

The government could establish a private company, using the IQWiG as template – as a component of functional, but not actual privatisation (*unechte funktionale Privatisierung*). This company could provide services in testing algorithm-based applications and preparing supervisory measures. Organising such a company under private law may – in comparison to installing a public authority – provide more flexibility and organisational freedom in recruiting staff and performing scientific tasks at a technically high level.

At the same time, organising an institute under private law limits the scope of action an "Institute for Software Testing" could have, as such an institute would gain access to business secrets of companies under its supervision and would be closely involved in performing sensitive supervisory functions through testing etc. It is thus necessary to establish strict legal guidelines to effectively constrain existing risks regarding the organisation under private law. In this regard, the scope of possible tasks which can be assigned to an "Institute for Software Testing" would differ from those assigned to the IQWiG: The IQWiG typically conducts cost-benefit analyses on the basis of already *published* scientific studies, without, however, being able to exercise sensitive sovereign rights or enjoying rights of inspection.

As an alternative to administrative assistants, it would be possible to *delegate* sovereign rights to a private individual (*Beleihung*): The state could transfer the sovereign duty to *supervise and audit* algorithm-based processes to a private institution – similarly to the German Technical Inspection and Certification Association (*Technischer Überwachungsverein/TÜV*, which checks the technical safety of vehicles) or notaries (that perform sovereign tasks in the transfer of real estates). Delegation differs from administrative assistance insofar as private individuals or entities are entitled to autonomously perform sovereign tasks, not as representative of an authority but *in their own name*. They are public authorities themselves, as sec. 1

[123] See *Martini*, WiVerw 2009, 195 (204).

(4) Administrative Procedure Act (*Verwaltungsverfahrensgesetz*/VwVfG) states. Such entrustment is only permissible on the basis of a legal authorisation by law:[124] In particular, legal guidelines must ensure that the delegates do not violate the supervised software operators' trade secrets.

d) Interim conclusion

In order to enforce law in the digital world, the legislator should adjust the state's institutional regulatory system. This is the only way the state can successfully meet the challenges posed by complex algorithm-based systems and channel their enormous potential in a direction beneficial to the common good.

Establishing a government support unit at the federal level is an appropriate step for providing already existing specialist authorities of data protection law, media law, financial services law and competition law with comprehensive and interdisciplinary competence and support. Just as the Federal Authority for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*/BSI) which has proven to be an important support unit through prevention, detection and response in the digital age in the field of "IT security", a (new) state support unit for algorithm-based procedures could constitute an effective component of an audit system for individual fundamental rights and issues of competition law.

The government could entrust this new institution with market and product supervision tools to enable it to exercise comprehensive control (e. g. through surveillance of corporate control systems of internal control or risk management). Individual aspects of government supervision – e. g. standardisation, certification or audit duties – could be delegated to private companies or administrative assistants by law.

III. Ex-post protection

A software process being opaque to consumers impacts their ability to take measures against unlawful practices. Thus, liability (1.) and procedural law (2.) should address asymmetries in knowledge arising from algorithm-based procedures.[125]

[124] See for example *Schmidt am Busch*, DÖV 2007, 533 (538); *Kiefer*, NVwZ 2011, 1300 (1300).
[125] Additionally, cf. already *Martini*, JZ 2017, 1017 (1023 f.); see also *Busch*, Algorithmic Accountability, 2018, p. 68 f.

1. Liabilities

a) Allocation of the burden of proof

If consumers cannot thoroughly understand the processes in the "engine room" of a software application, they will not be able to identify breaches of privacy, the underlying causalities and thus the culpability of service providers – let alone bring forth proof in legal proceedings.[126] Consequently, it is necessary to distribute the burden of proof in a way that allows consumers to more easily defend themselves in legal procedures.[127]

The risk of structural informational imbalances adversely affecting the individual has in the past influenced the regime for medical and producers' liability. To level the playing field, the legislator has reversed the burden of proof in these specific areas (cf. sec. 1 Product Liability Act [*Produkthaftungsgesetz*/ProdHaftG], sec. 630h para. 5 German Civil Code [*Bürgerliches Gesetzbuch*/BGB]). A comparable asymmetry exists in cases where complex software applications cause damage.[128] As a result, the law should ease the burden of proof for users of software applications sensitive to fundamental rights in liability proceedings through a graduated system:[129] it would be sufficient for data subjects to submit facts that strongly suggest that for example impermissible parameters were included in the data processing and have caused a discriminatory decision.[130] These facts brought forward may include findings from a test procedure.[131] Data controllers would then have to refute the presumption of proof by submitting records of their program sequences, providing evidence of adequate supervision of technical processes, or otherwise challenging the assumption of causality.[132]

[126] *Martini*, Blackbox Algorithmus, 2019, p. 274 f.; cf. also *Whittaker/Crawford et al.*, AI Now Report 2018, December 2018, p. 22 ff.
[127] *Martini*, Blackbox Algorithmus, 2019, p. 274 f.
[128] In addition already *Martini*, JZ 2017, 1017 (1023 f.).
[129] In addition already *Martini*, JZ 2017, 1017 (1023 f.).
[130] Similar approach regarding the anti-discrimination law of the General Equal Treatment Act, Federal Labour Court (*Bundesarbeitsgericht*/BAG), NJW 2018, 1497 (1499, marginal no. 23 with further notes).
[131] On the cognitive methods blackbox- and whitebox-test, *Martini*, Blackbox Algorithmus, 2019, p. 44 ff. Regarding the demand for an interface, see p. 27 above.
[132] In addition *Martini*, JZ 2017, 1017 (1024).

b) Strict liability?

Software applications do (in contrast to motor vehicles, for example) not represent a general operational risk. Thus, strict liability (*Gefährdungshaftung*) – mirroring the regulations on pet owners', motor vehicles and drug liability – is only appropriate for particularly sensitive applications[133] (for instance concerning the use of nursing robots). To justify strict liability, there must be a risk of particularly long-lasting damage to important legal assets, specifically life and limb.[134]

2. Legal protection

a) Competitors' powers to issue written warnings

To protect consumers, the state can draw on the vigilance and expertise of competing market participants to take action against inadmissible, but opaque software applications.[135] Companies regularly have an economic incentive to prevent illegal practices by their competitors. Hence, the legislator should extend the power to issue warnings set forth in sec. 12 (1) s. 1, sec. 8 (3) no. 1, (1) in conjunction with sec. 5 (1) s. 1 and 2 no. 6 German Act against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb*/UWG) respectively sec. 3 (3) UWG to software applications that are discriminatory or otherwise infringe personality rights.

However, the right to issue warning notices at the same time entails incentives for its misuse, for example to ensure less the protection of competition than the financial self-interest of the legal service providers. The legislator should counter such incentives by introducing safeguards, for example by capping the reimbursement of costs for warning letters at a fixed amount.[136]

b) Consumer associations' right to take legal action and creation of arbitration boards

A consumer who finds out about an infringement of his rights but does not suffer from long-term damages is typically not inclined to face the financial and time-consuming risks of legal

[133] Possible starting points for regulation thresholds see p. 40 ff. below.
[134] *Martini*, Blackbox Algorithmus, 2019, p. 288 ff.
[135] In addition already *Martini*, JZ 2017, 1017 (1024).
[136] *Martini*, Blackbox Algorithmus, 2019, p. 305 f.

proceedings.[137] As the "patron saints" of a fair market, consumer associations are regularly in a better position to confront companies in lengthy trials. It is therefore advisable to extend the right to bring representative action in sec. 2 (2) German Injunctions Act (*Unterlassungsklagengesetz*/UKlaG) to cases of algorithmic decision-making.[138] However, in order to prevent misuse, this right should be reserved exclusively to not-for-profit associations that are registered as such; furthermore, the rules governing reimbursement should also strictly serve the purpose of preventing misuse and circumvention.

In addition, a state-funded arbitration body that serves as an instance of alternative dispute resolution can lower the threshold and costs for consumers to enforce their rights (cf. in particular sec. 2 ff. Consumer Dispute Resolution Act [*Verbraucherstreitbeilegungsgesetz*/VSBG]).[139] Role models can be the Arbitration Board for Public Transport (*Schlichtungsstelle für den öffentlichen Personenverkehr*/söp) and the clearing house EEG|KWKG responsible for disputes and abstract questions in the area of the Renewable Energy Act (*Erneuerbare-Energien-Gesetz*/EEG) (sec. 81 para. 2, 3 EEG 2017).

IV. Self-regulation

Self-regulatory instruments can be advantageous where government and users have only limited problem-solving competences while software producers are holding superior knowledge. Therefore, it makes sense to include private actors in the regulatory task of enforcing the law. In a legal regime for algorithm-based processes, private actors can, in principle, assume an important supplementary function, which adds to conventional state supervision.

1. Auditing

A certification system legitimised by the state based on private inspection is already applied in numerous areas of law, for example in the field of organic farming (certification for organic products; "Bio-Siegel").[140] In data protection law, Art. 42 GDPR now also establishes the possibility for data controllers to undergo a certification process to obtain data protection seals

[137] Cf. also *Martini*, JZ 2017, 1017 (1024 f.).
[138] *Martini*, JZ 2017, 1017 (1024).
[139] In addition already *Martini*, JZ 2017, 1017 (1025).
[140] Cf. Council Regulation (EC) No. 834/2007 of 28 June 2007 on organic production and labelling of organic products and repealing Regulation (EEC) No. 2092/91, and the Act on the introduction and use of labelling for organic products (Act on labelling organic products (German designation: Öko-Kennzeichengesetz), as amended by

and marks. An accredited certification body could then, for instance, verify whether a facial recognition system meets the requirements of a privacy-by-design certification standard (Art. 25 (1), (3) GDPR)[141] specifically designed for this technology.

However, given the transformability of modern software systems, a mere *ex ante* assessment *certification process* carried out through single-event testing is only of limited use in achieving the intended purpose to protect consumers' rights. A better option is *continuous auditing* over the systems' entire life cycle. Integrating audits in the regulatory system (for example in a manner similar to the Eco-Audit Directive) is particularly useful to incorporate the expertise of private parties in the regulatory task of market and product surveillance.

With the aid of meaningful auditing results, consumers would then due to (ideally) increasing market transparency in the ideal case be able to make informed decisions for (or against) a product or service with specified quality standards – as they similarly do when purchasing food.[142] This would nurture societal and individual trust in digital applications.

2. Algorithmic Responsibility Code

To date, a private codex – be it on national or EU level – serving as a benchmark for corporate approaches to algorithmic decision-making and complementing government regulations has not yet been developed. This has many reasons – largely due to the heterogeneity of manufacturers and operators of software applications and the low level of organisation in protecting user interests. The first private codes of ethics are currently being developed postulating quality criteria for algorithm-based processes.[143]

promulgation of 20/01/2009 (Federal Law Gazette I p. 78), most recently amended by Art. 404 of the Regulation of 31/08/2015 (Federal Law Gazette I p. 1474).

[141] On approved certification mechanisms for privacy-by-design in regard to blockchain technology, *Wirth/Kolain*, Privacy by BlockchainDesign, in: Prinz/Hoschka (ed.), Proceedings of the 1st ERCIM Blockchain Workshop 2018, p. 2.

[142] *Reisman/Schultz et al.*, Algorithmic Impact Assessments, April 2018, p. 16, see an effective incentive structure for companies to gain a competitive advantage, in particular, through increased consumer trust.

[143] Cf., for example, the statement and set of principles of the *Association for Computing Machinery: ACM US Public Policy Council/ACM Europe Council*, Statement on Algorithmic Transparency and Accountability, http://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf (25/10/2018); the principles developed by the high-level think tank *Future of Life Institute*, Asilomar AI Principles, https://futureoflife.org/ai-principles (25/10/2018); the principles of the annual conference on *Fair, Accountable and Transparent Machine Learning: Diakopoulos/Friedler et al.*, Principles for Accountable Algorithms and a Social Impact Statement for Algorithms, https://www.fatml.org/resources/principles-for-accountable-algorithms

Yet empirically looking at past self-regulatory practices, codes of conduct are unlikely to significantly impact the programmers' decision-making when it comes to developing software.[144] Self-regulation has so far written only few success stories. Many existing codes of conduct have proven to be ineffective due to their vagueness and lack of sanctions. Often, they are a mere repetition of applicable law.[145]

The Stock Corporations Act (*Aktiengesetz*/AktG) gives an example of self-regulation "with teeth" in its corporate governance code (sec. 161 AktG).[146] The "German Corporate Governance Code" („*Deutscher Corporate Governance Kodex*") is designed as a private regulatory framework. It does not directly bind the addressees of the Code. However, sec. 161 (1) AktG requires the obliged companies to disclose whether and to what extent they have implemented the recommendations of the Code. If they have not implemented its recommendations into their business practice, they are required to state the reasons for their decision. The regulatory model therefore employs a "comply or explain" approach. As a result, there is an indirect pressure to comply.[147] Although the concrete implementation of the Corporate Governance Code is subject to criticism,[148] the regulatory concept on which it is based is convincing in principle.

Following its fundamental idea, the legislator could initiate an "Algorithmic Responsibility Code".[149] A government commission – consisting of representatives of the relevant stakeholders (especially consumer associations, civil society, software companies, public administration, and scientists) – would then be mandated by law to formulate recommendations on how algorithms should be used in areas sensitive to fundamental rights. Their providers must then explain whether and to what extent they have followed the recommendations.

If monitoring mechanisms manifest that a company's actual conduct is contrary to its public statements, this would ideally not merely trigger lasting loss of goodwill among consumers. Moreover, false statements should also be subject to fines.

(25/10/2018). For a summary and evaluation from a German and European perspectivesee *Rohde*, Gütekriterien für algorithmische Prozesse, 2018, p. 8 ff. and *Floridi/Cowls et al.*, Minds & Machines 28 (2018), 689 ff.

[144] *McNamara/Smith et al.*, ESEC/FSE '18, November 4–9, 2018, Lake Buena Vista, FL, USA, of the type script p. 4.

[145] Similarly critical, *Whittaker/Crawford et al.*, AI Now Report 2018, December 2018, p. 29 ff.

[146] *Martini*, JZ 2017, 1017 (1023); assenting *Busch*, Algorithmic Accountability, 2018, p. 68.

[147] Cf., e. g. *Hölters*, in: id. (ed.), AktG, 3rd ed., 2017, sec. 161, marginal no. 3.

[148] Vgl. etwa *Nowak/Rott et al.*, ZGR 2005, 252 (274, 276, 278 f.); *Bernhardt*, BB 2008, 1686 (1690 f.).

[149] *Martini*, JZ 2017, 1017 (1023).

Key elements of future regulation could be:

(1) Providers of algorithm-based processes sensitive to fundamental rights declare annually that they fully comply with the [...] recommendations of the "Government Commission's Code on Algorithmic Responsibility" or, if not, with which recommendations they do not comply and why.

(2) The declaration shall be permanently accessible to the public on the provider's website.

(3) If a provider's declaration proves to be incorrect, the competent authority may impose a fine in the amount of ... […]

C. Regulatory thresholds: catalogue of criteria to specify when certain regulatory measures apply

By regulating software, the legislator imposes compliance obligations, bureaucratic requirements and further costs on companies, which may negatively and permanently impact net production and growth. Especially when it comes to decentralised networks and learning systems, regulatory measures can be so costly to implement that they undermine the systems' cost-effectiveness.[150] Thus, regulatory caution is called for.

With this in view, a regulation indifferent towards the diversity of applications and software providers falls short. It should rather employ a risk-based approach: Only if and when necessary to contain dangers arising from algorithm-based applications, legal duties should apply.

One of the most important but also most challenging tasks of the legislator in dealing with algorithm-based processes is therefore to define regulatory thresholds ensuring that legal duties are constrained to minimally impact economic development and technological innovation ("I.") and to devise methods to classify individual applications accordingly ("II.").

I. Defining content-related standards

Regulatory thresholds can, in principle, be based on general, especially quantitatively measurable criteria irrespective of the area in which the software in question is used (1.). Vice versa,

[150] *Martini*, Blackbox Algorithmus, 2019, p. 109 f., cf. also *Reichwald/Pfisterer*, CR 2016, 208 (211).

regulatory thresholds may deliberately be adjusted to specific areas of application which are clustered accordingly (2.) or, thirdly, both approaches may be combined (3.).

1. Regulatory thresholds in general

a) Fixed thresholds (e. g. number of employees; turnover)

In data protection law, Art. 30 (5) GDPR constitutes an initial attempt at establishing a suitable regulatory threshold: Regarding procedural requirements, the provision differentiates between companies with more, respectively less than 250 employees. All data controllers below this threshold are generally[151] exempted from the requirement to maintain a record of processing activities under EU law.

The *number of employees* may serve as a guideline for appropriate technical and organisational measures which can *reasonably* be expected of a company. However, it only provides information about how many people would be affected *as employees* by the closure of a business – it does not allow for conclusions regarding the number of people affected by *processing operations*, let alone the processes' sensitivity in terms of data protection. Thus, the number of employees can only serve as a criterion to a very limited extent when defining a threshold determining which companies should be subject to regulatory measures concerning their software applications.

Antitrust law (as well as the law governing algorithmic trading in financial instruments[152]) takes an approach somewhat different from the GDPR: it reverts to *economic turnover* as threshold; see for example, sec. 35 (1) German Act against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen*/GWB): "turnover of more than EUR 500 million", or Art. 1 (2) of Regulation (EC) No. 139/2004.

The turnover provides an indication of the market penetration of an offer. However, the experience in antitrust law shows that a turnover threshold more and more loses its precision

[151] However, the requirement is upheld if data are processed regularly, data processing involves personal data on criminal convictions and offences, or if there is a risk to the rights and freedoms of data subjects for other reasons. With regard to this provision and its initial, ambiguous wording, cf. *Martini*, in: Paal/Pauly (ed.), DS-GVO/BDSG, 2nd ed., 2018, Art. 30 GDPR, marginal no. 26 ff.

[152] The legislator assumes that high-frequency trading poses a higher risk due to the increased trading volume than purely algorithmic trading. Therefore high-frequency trading is subject to a fundamental reservation of permission and extended documentation requirements, in detail *Martini*, Blackbox Algorithmus, 2019, p. 147 ff.

as a criterion of selection in a digital network economy.[153] In order to take into account the particularities of the digital economy, the legislator has recently adapted sec. 18 (2a), (3a) GWB: network effects and the market advantage of access to data have to be taken into account when determining a company's market position. It is no longer decisive for the assessment under antitrust law whether the service provider grants services in exchange for payment or in exchange for data.

It remains to be seen whether the new criteria are sufficiently specific and applicable.[154] However, they trigger extensive valuations by the antitrust authorities: based on a complex set of criteria, they must first determine whether sec. 18 GWB applies.[155] The legislator apparently chose this open-textured course specifically to keep the GWB receptive to innovation[156] and to avoid rigidly defining the scope of application of sec. 18 GWB.[157]

However, the criteria used in sec. 18 (2a), (3a) GWB are only to a very limited extent suited for defining regulatory thresholds oriented towards *personal rights* that a software application might infringe: A company's turnover says little to nothing about whether the data it processes or the decisions it makes are sensitive to individuals' fundamental rights or associated with substantial risks to society. The example of *Cambridge Analytica* has impressively demonstrated that there is no need for billions in revenues to threaten collective privacy. Antitrust law has a different focal point than the regulation of algorithm-based processes which aim at the protection of the end user: the former is market-regulating and directed at *companies' impact on competition*. The regulation of algorithm-based processes, on the other hand, primarily serves to protect consumers as market participants and holders of personal rights. A threshold based on turnover thus can at best serve as an initial indicator for the level of market relevance. It would, however, be conceivable to use a turnover criterion in order to *remove*

[153] Experiences gained from antitrust law show that profit thresholds hold little promise for defining scopes in the digital domain; cf., for example, the acquisition of WhatsApp by Facebook: *Federal Cartel Office*, Joint Guidelines on the new transaction value thresholds for merger control rules in Germany and Austria – public consultation, 14/5/2018; *Anonymous*, EU prüft Übernahme von WhatsApp, Focus Online, 14/7/2014.
[154] Cf. *Podszun/Schwalbe*, NZKart 2017, 98 (101).
[155] Cf., for example, *Paal*, in: Gersdorf/Paal (ed.), BeckOK InfoMedR, 21st ed. (status 1/8/2018), sec. 18 Restriction of Competition Act (*Gesetz gegen Wettbewerbsbeschränkungen*/GWB), marginal no. 9.
[156] Cf. Bundestagsdrucksache 18/10207, p. 48 f. ("case by case assessment", "on the basis of an overall view of all given circumstances"); cf. *Podszun/Schwalbe*, NZKart 2017, 98 (100).
[157] The antitrust literature speaks of a "practical search process" in digital markets to define markets and assess market power, cf. *Podszun/Schwalbe*, NZKart 2017, 98 (102).

small companies from specific regulatory restrictions which threaten to strangle their innovative capacities.[158]

b) Number of data subjects (potentially) involved

The number of (potentially) affected persons indicates that the impact of a possible infringement is higher than in other cases. Accordingly, how risky a particular software is, depends on, amongst other factors, the number of its users. The number of fundamental rights holders currently (or in the future) exposed to a software application constitutes an important benchmark for determining the appropriateness of a regulatory measure. Therefore, Art. 35 (1) s. 1 GDPR ties the threshold for the obligation to conduct a data protection impact assessment to the "scope" of the processing.

French legislation uses a similar point of reference: Platforms with over 5 million connections per month are regulated more strictly than those with fewer connections. Only large platforms are required to comply (in addition to general transparency regulations, which specifically oblige them to disclose information about their economic dependencies) with (self-imposed) best practice rules (so-called *bonnes pratiques*) monitored by the authorities.[159]

However, it is difficult for stakeholders on both sides of the regulation, addressees and protected, to make any legally reliable predictions for individual cases based on the criterion “number of persons affected”. If legislators were to set a specific number, this would only

[158] For example, Art. 17 (6) of the new Copyright Directive (EU) 2019/790 with regard to exceptions to provider responsibility for constellations in which users share online content ("whose annual turnover (...) does not exceed EUR 10 million").

[159] See Art. D111-15 (in force from 1/1/2019), Art. 111-7, Art. 111-7-1 Code de la consommation: “I.-Le seuil du nombre de connexions au-delà duquel les opérateurs de plateformes en ligne sont soumis aux obligations de l'article L. 111-7-1 est fixé à cinq millions de visiteurs uniques par mois, par plateforme, calculé sur la base de la dernière année civile. […]”;
Art. 111-7-1 Code de la consommation: “Les opérateurs de plateformes en ligne dont l'activité dépasse un seuil de nombre de connexions défini par décret élaborent et diffusent aux consommateurs des bonnes pratiques visant à renforcer les obligations de clarté, de transparence et de loyauté mentionnées à l'article L. 111-7. […]”;
Art. 111-7 Code de la consommation: “[…] II.-Tout opérateur de plateforme en ligne est tenu de délivrer au consommateur une information loyale, claire et transparente sur:
1° Les conditions générales d'utilisation du service d'intermédiation qu'il propose et sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder;
2° L'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération à son profit, dès lors qu'ils influencent le classement ou le référencement des contenus, des biens ou des services proposés ou mis en ligne;
3° La qualité de l'annonceur et les droits et obligations des parties en matière civile et fiscale, lorsque des consommateurs sont mis en relation avec des professionnels ou des non-professionnels […]”.

provide limited information about how many cases involve a risk for fundamental rights and how rigorous the violations would be; it would disregard the impact on individual cases. For example, calculator apps (without additional background data processing), are used by millions of people and do usually not pose a threat to the users' personal rights. In contrast, a collaborative robot, of which only 80 units are used in a special market segment (e. g. transport of chemical substances), can pose a much greater risk. An *exclusively* "quantitative" approach therefore threatens to overlook actual sources of danger.

c) Fundamental rights sensitivity as the connecting factor to the purpose of protection

The quest for an adequate threshold should above all be guided by the objective in regulating software applications: it intends to satisfy the state's obligation to protect its citizens – especially protecting their fundamental rights closest to the constitutional guarantee of human dignity, such as the right to informational self-determination and the fundamental rights to equality ("To respect and protect it [human dignity] shall be the duty of all state authority" [Art. 1 (1) s. 2 GG respectively Art. 1 s. 2 European Charter of Fundametal Rights (ECFR)[160]]).

This implies that the *sensitivity to fundamental rights* of algorithmic decisions should be used as basis for defining regulatory thresholds: The more extensively an application interferes with interests protected by fundamental rights, the stronger is the need for transparency, equal treatment and fair market opportunities – and the easier it is vice versa to constitutionally justify necessary restrictions on occupational freedom (Art. 15 (1) and Art. 16 ECFR; Art. 12 (1) GG) and freedom of property (Art. 17 ECFR; Art. 14 (1) GG). In line with these considerations, the GDPR refers to the "purpose of the processing" and whether it is "likely to result in a high risk to the rights and freedoms of natural persons" in Art. 24 (1) s. 1, Art. 25 (1) s. 1, Art. 32 (1) s. 1 and Art. 35 (1) s. 1 GDPR.

Whether a specific software application is sensitive to fundamental rights, should be assessed on the basis of a tiered model: It differentiates in particular according to the sensitivity to the personal expression involved in individual cases of algorithm-based processes. It specifically distinguishes between the public sphere, the everyday social sphere and the private sphere (as the core area of most private way of life [in German constitutional judicature: *Kernbereich privater Lebensführung]*). However, this can, again, merely serve as an initial indication: On

[160] "It must be respected and protected".

the one hand, the individual spheres of life are not hermetically shielded from each other, but rather merge and overlap. On the other hand, personal expression can also be sensitive, precisely because it takes place in the public sphere.

aa) Impacts on fundamental rights other than the right to informational self-determination

The legislator should grant special protection where algorithm-based processes have lasting effects not only on privacy and personality rights but also on other fundamental rights. In that case, the core guarantees of fundamental rights to be protected by the state even between private actors (*objektiv-rechtlicher Gehalt der Grundrechte*) intensify and constitute the state's duty to protect entitled individuals. This is particularly true for the *right to life and physical integrity* (Art. 2 and 3 ECFR, Art. 2 (2) s. 1 GG), the *principle of equality before the law* (Art. 20 ECFR, Art. 3 GG including the special principles of non-discrimination in Art. 21-26 ECFR, Art. 3 (2 and 3) GG), and the *freedom of faith and conscience* (Art. 10 ECFR, Art. 4 GG), the *freedom of expression* and information (Art. 11 ECFR, Art. 5 GG), the *freedom of assembly* and of association (Art. 12 ECFR; Art. 8 (1), 9 (1) GG), the *occupational freedom* (Art. 15 (1) and Art. 16 ECFR; Art. 12 (1) GG), the *freedom of property* (Art. 17 ECFR; Art. 14 (1) GG), the *principle of effective judicial protection* (Art. 47 (1) ECFR, Art. 19 (4) GG) as well as for the *principle of a fair trial* and the associated *principle of procedural equality* (Art. 47 (2) ECFR, Art. 6 ECHR).

Again, it is necessary to regulate with acute awareness of proportionality: as a rule, private sector operators of algorithm-based processes are not directly bound by fundamental rights (Art. 51 (1) s. 1, Art. 1 (3) GG). Rather, they are *protected* by fundamental rights: they can evoke their occupational freedom, freedom of contract and freedom of property in order to defend themselves against intrusive government action. Adequate regulation must therefore aim at balancing the competing freedom and equality rights with as little encroachment to any affected fundamental right of operators as possible (known as *praktische Konkordanz*, "practical concordance").

bb) Risk of excluding consumers from important areas of life - Relevance of participation and availability of alternatives

Under German constitutional law, private individuals are generally not bound by fundamental rights. But in exceptional cases, the actions of private individuals can impair the fundamental rights of others so profoundly in their conduct of life that they are by exception (directly) bound by fundamental rights.[161] This is the case when private parties accumulate so much power that they can exclude people from important areas or life. Determining factors are the "social significance of certain services" or the "social superiority of one party" arising from a dependency on a service (e. g. because there is no equivalent alternative available to those excluded).[162] The *Bundesverfassungsgericht* has developed these criteria specifically for bans from (football) stadiums. But they can also serve a useful evaluation category for defining a threshold for the regulation of algorithm-based procedures that recur to the state's duty to protect under Art. 20 ECFR, respectively Art. 3 GG: if an application – either because of its market power (e.g. Facebook)[163] or because of its content orientation (e. g. online offers of public agencies) – grants access to central areas of life and thus assumes a gatekeeper function for pursuing life plans, it is justified to subject it to stricter regulatory measures. Where, on the other hand, consumers have a large number of alternatives which satisfy their needs and interests in an equivalent manner (i. e. where there is a fully functioning market), the need for regulation diminishes and the individual's responsibility for making an appropriate choice takes over.

If, in certain sectors of the labour market, a software system controls the screening of applicants either predominantly or exclusively (such as the analysis software of the company "HireVue")[164] it obtains a monopoly over applicants comparable to a credit agency based off a credit score.

It is difficult to operationalise the abstract criteria of "exclusion from important, participation-relevant areas of life" or "social power of one side" with any degree of legal certainty. Neither those affected by the use of algorithms nor the supervisory authorities nor the operators

[161] Cf. – regarding Art. 3 (1) GG – Federal Constitutional Court (*Bundesverfassungsgericht*/BVerfG), NVwZ 2018, 813 (815, marginal no. 33).
[162] With regard to this subject area, cf. Federal Constitutional Court, NVwZ 2018, 813 (815, marginal no. 33).
[163] Cf. e. g. *Weinzierl*, Warum das Bundesverfassungsgericht Fußballstadion sagt und Soziale Plattformen trifft, JuWissBlog No. 48/2018 of 24/5/2018.
[164] See also *Wischmeyer*, Der Computer, der mich einstellte, brand eins of 4/12/2017.

would be able to assess with legal certainty whether a particular regulatory threshold has been met or not. These criteria are consequently poorly suited as sole benchmarks for defining legal scope. It is therefore more expedient to use these criteria as an orientation framework, on whose basis the legislator can either himself draw down sector-specific regulatory thresholds for individual applications or, within the limits of the parliamentary reservation, delegate to the enforcement authorities the possibility to take an evaluative decision for or against regulation.

cc) Specially protected categories of personal data

If a software application accesses specially protected categories of personal data within the meaning of Art. 9 (1) and Art. 10 GDPR (cf. also recital 51 ff. GDPR), this strongly indicates its sensitivity and need for regulation (cf. also Art. 35 (3) lit. b GDPR). Sensitive data include, in particular, racial and ethnic origin, political opinions, religious or philosophical beliefs as well as genetic and biometric data, data concerning health or data on a person's sex life or sexual orientation. Data relating to children also deserve special protection (cf. also Art. 8 GDPR, recital 38).

d) Interim conclusion

The difficulty in fine-tuning regulation on algorithm-based processes is not primarily due to the fact that there are no differentiation and prediction criteria. On the contrary, there are too many criteria for a simple and meaningful distinction between different tiers of specific risks. A general criterion, such as the category "connected to risks to fundamental rights" or a decision "which produces legal effects […] or similarly significantly affects him or her" (Art. 22 (1) GDPR) may be useful as lowest common denominator, but remains too unspecific to form precise legal classifications or to be tied to any specific legal consequences. Thus, a *one-size-fits-all*-approach cannot do justice to the variety of algorithm-based processes, their objectives and the varying risk spheres of fundamental rights involved. Depending on the economic sector and area of use of software applications, varying parameters and criteria will consequently – *nolens volens* – be required to address predictable risks.

2. Regulatory thresholds in specific areas – Identification of applications requiring regulation

If the legislator tries to develop a regulatory model with different tiers taking into account variable risk factors, it appears useful to take a sector-specific approach identifying particularly high-risk sectors which should be subject to both, increased regulatory supervision and stricter requirements – ranging from a preventive mechanism, such as market access permits and *ex ante* impact assessments, to strict liability standards. On the other hand, the legislator could apply less intrusive obligations more widely – such as access rights for testing and audits for supervisory bodies as well as transparency and labelling obligations – to enable supervision and counteract risks in individual cases.

Particularly relevant sectors that the legislator should consider for a stricter regulatory regime include:

- systems *processing health data* and affecting medical treatments (in particular health apps) or applications whose decisions may result in *physical harm* (e.g. care robots);
- *credit agency* scoring and profiling, as far as it impacts important areas of life;
- algorithm-based decisions regarding *insurances* essential for a person's lifestyle (e. g. health insurance, motor vehicle liability insurance, household contents insurance, disability insurance);
- new technologies that allow for a *particularly intense analysis* affecting sensitive personality spheres, in particular facial recognition, key logging, sentiment analysis, digital language assistants with smart home applications (Siri, Alexa, etc. ["Internet of the voice"], especially those associated with the risk of collecting and sending unauthorised data, as well as the risk of external attacks or of analysing emotions and moods or information from the core area of private life) and personalised digital *educational services*;
- *autonomous driving*, in particular analysis of driving behaviour;
- applications that can have a lasting impact on the *formation of public opinion*, e. g. social bots, rating websites;
- algorithm-based decisions affecting *professional life* (internal and external applicant selection; performance monitoring through scoring or profiling);

- human-machine collaboration, e. g. cobots, exoskeletons[165] or digital work glasses;
- private or governmental *systematic monitoring of publicly accessible areas*[166] and smart city concepts tracking the mind-set in local communities using sensors and combining data from different sources into a local control concept;
- algorithm-based procedures applied *by the state*, including those used to prepare or support a decision, especially in the judiciary and administration.

3. Combined solution

An efficient monitoring system for algorithm-based procedures which strives to take into account any possible risks should identify sectors with specific needs for regulation and establish general risk criteria, thus relying on a *holistic assessment* of all individually relevant aspects and connecting them to define regulatory thresholds. Only an *overall risk assessment* can ultimately cope with the Herculean task of defining critical regulatory thresholds.[167]

a) Risk factors

Whether a software application comes with a "risk" needs to be determined by two factors: the probability of occurrence multiplied by the severity of the expected damage.[168] The risk factors determining the severity of the damage include in particular the type (aa) and the extent (bb) of an expected damage.

aa) Types of damage

Typical risks which, due to the *type* of expected damage, necessitate regulation include in particular:

- *discrimination* against persons, in particular by systems extensively processing specific categories of personal data or data relating to criminal offences (cf. Art. 9 f. GDPR);[169]

[165] See also *Martini/Botta*, NZA 2018, 625 (625 ff.).
[166] Cf. also Art. 35 (3) lit. c GDPR.
[167] This understanding is also the basis for the risk concept in the GDPR, as expressed in particular in Art. 24 (1) s. 1, Art. 25 (1), Art. 32 (1), Art. 35 (1) GDPR.
[168] *Martini*, in: Paal/Pauly (ed.), DS-GVO/BDSG, 2nd ed., 2018, Art. 35 GDPR, marginal no. 15b; cf. also recital 90 p. 1 and *Article 29 Data Protection Working Party*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248, 4/10/2017, p. 9 ff.
[169] Cf. also the normative component of Art. 35 (3) lit. b GDPR.

- damage that is *not easily or not at all reversible*, in particular:
  - reputational damage, identity theft or fraudulent use of identities,
  - breach of confidentiality in regard to data protected by professional secrecy,
  - destruction, loss, manipulation, or unauthorised disclosure of, or unauthorised access to, personal data;[170]
- decisions that are based on a *comprehensive assessment of personal characteristics* with lasting negative impact, such as profiling measures, in particular when combined with location data;[171]
- the extraction of (in particular sensitive) data from the original processing context in order to direct them to new processing purposes within the framework of a *big data analysis*.

bb) Extent of expected damage

Risks arising from the *extent* of the damage include in particular:

- a *large number* of affected data subjects;[172]
- impacts on *fundamental rights other than the right to informational self-determination*, in particular the right of life and physical integrity, the freedom of assembly as well as the freedom of expression;[173]
- the *scope, circumstances, frequency and duration* of the processing or storage. The more data are entered into a tool of big data analysis, the more closely the software links the data together, the more sensitive the context in which the processing takes place, the longer the processing takes and the more frequently it happens, the bigger is typically the sensitivity emanating from the processing operation (cf. also Art. 24 (1) s. 1, Art. 25 (1) and Art. 35 (1) s. 1 GDPR).

[170] Cf. also recital 75, 83 p. 3 and 85 p. 1 GDPR.
[171] Cf. also Art. 35 (3) lit. a GDPR.
[172] See p. 43 f. above.
[173] See p. 45 f. above.

b) (Qualitative) specification of risk thresholds

Although the need for easily definable differentiation criteria is high, it is inevitable to include interpretive elements. In particular, attention must be paid to whether the cumulation of various individual aspects leads to an exceedance of a predefined (quantitative and qualitative) threshold. The decision as to whether or not the risk threshold has been exceeded can generally be based on *abstract lists*[174] of positive and negative criteria.

II. Procedural instruments of specification – limits to the delegation of regulatory power

Due to the speed at which technical innovations of the digital world progress, the legislator is forced to rely on predictions when specifying regulatory thresholds. By their very nature, predictions are marked by uncertainty. Not all developments and risks can be anticipated. Normative specifications which are too narrow lack the flexibility that is required in order to be able to react precisely to the particularities of each individual case. Even last century, *Georg Jellinek* regarded it as almost "impossible to want to govern the real life of the state a priori without exception by law".[175]

In order to maintain the accuracy of the regulatory system even under the dynamic conditions of rapid technological developments and in order to be able to adequately react to situational regulatory needs, a viable solution is to entrust the executive branch with specification. The legislator could, in particular, establish exemptions and flexibility clauses for specific regulatory instruments to permit – dependent on a categorising case-by-case assessment – derogations from the underlying legal rules. They would grant supervisory authorities sufficient executive discretion, which they could exercise based on accrued knowledge and expertise. As a result of this normative approach it would therefore be conceivable to have an algorithmic system which inherently presents a high risk, but does not reach the threshold invoking regulation if the controller has implemented special protective measures. Instruments of executive self-programming could in this way, principally, specify rules of exemptions and identify

[174] Cf. the similar regulatory model of Art. 35 (4) and (5) GDPR; an overview of DPIA-lists can be found in the opinion of the European Data Protection Board (EDPB), https://edpb.europa.eu/our-work-tools/our-documents/topic/data-protection-impact-assessment-dpia_en (24/4/2019).
[175] (Own translation of) *Jellinek*, Gesetz und Verordnung, 1919 (1887), p. 369.

unique cases in which those rules should apply to provide for a timely and appropriate response to technical change. Such rules would grant supervisory authorities a margin of discretion within which they could make use of their executive judgment and experience.

The law already provides for numerous executive assessment procedures designed for adjusting and determining the need for regulation on a case-by-case basis – from market definition and market analysis according to sec. 10 f. German Telecommunications Act (*Telekommunikationsgesetz*/TKG; which grants the regulatory authority a margin of discretion; sec. 10 (2) s. 2 TKG) to the exemption from the obligation to make and publish an offer for a target company (sec. 37 (1) German Securities Acquisition and Takeover Act [*Wertpapierübernahmegesetz*/WpÜG]), the exemption from the obligation to hold a passport (sec. 2 (1) Passport Act [*Passgesetz*/PassG]) through to special dispensation under construction laws based on sec. 31 (2) German Building Code (*Baugesetzbuch*/BauGB).

As part of its risk assessment in the future, the administration should, regarding the valuation of algorithm-based processes, assign a risk score to both the severity of potential damage (particularly with regard to the relevance of fundamental rights, the number of persons affected, etc.) and the probability of its occurrence, aggregating the score for a comprehensive decision. It then compares the risk score with the threshold as defined by the legislator.

Once the risk threshold has been reached, however, the (economic) interests of the provider have to be taken into account in a "reverse impact assessment": The legislature and the supervising authority are bound by the fundamental principle of proportionality – also and especially vis-à-vis actors in the private sector in the digital economy. In particular, the required resources, the feasibility of complying with the additional obligations (e.g. with regard to start-ups) and the risk that business and company secrets could be disclosed to the public fall into balance for a revocation exemption.

As part of a “self-categorising approach”, it is conceivable to delegate the assessment whether certain obligations are complied with to the subject of regulation, respectively the operator of the algorithm-based system. An incorrect assessment could be legally punished by (strict) liability in particular by shifting the burden of proof, the presumption of culpability and with sanctions. A self-assessment system could help to minimise bureaucratic and financial cost – not least, the operator can respond more quickly to changes in conditions affecting its system than a supervisory authority. However, such an approach would entail a significant amount of

legal uncertainty. Secondly, risk self-assessments can generally only be acceptable where the risk remains below a critical threshold and does not require extensive regulation (and particularly: no in-depth state supervision).

1. Specification of provisions in national law

a) Constitutional framework for the specification of provisions – delegated regulations as an instrument for specifying provisions

The right to specify regulatory instruments through normative guidelines in order to operationalse them is, in principle, constitutionally reserved to the parliament. As the democratic center of gravity for political decision-making, it is appointed to make key policy decisions of the democratic community.

However, the parliament does not have a legislative monopoly.[176] It may – within the limits of Art. 80 German Constitution (*Grundgesetz*/GG) – delegate *the normative fine-tuning process* to the executive branch. The legislator may in particular grant the regulatory authority the power to define exemptions from statutory regulation obligations by means of delegated acts or, conversely, to define a specific scope of regulatory obligations in certain domains again, by means of specifying the related norms.

The imission control law, for example, makes use of this tiered regulatory method regarding a decisive matter. Annex 1 to the 4th Federal Immission Control Ordinance (Vierte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes /4. BImSchV) defines all installations that require a permit within the meaning of sec. 4 (1) s. 3 Federal Immission Control Act (*Bundes-Immissionsschutzgesetz*/BImSchG) in conjunction with sec. 1 (1) s. 1 of the 4th BImSchV. Such an approach is also feasible as part of a regulatory system for algorithm-based processes in principle: The legislator could delegate the specification of software applications that fall under a specific risk class. Conversely, the legislator could allow the (executive) regulator to provide for sector-specific exceptions for individual normative instruments with low-threshold delegated acts in order to keep pace with the dynamics and response needs of the digital world. This allows the delegating legislator – i. e. the federal government or one of its minis-

[176] *Martini*, AöR 133 (2008), 155 (160).

tries – to exempt particular sectors or forms of applications from otherwise generally applicable rules – or to modify and fine-tune any of its legal obligations sector-specifically for individual applications. The legislator used a similar approach in legislation concerning genetic engineering (e. g. in sec. 30 and, among others, sec. 17b, 18 (3), 36 Genetic Engineering Law [*Gentechnikgesetz*/GenTG]).[177] Sec. 17b (1) s. 2 GenTG, for example, authorises the executive to exempt individual products from otherwise mandatory labelling obligations by delegated regulation, if they are below a *predefined threshold*, in which the accidental or technically unavoidable presence of genetically engineered organisms cannot be excluded, (cf. Art. 21 Directive 2001/18/EC).

The legislator also chooses such a "normative-iterative" approach in water legislation – i. e. to define risk thresholds or to specify application sectors and to categorise their scope of obligations in detail by means of a statutory order. Sec. 57 (2) German Water Resources Act (*Wasserhaushaltsgesetz*/WHG) authorises the executive to define, by means of delegated regulations, requirements regarding the “state of the art” in the discharge of waste water into water bodies.[178] The legislator made use of this in 57 annexes to the German Waste Water Ordinance and specified in detail which requirements and limit values are to be considered for specific discharge processes – from domestic and municipal waste water to milk processing and wool laundries.

b) Limits of delegation of regulatory powers by law to private actors, in particular to an expert committee in technology and ethics

At first glance it appears tempting for the legislator to directly enable a *committee of experts* to specify norms and exempt sectors or forms of applications from otherwise generally applicable laws. However, the German constitution sets insurmountable limits for leaving it to an interdisciplinary committee to specify the applicable law.

[177] The jurisdiction based on higher court decisions has confirmed the administrative authorisation to substantiate norms in genetic engineering law; cf. Federal Administrative Court (*Bundesverwaltungsgericht*/BVerwG), NVwZ 1999, 1232 (1233 f.).

[178] With regard to the predecessor regulation, sec. 7a Water Resource Act (*Wasserhaushaltsgesetz/*WHG*),* old version, for which the administrative is authorised by the jurisdiction to substantiate norms according to case law, cf. Decisions of the Federal Administrative Court (*Bundesverwaltungsgerichtsentscheidungen*/BVerwGE) 107, 338 (340 ff.).

As an expression of the principle of the separation of powers and of democracy, Art. 80 GG sets a narrow constitutional frame for delegating normative regulatory powers: principally, the constitution does permit the setting of legal norms in a collaborative, decentralised manner to unburden parliament and adjust legislation to the needs of a dynamic society.[179] At the same time, it defines strict prerequisites under which legislation may be delegated to *administrative bodies* – in particular with regard to content, substance, purpose and scope. Neither the regulatory authority nor the parliament as legislator may depart from them. In the reverse conclusion, other forms of delegating legislative power – in particular to entrust them to private actors – are not permitted. Otherwise the requirements established by Art. 80 GG could be easily circumvented and the purpose of this article undermined.

Art. 80 (1) s. 4 GG allows another sub-delegation of regulatory power: it is permitted insofar as a law states "that an authorisation can be transferred further" and that the executive transfers the authorisation via a statutory ordinance.[180] But only state institutions, integrated into the uninterrupted democratic chain of legitimation, are permissible delegatees. Art. 80 GG thus safeguards democracy: it is intended to protect the "integrity of democratic legitimacy"[181] for all governmental activities. As a result, it is constitutionally inadmissible to delegate primary regulatory powers to non-state bodies.[182]

Especially dynamic references to sources of law that have not been formally created as constitutionally required,[183] by parliament, are not admissible – for example references to specific DIN legal standards "as amended": the legislator must assume responsibility for each individual case in the knowledge of its specific content.[184] Otherwise, the legislator transfers legislative power to private actors in an unconstitutional manner. They would be in a position to take on the central task of defining democratically legitimised rules for the community and to restrict the fundamental rights of third parties on their own authority. The legislator could

[179] *Martini*, AöR 133 (2008), 155 (160).
[180] Cf. regarding legal ban on delegations of Art. 80 German Constitution (*Grundgesetz*/GG) *Martini*, AöR 133 (2008), 155 (159 ff.).
[181] *Martini*, AöR 133 (2008), 155 (161).
[182] *Lepa*, AöR 105 (1980), 337 (359); *Kloepfer*, Umweltrecht, 4th ed., 2016, p. 153 with further notes.
[183] For further detail cf. *Becker*, Kooperative und konsensuale Strukturen in der Normsetzung, 2005, p. 381 ff.; with regard to practical application cf., above all, *Augsberg*, Rechtsetzung zwischen Staat und Gesellschaft, 2003, p. 173 ff.
[184] *Kloepfer*, Umweltrecht, 4th ed., 2016, p. 154.

easily circumvent the differentiated delegation system of Art. 80 German Constitution – and thus its meaning as a bulwark of the constitutional order.

While dynamic references exceed the limits of permissible delegation of power,[185] the admissibility of *static* references to rules and regulations of private institutions, for example industrial standards of DIN, is an entirely different matter:[186] Its content is fixed at the point in time when the legislation enters into force. The legislator can incorporate it into its will and commit itself to its content by legislative decision.[187] It thus frequently makes use of the possibility of statically referring to DIN standards, especially in environmental and technical law – for example in the references of sec. 3 (1) First Federal Immission Control Ordinance (*1. Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes [Verordnung über kleine und mittlere Feuerungsanlagen]* /1. BImSchV) and sec. 2 (8), sec. 19, 6 (1) Thirteenth Federal Immission Control Ordinance (*13.* Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes /13. BImSchV).[188]

The mere *participation* of an expert committee in developing proposals for the delegating legislator is also generally permissible under constitutional law. Participatory consultation is something other than the setting of regulations; rather, only (directly binding) legislative imperatives which result from decisions require democratic legitimation.

The states' task consequently consists in ensuring an adequate level of legitimacy through facilitating proper conditions for a decision even when private individuals are involved in de-

[185] From the perspective of the functional order given by the German Constitution, the reservation of the right to make amendments granted to the Bundestag under sec. 113 s. 5 Act against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen*/GWB) regarding the Regulations on the Award of Public Contracts (*Vergabeverordnung*/VgV) is dogmatically remarkable and unconstitutional: the Bundestag may amend the Regulation by resolution; cf. *Fandrey*, in: Kulartz/Kus/Portz et al. (ed.), 4th ed., 2016, sec. 113, marginal no. 8 f. As a result, the parliament turns into an issuer of a statutory instrument, outside of the constitutionally defined types of legislation (namely by resolution). However, such reservations of the right to make amendments undermine the dogma expressed in Art. 80 German Constitution. With regard to the constitutional difficulty of parliamentary reservations of the right to make amendments in delegated legislation cf. *Saurer*, NVwZ 2003, 1176 (1177 ff.); *Martini*, AöR 133 (2008), 155 (176). An amendment of the regulation would only be admissible by law amending the regulation.

[186] *Kloepfer*, Umweltrecht, 4th ed., 2016, p. 154 with further notes.

[187] With regard to the copyright implications of an incorporation of private sets of rules in laws, see sec. 5 (1) Copyright Act *(Urhebergesetz*/UrhG), regarding the reference see sec. 5 (3) Copyright Act.

[188] Also the TI Air and TI Noise frequently refer to directives of the VDI and DIN standards, as binding administrative regulations, see e. g. Number 5.1.1. last sentence and Number 5.2.6.3 of the TI Air or Number 2.6 and A.1.6 (annex) of the TI Noise.

veloping legislation. The legislator especially must ensure that the decision-making environment is adequately democratic.[189] This specifically includes a sufficient level of overall democratic legitimation.[190] In particular, the state has to define the framework for the involvement of private parties in the decision process and guarantee the transparency of the decision process.[191] The stronger the private parties' proposals affect those subject to a law, the more precise the framework provided by the state has to be, both on a procedural and substantive level.[192] As long as the regulations proposed by an expert committee are *non-binding* and as long as the state remains in charge of the legislative process, it will generally be admissible to make proposals to specify the law in force in a particular way. Sec. 1 (2) s. 2 of the German Minimum Wage Act (*Mindestlohngesetz*/MiLoG), for example, establishes a right of proposal for a standing commission of the social partners (so-called Minimum Wage Commission). Sec. 36 (1) s. 1 of the Drug Act (*Arzneimittelgesetz*/AMG), for example, expressly demands that experts have to be heard before an ordinance is issued.

An important practical example for the executive specification of laws based on external consultation with numerous other private bodies are the "technical instructions" within the meaning of sec. 48 Federal Immission Control Act (*Bundes-Immissionsschutzgesetz*/BImSchG), i. e. the Technical Instructions Air (*Technische Anleitung Luft*/TA Luft) and Technical Instructions Noise (*Technische Anleitung Lärm*/TA Lärm): as general administrative regulations within the meaning of Art. 84 (2) German Constitution (*Grundgesetz*/GG), issued by the federal government after hearings as provided for in sec. 51 Federal Immission Control Act and approval by the German Federal Council (*Bundesrat*), Technical Instructions Air und Technical Instructions Noise specify provisions in the Federal Immission Control Act (which is subject to *Länder* (states) administration). Due to their status as *norm specifying administrative regulations*, based on scientific research and a complex balancing mechanism which guarantees a high level of expertise, accuracy and legitimacy through procedures[193], the Technical Instructions

[189] *Augsberg*, Rechtsetzung zwischen Staat und Gesellschaft, 2003, p. 84; *Ruffert*, Rechtsquellen und Rechtsschichten des Verwaltungsrechts, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (ed.), Grundlagen des Verwaltungsrechts Vol. I, 2nd ed., 2012, p. 1163 (1214 f.).
[190] Decisions of the Federal Constitutional Court (*Bundesverfassungsgerichtsentscheidungen*/BVerfGE) 47, 253 (273); 83, 60 (73); 93, 37 (68); 107, 59 (94).
[191] *Augsberg*, Rechtsetzung zwischen Staat und Gesellschaft, 2003, p. 84.
[192] *Augsberg*, Rechtsetzung zwischen Staat und Gesellschaft, 2003, p. 85.
[193] In particular, the consultation of the municipalities involved and the approval of the Bundestag contribute to this. Both in the initial draft of the Ministry and in the participation pursuant to sec. 51 Federal Immission Control Act (*Bundes-Immissionsschutzgese*tz/BImSchG), private, expert bodies are involved to a large extent (namely a

Air and Technical Instructions Noise do not only legally bind the administration.[194] They are also, to a certain extent, binding in court proceedings (*begrenzte Außenwirkung* – limited binding effect extending beyond the administration's sphere).[195]

Similar to these forms involving private actors, an expert commission composed of legal, technical, ethical and economic experts could submit proposals to the delegated legislator regarding the sectors and forms of applications which should be exempted from the general law for *algorithm-based processes*. Such proposals presented by an expert committee as preparation of delegated acts, could then be passed on from the legislator to the executive to be used as procedural templates.

The legislator may thus draw on both approaches – delegated administrative regulation specifying the law and static reference to rules and regulations of private institutions – in order to define specific thresholds or criteria for the applicability of the regulatory instruments regarding algorithm-based processes. For example, the legislator could leave (within the limits of essential-matters doctrine/*Wesentlichkeitslehre*)[196] regulatory instruments open to specification. On that basis, the legislator could authorise the executive branch – in collaboration with all relevant stakeholders – to develop criteria for determining under which conditions specific regulatory tools should be applicable or suspended. This approach would facilitate specification of an abstract, broadly defined set of rules through statutory instruments and detailed administrative regulations.

2. EU legal framework for the specification of provisions

The legal instrument of specification through the executive branch is not restricted to domestic law but also common in European Union law.

"circle of representatives of science, the affected parties, the industry involved, the transport system involved […]").

[194] Initially, they were considered anticipated expert opinions; Decisions of the Federal Administrative Court (*Bundesverwaltungsgerichtsentscheidungen*/BVerwGE) 55, 250 (256 ff.).

[195] Cf. Decisions of the Federal Administrative Court (*Bundesverwaltungsgerichtsentscheidungen*/BVerwGE) 72, 300 (320 f.); 129, 209 (212, marginal no. 12).

[196] The essential decisions concerning the exercise of individual fundamental rights must always remain with the parliament; the legislator may not delegate them. Cf. e. g. Decisions of the Federal Constitutional Court (*Bundesverfassungsgerichtsentscheidungen*/BVerfGE) 47, 46 (55).

a) Delegated acts of the Commission

The Treaty on the Functioning of the European Union (TFEU) allows the Union legislator to confer power to the Commission. For this purpose, it includes the instrument of delegated acts (Art. 290 (1) subpara. 1 s. 1 TFEU). In case that the Commission is authorised by a Union legal act to apply this instrument, the Commission can use it to supplement and (formally) amend the underlying act.[197]

With regard to the power to amend, delegated acts are in their function similar to delegated regulations under German law within the meaning of Art. 80 German Constitution (*Grundgesetz*/GG). They ensure the enforceability of general secondary legislation (regulations and directives) at Member State and Union level.[198]

In the area of algorithmic trading in financial instruments, the EU has already drawn on instruments of specification by the executive branch. Three delegated acts of the Commission[199] specify the scope of application[200] and the required thresholds[201] as well as the individual operational obligations[202] for algorithmic trading in financial instruments.

Delegated acts may not supplement or amend *relevant parts* of legislative acts within the meaning of Art. 289 (3) TFEU. A delegated act must expressly define the objectives, content, scope and duration of the delegation of power to the Commission.[203] This so-called essential-matters doctrine is designed to prevent the Commission from taking charge, thus violating the institutional order by providing key aspects of a regulation (Art. 290 (1) subpara. 2 s. 2 TFEU). Similar to the ratio behind Art. 80 (1) GG, this restriction aims at safeguarding the legislative

[197] *Weiß*, EuR 2016, 631 (642 f.).
[198] Besides this, EU primary law knows the instrument of the implementing act (Art. 291 (2) TFEU). It is basically in the hands of the Commission (exceptionally the Council) to adopt such an instrument. The legal regime for state aid, for example, provides for such a specific procedure: On the basis of Art. 109 TFEU, the Council can issue implementing regulations. It makes use of this in the so-called block exemption regulation. It specifies the conditions under which individual support measures in the individual sectors are subject to the assistance-law obligation regime. The block exemption regulations in antitrust law under Art. 101 (3) TFEU, which also apply in German antitrust law by virtue of sec. 2 (2) Act against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen*/GWB), are similar.
[199] Delegated Regulation (EU) 2017/589 of 19/7/2016, OJ No. L 87 of 31/3/2017, p. 417; Delegated Regulation (EU) 2017/565 of 25/4/2016, OJ No. L 87 of 31/3/2017, p. 1; Delegated Regulation (EU) 2017/588 of 14/7/2016, OJ No. L 87 of 31/3/2017, p. 411.
[200] Art. 18 Delegated Regulation (EU) 2017/565.
[201] Art. 2 Delegated Regulation (EU) 2017/588.
[202] Delegated Regulation 2017/589.
[203] See also Art. 290 (1) subpara. 2 s. 1 TFEU.

process against the threat of excessive delegation of legislative power – and with that formative power – to the executive branch. In contrast to the essential-matters doctrine in German constitutional law, essential character is implied by decisive influence in the respective political arena ("aspects of an arena")[204] and not by the exercise of fundamental rights[205].

In the recent past the *EU* legislator delegates more and more some of its powers to other institutions established under secondary law serving the purpose of pooling expertise.[206] It thus outsources decisions to expert bodies, which then have decisive influence on the Commission's decision-making or even act similar to legislators themselves. The European administrative network includes *agencies* (e. g. the European Environment Agency[207], the European Trademark Office[208], the European Defense Agency[209]) or the three European *Supervisory Authorities* (the Banking Authority [EBA][210], the Securities and Markets Authority [ESMA][211] and the Insurance Supervisory Authority [EIOPA]).[212] The ECJ has held the abstract possibility of delegating tasks to agencies admissible.[213] Particularly in the area of securities supervision, the delegation of quasi-legislative powers is continuously evolving: Art. 28 Regulation (EU) No. 236/2012[214] for example grants ESMA discretionary powers to regulate so-called short sales.

---

[204] "The essential provisions are those which implement the fundamental orientations of Community policy." ECJ, case no. C-240/90, *Germany/Commission*, ECR 1992, I-5383, ECLI:EU:C:1992:408, marginal no. 37.
[205] See fn. 196 above and Federal Constitutional Court (*Bundesverfassungsgericht*/BVerfG), NJW 1998, p. 2515 (2520): "essential for the realisation of individual fundamental rights".
[206] *Weiß*, EuR 2016, 631 (631).
[207] Constituted by Regulation (EEC) No. 1210/90 of the Council of 7 May 1990 establishing a European Environment Agency and a European Environment Information and Observation network, OJ No. L 120/01 of 11/5/1990. The foundations of environmental policy are now defined in Art. 191 ff. TFEU.
[208] Originally established by Regulation (EC) No. 40/94 of the Council of 20 December 1993 regarding the European Community trademark, OJ No. L 11/1 of 14/1/1994.
[209] Cf. Art. 42 (3) subpara. 2 TFEU.
[210] Constituted by Regulation (EU) No. 1093/2010 of the European Parliament and the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Supervisory Authority), amending the resolution No. 716/2009/EC and repealing the resolution 2009/78/EC of the Commission, OJ No. L 331/12 of 15/10/2010.
[211] Constituted by Regulation (EU) No. 1095/2010 of the European Parliament and the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending the resolution No. 716/2009/EC and repealing the resolution 2009/77/EC of the Commission, OJ No. L 331/84 of 15/12/2010.
[212] Established by Regulation (EU) No. 1094/2010 of the European Parliament and the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending the resolution No. 716/2009/EC and repealing the resolution 2009/79/EC of the Commission, OJ No. L 331/48 of 15/12/2010.
[213] Cf. ECJ, case no. C-270/12, *United Kingdom/Parliament and the Council*, ECLI:EU:C2014:18, marginal no. 79.
[214] Regulation (EU) No. 236/2012 of the European Parliament and the Council of 14 March 2012 regarding short selling and several aspects about Credit Default Swaps.

The ultimate decision authority (e. g. on banning short selling) thus no longer lies with the Commission but with the Agency itself.[215]

b) EU Guidelines

Other than delegated acts, the Union law includes *informal instruments*, in particular guidelines. Guidelines provide programming-like specification in the execution of laws. They are similar to delegated administrative regulations:[216] They facilitate specification by the executive branch as well as cooperative execution of laws and aid executive authorities by providing precise instructions. For example, the Commission uses guidelines to assess whether subsidies are legitimate under state aid law.[217] Within the framework of joint structural fund management, guidelines control the principles and priorities in order to promote equal regional development within the EU (so-called "cohesion policy"). In antitrust, telecommunications and energy regulation, guidelines also fulfil an important specification function by operationalising normative objectives of Union law. For example, guidelines in telecommunications law serve as an instrument to cope with the complex task of market analysis or the assessment regarding whether an actor has significant market power.[218]

Especially in the field of data protection law, the EU has recently been particularly emphasising the programming effect of guidelines. They are one of the most important instruments used by the European Data Protection Board (EDPB).[219] In order to guarantee the consistent interpretation of indeterminate legal terms of the GDPR,[220] it is its task to operationalise the deletion of links based on Art. 17 (2) GDPR, the regulations of Art. 22 (2) GDPR for profiling or the

[215] The ECJ found that the powers conferred on ESMA were sufficiently limited to prevent a feared shift of ultimate responsibility for economic policy decisions too far from the executive to bodies with remote democratic legitimacy. ECJ, case no. C-270/12, *United Kingdom/ Parliament and the Council*, ECLI:EU:C2014:18, marginal no. 41 ff., in particular marginal no. 48 and 53.
[216] See p. **Fehler! Textmarke nicht definiert.** with fn. 195.
[217] See e. g. from the jurisdiction of the ECJ: ECJ, case no. C-526/14, *Kotnik among others*, ECLI:EU:C:2016:570, marginal no. 69 and ECJ, case no. C-189/02 P, *Dansk mortar industry*, ECR 2005, I-5425, marginal no. 209 ff.
[218] Art. 15 (2) Framework Directive, Directive 2002/21/EC of the European Parliament and the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services, OJ No. EC 2002, L 108, p. 33 ff., modified by Art. 1 Amending Directive 2009/140/EC of 25/11/2009 (OJ No. EC L 337, p. 37), sec. 11 (3) s. 1 Telecommunications Act (*Telekommunikationsgesetz*/TKG); see also *Britz*, EuR 2006, 46 (46 ff.).
[219] Cf. Art. 70 (1) s. 2 lit. d-j, k and m GDPR. Besides, it also has in particular the competence to act legally by resolution - but only on a case-by-case basis, Art. 65 (1) GDPR.
[220] See Art. 70 (1) s. 1 GDPR.

transfer of personal data to third countries for the administrative execution with the help of guidelines.[221]

The guideline as an instrument can pro futuro also assume an important specification function regarding the numerous indeterminate legal terms used in the risk assessment and mitigation of algorithm-based procedures and, on this basis, devise a suitable risk threshold concept for the GDPR in synergy with delegated legal acts.

III. Summary: basic structure of a normative risk threshold system for algorithm-based processes

In order to specify appropriate regulatory thresholds, the legislator has to answer the question to which extent a software application threatens to impair the fundamental rights and therefore triggers a need for regulation. Based on an assessment of whether and to what extent the system affects fundamental rights, a regulatory system should differentiate levels of sensitivity allowing data controllers and supervisory authorities to identify the regulatory level of a specific or typified application.

The likelier and more intensive life and limb are affected (e. g. in the control software of a piloted vehicle or a nursing care robot), the more probable it is that there will be a justification for a strong interference on the occupational freedom and freedom of ownership of a software provider – e. g. via market permits by authorities.[222] Vice versa, the more a regulatory measure restricts the freedom of providers and operators, the bigger the need for legitimacy and for a high level of protection achieved by these measures.

A systematic approach to assigning software applications to special risk classes could be set up in three stages: In *a first step*, the legislator excludes those applications from its regulations in a negative list, that do not require special supervision,[223] and defines abstract risk classes that require abstract regulation and are subject to special, tiered supervision.

[221] See Art. 70 (1) s. 2 lit. d, f, j GDPR.
[222] In this respect, pharmaceutical law could basically be the blueprint, cf. sec. 21 Medicines Act (*Arzneimittelgesetz*/AMG).
[223] In pharmaceutical law, for example, homeopathic and traditional herbal medicinal products do not require market authorisation; their manufacturers only have to register them with the state, cf. sec. 38, 39a Medicines Act (*Arzneimittelgesetz*/AMG).

In a *second step*, a government agency determines the prognostic risk for typified basic applications (such as data mining or scoring), for example via delegated act.[224] The instrument of impact assessment, which the GDPR already includes, may play an important role in the adjusting process: it is predestined to provide a procedural sensorium in order to classify the degree of risk posed by an application using risk classes. The EU legislator could and should further develop this instrument to this purpose and link it to a tiered regime of obligations of varying intensity. In case a matter touches on fundamental rights but only to a marginal extent, the obligation to publish a comprehensive impact assessment for a specific product or algorithm-based procedure and thus subjecting to public control may be dispensed. In this case, for example, keeping records or an interface for official access could also be dispensable.

In a *third step*, a broader classification of risk classes can be fine tuned: with the help of organisational, technical and legal measures, the data controller can reduce the software application's sensitivity to fundamental rights. As far as the accompanying risk reduction steps considerably reduce the relevance of fundamental rights, an application could then be privileged. This should in particular be the case where the operator itself takes adequate measures to minimise risks.[225]

Instruments that reduce a "high" sensitivity to fundamental rights to a "normal" sensitivity include in particular actual and verifiable anonymisation or pseudonymisation[226] of large parts of data processing, synthetic data instead of people-related data,[227] so-called strong encryption for specific data packages and, complete or partial abstaining from data within the meaning of Art. 9 (1) and Art. 10 GDPR or measures of differential privacy.[228]

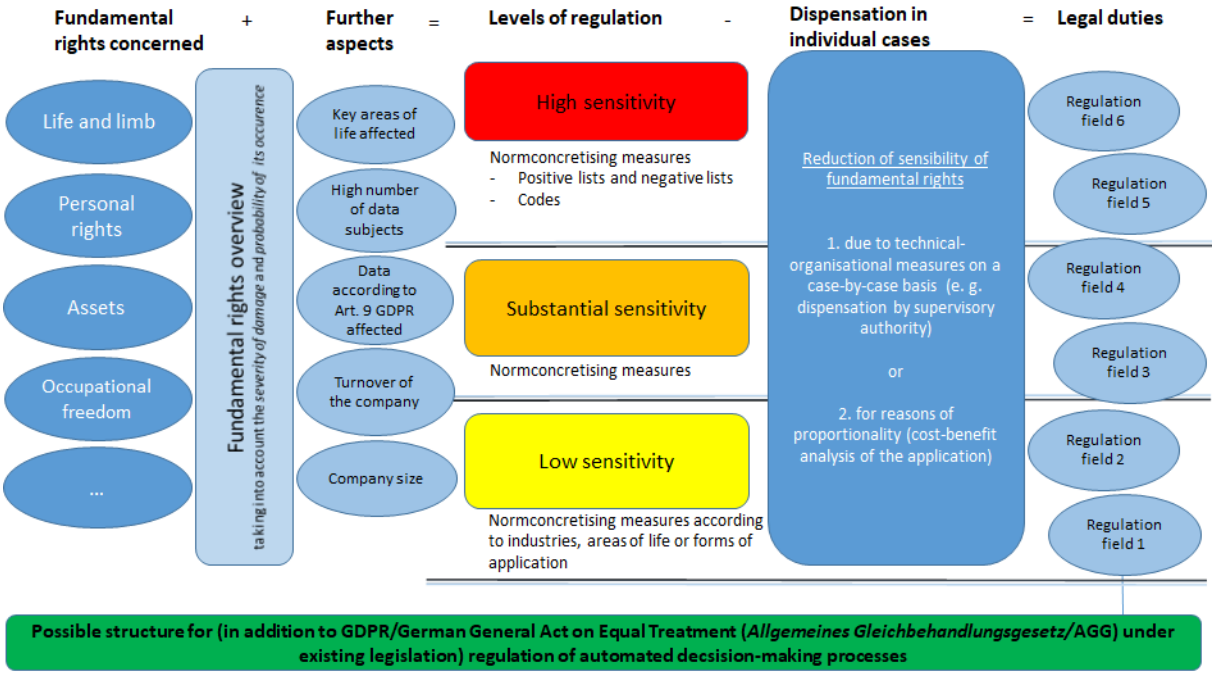
Voluntary transparency measures can also reduce the sensitivity to fundamental rights. In addition to the publication of (anonymised) comparison groups, regular, non-mandatory inspections of the data basis relevant to the algorithmic decision-making process (especially with

[224] A differentiation could be made between "high", "significant" and "low" sensitivity.
[225] In order to classify proven methods of *privacy by design* (Art. 25 (2) GDPR) and to make them fruitful for the evaluation of a large number of software applications, the legislator could resort to instruments of delegated legal power or provide for static references to private norms.
[226] Cf. Art. 25 (1) GDPR, which emphasises the pseudonymisation exemplarily as technical-organisational measure for the implementation of the data protection principles. Cf. *Hartung*, in: Kühling/Buchner (ed.), DS-GVO/BDSG, 2nd ed., 2018, Art. 25 GDPR, marginal no. 16.
[227] Cf. e. g., *Drechsler/Jentzsch*, Synthetische Daten, 2018, p. 5 ff.
[228] *Martini*, Blackbox Algorithmus, 2019, p. 243.

regard to possible discrimination), are also possible. Results of the inspections could also be subject to publication obligations.

The burden of proof regarding the applicability of a privilege – according to the basic idea of accountability set forth in Art. 5 (2) GDPR – should lie with the controller and be verifiable by the supervisory authority. This creates an incentive – in accordance with Art. 25 (2) GDPR – to commit software solutions to the protection of privacy from the beginning. Compliance would be awarded with a reduced intensity of supervision.[229] To this purpose, the supervisory authority issues a declaratory dispense ensuring that the downgrading to a lower sensitivity level becomes effective.

The classification into the different levels of sensitivity is then tied to different levels of obligations: in case of a "high sensitivity to fundamental rights", the legislator may, for example, impose an obligation to undergo a certification procedure or an external audit, to continuously grant a supervisory authority or the technical service unit[230] monitoring access to the software environment and to implement an obligation to state reasons.



[229] In order to stop circumvention strategies, however, there must be at the same time significant sanctions for companies that intentionally or grossly negligently underestimate the level of risk. As Art. 24 (3) and Art. 40 f. GDPR paradigmatically show, it is not alien to the data protection law that controllers make adequate self-assessments and are "rewarded" for it; Art. 24 GDPR is, however, a general standard whose concrete canon of duties the Union legislator has not yet clearly specified, cf. *Hartung*, in: Kühling/Buchner (ed.), DS-GVO/BDSG, 2nd ed., 2018, Art. 24 GDPR, marginal no. 24.

[230] Cf. p. 26 f. above.

Figure 1: Strongly simplified basic framework of a regulatory concept for algorithm-based decision-making processes. (Source: Michael Kolain)

D. Regulatory competence: implementation of regulatory proposals in a multi-tiered system – Summary

The Union legislator has already set some cornerstones for regulating algorithm-based applications in data protection law. However, the GDPR is merely the shell of a building yet to be raised. In particular with regard to algorithmic *assistance* in human decisions ("partial automation"), the GDPR exposes an architectural void.

The German legislator cannot easily fill the large gaps on its own. This is a consequence of the GDPR's primacy over national regulations regarding all matters in its scope of application – e. g. processing and free circulation of personal data (Art. 1 (1) GDPR): it serves the aim of fully harmonising data protection law throughout the Union. The Member States may therefore only define supplementary regulations to the extent that the GDPR explicitly allows in its (numerous) opening clauses (cf. in particular recital 8 GDPR).[231]

The regulatory fields of anti-discrimination law[232] as well as parts of competition law and fair trading law[233] have already been sustainably reformed under Union law. The national legislator is therefore significantly limited in its scope of action in many reform efforts of consumer-protection.[234]

At the same time, the regulation of algorithm-based procedures at *the level of Union law* adheres to an appropriate legal policy concept: in a globalised digital cosmos, national borders are losing their significance; under these conditions only EU-wide regulations are capable of setting effective standards. Although, the German level of data protection regulation is traditionally high and carefully elaborated, both in global and European comparison. What at first glance may appear to be an expression of German scepticism regarding technology is not least the product of the historical experience of two totalitarian regimes. It is to date still reflected

[231] See *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, p. 3 ff.
[232] Cf. in particular Directive 2000/43/EC, 2000/78/EC, 2004/113/EC and 2006/54/EC.
[233] Cf. Art. 101 ff. TFEU on competition law and the legal acts enacted on the basis of Art. 103 (1) TFEU; on fair trading law, cf. Directive 2005/29/EC, which has been attributed a fully harmonising character to by the ECJ, ECJ (Plus Warenhandelsgesellschaft), judgment of 14/1/2010, ECLI:EU:C:2010:12, marginal no. 41.
[234] Cf. on data protection law, *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, p. 4 ff.

in a particular sensitivity regarding questions of informational self-determination, which many Germans share.

As much as the desire to set standards leading by good example instead of waiting for an EU-wide agreement is understandable: new national regulations in Germany could initiate *forum shopping*[235] within the European Union. Member State's regulatory approaches regarding algorithmic procedures often lead to companies in the digital economy preferably settling in Member States allowing for more "digital freedom" and a lower level of data protection. As a result, consumers' chances of effectively enforcing high standards of protection are compromised if member states build their own regulatory castles.

I. Transparency obligations

1. Labelling obligations ("if") and content-related information obligations ("how")

As a regulatory component of an EU-wide normative structure for algorithm-based processes, transparency requirements and mechanisms of legal content control can counteract the information asymmetry that is characteristic for the application of algorithms in software.[236] Users of digital services, communication tools and platforms which owe their economic driving force to complex algorithms often lack a comprehensive overview, let alone control measures regarding whether their data is processed in a way consistent to their right to privacy. The typical consumer for example does not know if a company is combining individual data to form a personality profile, processing data in simulations using artificial intelligence or if – in breach of data protection regulations – data is passed on to third parties without authorisation.

[235] *Forum shopping* here means the systematic exploitation by companies of parallel jurisdictions to obtain certain legal or factual advantages, cf. for example *Schack*, Internationales Zivilverfahrensrecht, 7th ed., 2017, p. 97.
[236] See p. 8 ff. above.

Who possesses the legislative competence to extend transparency obligations – for instance labelling, content-related information or justification of decisions[237] – to algorithm-based processes (also beyond the scope of Art. 22 GDPR)[238] is primarily determined by Union law, specifically in Art. 12 ff. GDPR in conjunction with Art. 1 (2) s. 2, Art. 16 (2) TFEU, Art. 4 (3) s. 3 TEU. The regulations in Art. 13 (2) lit. f respectively Art. 14 (2) lit. g GDPR, Art. 15 (1) lit. h, Art. 22 GDPR establish an exhaustive framework of legal protection for the sub-area of fully automated decisions.

If these information obligations were to apply in principle not only to fully automated procedures but also to other algorithm-based procedures sensitive to fundamental rights, the EU legislator is faced with the challenge of accurately specifying the extended *circle of addressees* of the information obligations (on which a fine may be imposed). Otherwise he could overstretch the bureaucratic costs associated with information obligations on the one hand and create legal uncertainty on the other. In this respect, especially a "traffic light grid" is conceivable to grade the extended information obligations according to the degree of sensitivity inherent to the applications. The Union legislator could define in an annex to Art. 12 ff. GDPR positive and negative lists specifying which applications are subject to the information obligations and which are exempt from them.

If the *national legislator* wishes to deviate from the level of data protection provided for data subjects in Art. 12 ff. GDPR, Art. 23 GDPR enables it to do so within a certain scope.[239] However, Member States' regulatory powers are linked not only to high legal prerequisites. They are furthermore confined to *reducing* the level of protection. The Member States are, based on the wording of Art. 23 (1) GDPR ("are restricted"), not allowed to establish new obligations

[237] The legislator could shape this as a "right to explanation of the decision and explanation of the decision-making process" and orient its scope in particular to sec. 39 Administrative Procedure Act (*Verwaltungsverfahrensgesetz*/VwVfg). Consumers could then not only - as in the current version of Art. 13 - 15 GDPR - understand the scope and logic of the algorithmic procedure, but could also better understand the decision itself and, if necessary, seek effective legal protection.

[238] See p. 8 ff. above.

[239] A lowering deviation must ensure in particular an overriding protection goal, such as public safety (Art. 23 (1) GDPR), respect the essence of individual fundamental rights and be proportionate overall. The catalog of Art. 23 (1) GDPR is exhaustive. Cf. also *Bäcker*, in: Kühling/Buchner (ed.), DS-GVO/BDSG, 2nd ed., 2018, Art. 23 GDPR, marginal no. 11 ff.

exceeding the scope of Art. 12 ff. GDPR. Any supplementary regulation expanding existing information obligations under data protection law would need to be adopted at EU level.[240]

2. Obligation to publish a *comprehensive* impact assessment

Similar to information obligations, the national legislator does not have the freedom to impose legal obligations on its own to carry out and publish a new comprehensive data protection impact assessment[241] going beyond assessing the impact of data processing on personal rights. Art. 35 GDPR has in this regard a limiting effect restricting Member State's competences.

However, national legislatives may impose obligations to prepare impact assessments for consequences *outside* data protection law in the form of sectoral impact assessments. In order to extend the scope and content of the impact assessment to a *general technology assessment*, the Union legislator can in particular not rely on its competence to adopt secondary regulation. Otherwise the EU would overstretch the original scope of data protection law. Art. 16 (2) TFEU, at least when read narrowly, does not suffice as a basis of competence for this purpose. However, a general technology assessment as an extension of the data protection impact assessment can be based on the final programme of Art. 114 s. 2 and Art. 115 TFEU, namely the regulatory competence for the approximation of laws in the internal market. The coexistence of a Union-wide data protection impact assessment and a supplementary national impact assessment for non-data protection-specific consequences would be misguided in terms of regulatory policy, also regarding the effort a second impact assessment would entail.

The Union legislator should implement an obligation to *publish* the data protection impact assessment by means of a new Art. 35 (1) s. 2a GDPR ("*data controllers operating with sensitive software applications are obliged to publish the essential contents and results of the impact assessment on their homepage and to update them with each new impact assessment*").

[240] The same applies to the proposal to impose an obligation on news aggregator services to provide insight into their technical news selection and prioritisation process. See *Martini*, JZ 2017, 1017 (1021).
[241] See p. 16 f. above.

II. Content control

1. Instruments

The Member States do not posses the competence to independently incorporate (new) aspects of content control of algorithm-based applications[242] into data protection law under the regime of the GDPR: Instead, the regulatory power predominantly lies in Brussels. Only the Union legislator can, for instance, enforce the proposal to oblige the operators of algorithm-based procedures to integrate a risk management system into their data processing by a respective provision. Risk management is an instrument intrinsic to compliance in data protection law that directly controls data processing (for which the GDPR has pursuant to Art. 16 TFEU primacy under Union law).

The EU is in particular well-advised to include the ratio behind recital 71 subpara. 2 GDPR for algorithm-based procedures (especially profiling) into its decreeing parts (preferably in Art. 25 (1) GDPR or in a new Art. 22a GDPR) – not only as far as they are part of fully automated procedures in the sense of Art. 22 GDPR, but also for other sensitive algorithm-based procedures which the legislator will define. The controller would then be directly obligated under sanction to establish "suitable mathematical or statistical procedures" and to continuously monitor their methods and data basis in order to minimise failure.

However, the national legislator still holds regulatory power regarding the adaptation of anti-discrimination provisions in the *General Equal Treatment Act (Allgemeines Gleichbehandlungsgesetz/*AGG). He can of his own regulatory power address unequal treatment arising from algorithmic decision-making. The anti-discrimination law is also subject to overriding directives under EU law, although these do not impose full harmonisation but rather leave Member States legislative flexibility. The GDPR also sets single anti-discriminatory limits (Art. 22 (2), (3) and (4), Art. 9 (1) GDPR). Nevertheless, the competences of EU data protection laws (Art. 16 (2) TFEU), in principle, only extend to regulation concerning the data *processing* as such but not to the processing *result* (i. e. the content of an algorithmic decision).

[242] See p. 18 ff. above.

In all other areas of a regulatory system for algorithm-based processes, national legislation is constrained and has only limited flexibility: The GDPR specifies, for instance, the *data controllers' procedural obligations* (cooperation, information and documentation obligations etc.)[243] in a *conclusive* manner (Art. 30, 31 GDPR). The accountability obligation created by Art. 5 (2) GDPR is substantiated based on the EU's own regulatory powers (cf. Art. 28 (3) s. 2 lit. a, Art. 30 (1) and (2), Art. 33 (5) s. 1, Art. 49 (6) GDPR). National legislatives may also not introduce preventive permits for data processing systems,[244] as such a method of market admission potentially undermines the EU's intent to harmonise the requirements regarding the processing of personal data across the EU: in Art. 6 GDPR, the European Union has given substance to this intention (exempting the public sector – Art. 6 (1) subpara. 1 lit. e and lit. c GDPR) exhaustively.

However, the Member States may enact their own laws in areas in which they do *n*ot establish specific obligations of data protection law, but aim to protect *other legal interests*, especially health, freedom of expression, protection of the democratic order or the design of labour relations (cf. especially Art. 85 (2), Art. 88 GDPR). The Member States may therefore, in particular, establish a procedure of *market approval for software applications in the health sector* under their own law in order to protect the life and health of patients. The same applies, for example, to product approval obligations for care robots or highly automated driving (for example within the framework of the German Road Traffic Act).

2. Regulatory thresholds

The threshold at which parts of a regulatory system for algorithm-based processes are applicable is one of the most sensitive aspects in algorithm legislation. Regulatory efforts to properly confine (machine learning) software applications have to be highly detailed as well as balanced in order to provide legal certainty and proportionality. Algorithm-based processes should not be defined solely based on general and quantitative aspects (such as the number of potentially affected data subjects or the probability of damage) as these do not reflect the

[243] See p. 9 ff. above.
[244] See p. 18.

diversity of algorithm-based processes on the market. This issue rather demands sector-specific solutions as well as a comprehensive (and also qualitative) assessment, including exceptions and exemptions.[245]

A regulatory system for software applications should initially address the sensitivity to fundamental rights and the market relevance of each case of algorithm-based procedure. The legislator defines abstract risk classes that require abstract regulation and are subject to special, tiered supervision. A law enforcement agency compares the abstract risk of a software application with concrete application scenarios. The predicted risk associated with the underlying application (for example scoring in central domains of life) is part of an evolved impact assessment (with applications being rated as having high, substantial or low fundamental rights sensitivity). Finally, technical, organisational and legal measures a provider has taken could be considered in order to reduce the sensitivity to fundamental rights on a case-by-case basis.[246] Based on this categorisation, the legal system could define which regulatory instruments do or do not apply to a specific software application.

3. Institutional design

The regulation of algorithm-based procedures must be aimed at not only demanding but consistently *enforcing* regulatory requirements. For governmental supervision to be able to keep pace in the race between technical development and its control by virtue of adequate equipment and personnel competence, it is thus necessary to have a suitable institutional and organisational framework. From a legal policy perspective, it is not very promising to establish a separate supervisory authority for this purpose in the future[247] as the regulation of algorithm-based processes is a highly complex, interdisciplinary task that a uniform regulatory umbrella cannot fulfil. The regulatory field is closely related to data protection law on one hand and anti-discrimination and competition law on the other hand. Given this background, a new authority cannot be established without restricting the tasks performed by existing specialist authorities at the same time.

The Member States are responsible for the design of their specialised supervisory structures in general. But the European Union has defined a number of requirements for the institutional

[245] See p. 51 ff. above.
[246] See p. 51 ff. above.
[247] See p. 29 ff. above.

design of data protection supervision in Art. 51 ff. GDPR. This includes, in particular, the obligation to maintain and fund data protection supervisory authorities as separate, independent supervisory bodies (Art. 52 ff. GDPR).

It is, however, possible and useful to the German federal legislator to establish a state *support unit* to assist the various existing federal and state supervisory with customised expertise.[248] This would result in a national centre of competence that is able to contribute its scientific expertise to the multi-faceted supervisory and legal structures in a targeted manner. Its services could, for example, include establishment of public standards or the training and structured guidance of interdisciplinary testing teams. The legislaor could additionally extend the new body's reach by providing it with institutional elements of a market and product monitoring body.[249] Another conceivable option (but only recommendable to a limited extent or only in specific sub-areas) is to integrate private institutions in supervisory tasks as administrative support (*Verwaltungshelfer*) or by way of delegation (*Beleihung*).[250]

III. Liability and legal protection

Strict liability in particularly sensitive areas (for example digitalised medical applications or nursing care robots),[251] authority to inspect for competitors,[252] associations' rights to bring representative action[253] or "ancillary consequences competence" for civil law courts[254] do not regulate typical data protection law: They are not directly linked to the "protection of natural persons with regard to the *processing* of personal data" (cf. Art. 1 (1) GDPR). The GDPR consequently does generally not create limitations for national legislature[255] in terms of legislative competence. Art. 80 GDPR explicitly requires member states to normatively grant consumer

[248] See p. 31 above. This would be possible already at the current time, in particular without adaptations of the GDPR.
[249] Similar supervisory structures exist, for example, for pharmaceuticals, high-frequency trading or motor vehicles.
[250] See p. 32 ff. above.
[251] See p. 36 above.
[252] See p. 36 above.
[253] See p. 37 f. above.
[254] See *Martini*, JZ 2017, 1017 (1024 f.).
[255] In this respect, the Federal Supreme Court recognises considerable legal uncertainty. In the preliminary ruling procedure, it asked the ECJ whether the provisions of Art. 22 to 24 Directive 95/46/EC (Data Protection Directive) oppose a national provision which – like sec. 8 (3) No. 3 Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*/UWG) – grants non-profit associations the right to take action against the infringer in the event of an infringement of data protection provisions in order to safeguard the interests of consumers. Federal Supreme Court (*Bundesgerichtshof*/BGH), Res. of 11/4/2009 – I ZR 186/17.

associations and mediation boards a separate right to bring representative action.[256] The regulatory proposals regarding liability and legal protection[257] are therefore, in principle, open to implementation by the Member States.

IV. Self-regulation

Union data protection law expressly welcomes national initiatives for strengthening self-regulation instruments (Art. 40 (1) GDPR; cf. also Art. 35 (8) and Art. 24 (3) GDPR). At the same time, it sets a formal framework within which the Member States can create the relevant instruments of self-regulation. In its current form, the GDPR does not provide for a "comply or explain" approach[258] to self-regulation. The national legislator is therefore barred from introducing an "Algorithmic Responsibility Code" based on the model of the Corporate Governance Code (underpinned by sanctions) beyond the forms of self-regulation established by the GDPR.[259] Audit systems[260] creating incentives for data controllers to continually improve the level of protection provided by their data processing operations are also reserved to the EU level by means of Art. 42 GDPR.

V. Table with regulatory proposals for exemplary applications

The various categories of a regulatory system can be illustrated in a *strongly simplified manner* by tabularly applying them to typical application scenarios. These classifications are provisional basic values that can vary depending on the design, degree of processing and concrete use case of the application. The table outlines a methodological approach rather than a comprehensive concept of risk classification.

[256] *Martini*, JZ 2017, 1017 (1024 f.).
[257] In detail see p. 35 ff. above and *Martini*, JZ 2017, 1017 (1023 f.).
[258] See above p. 38 ff.
[259] See p. 38 f. above.
[260] See p. 38 f. above.

	Smart-home applications (e. g.domestic robots)	Preferential entertainment software (e. g. *Facebook* homepage, Netflix suggestions)	Individual pricing	Rating portals (e. g. ratings of doctors, service providers, teachers)	Speech-based assistants (e. g. Alexa)	Facial recognition software	Applicant selection (employment and training)	Government AI applications	Medical applications (e. g. image interpretation for tumour detection)	Nursing care robots	Autonomous vehicles
Obligatory labelling	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Obligatory information on the system logic	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Obligatory justification	–	–	✓	–	–	–	✓	✓	✓	✓	–
Impact assessment	✓	–	–	–	✓	✓	✓	✓	✓	✓	✓
Ex-ante permit(in general)	–	–	–	–	–	✓	–	✓	✓	✓	✓
Extended anti-discrimination protection	–	✓	✓	–	✓	✓	✓	✓	✓	✓	✓
Audit algorithms	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Official access and inspection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

rights, co-operation obligations											
Risk management, in particular appointment of a responsible officer	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
Easier burden of proof	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
(Fundamental) documentation obligation	–	Poss. ✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Strict liability	–	–	–	–	–	–	–	–	✓	✓	✓
Competitors' powers to issue written cautions	✓	✓	✓	✓	✓	✓	✓	–	✓	✓	✓
Consumer protection associations' right to bring representative action	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Obligatory "Algorithmic Responsibility Codex"statement	–	✓	✓	✓	✓	✓	✓	Poss. ✓	✓	✓	✓

E. List of References

ACM US Public Policy Council/ACM Europe Council, Statement on Algorithmic Transparency and Accountability, http://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf (25/10/2018).

Anonymous, EU prüft Übernahme von WhatsApp, Focus Online of 14/7/2014.

– LfDI Rheinland-Pfalz: Macht der Algorithmen – Macht ohne Kontrolle?, ZD-Aktuell, 2015, 04675.

Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP 248, Brussels, 4/10/2017.

Augsberg, Steffen, Rechtsetzung zwischen Staat und Gesellschaft, Möglichkeiten differenzierter Steuerung des Kapitalmarktes, Berlin, 2003.

Bauer, Jobst-Hubertus/*Krieger*, Steffen, 10 Jahre AGG – Tops und Flops, NZA 2016, p. 1041–1046.

Beck, Susanne, Grundlegende Fragen zum rechtlichen Umgang mit der Robotik, JR 2009, p. 225–230.

Beck, Susanne (ed.), Jenseits von Mensch und Maschine, Ethische und rechtliche Fragen zum Umgang mit Robotern, Künstlicher Intelligenz und Cyborgs, Baden-Baden, 2012.

Becker, Florian, Kooperative und konsensuale Strukturen in der Normsetzung, Tübingen, 2005.

Bernhardt, Wolfgang, Sechs Jahre Deutscher Corporate Governance Kodex - Eine Erfolgsgeschichte?, BB 2008, p. 1686–1692.

Böhning, Björn, Datenschutz – Die Debatte muss geführt werden, ZD 2013, p. 421–422.

Brand, Christian/*Rahimi-Azar*, Shahin, „AGG-Hopping" – eine Einnahmequelle mit strafrechtlichen Risiken, NJW 2015, p. 2993–2997.

Britz, Gabriele, Vom Europäischen Verwaltungsverbund zum Regulierungsverbund? – Europäische Verwaltungsentwicklung am Beispiel der Netzzugangsregulierung bei Telekommunikation, Energie und Bahn, EuR 2006, p. 46–77.

Busch, Christoph, Algorithmic Accountability, Osnabrück, 2018.

Citron, Danielle Keats/*Pasquale*, Frank, The Scored Society: Due Process for Automated Predictions, Washington Law Review 89 (2014), p. 1–33.

Coglianese, Cary/*Lehr*, David, Regulating by Robot, Administrative Decision Making in the Machine-Learning Era, Georgetown Law Journal 105 (2017), p. 1147–1223.

Council of Experts on Consumer issues at the German Federal Ministry of Justice and Consumer Protection, Verbraucherrecht 2.0, Verbraucher in der digitalen Welt, Berlin, Dec. 2016.

Diakopoulos, Nicholas/*Friedler*, Sorelle A./*Arenas*, Marcelo/*Barocas*, Solon, et al., Principles for Accountable Algorithms and a Social Impact Statement for Algorithms, https://www.fatml.org/resources/principles-for-accountable-algorithms (25/10/2018).

Domurath, Irina/*Neubeck*, Irene, Verbraucher-Scoring aus Sicht des Datenschutzrechts, Working Paper, Berlin, October 2018.

Drechsler, Jörg/*Jentzsch*, Nicola, Synthetische Daten, Innovationspotential und gesellschaftliche Herausforderungen, Berlin, 2018.

Edwards, Lilian/*Veale*, Michael, Slave to the algorithm?, Why a 'right to explanation' is probably not the remedy you are looking for, Duke Law & Technology Review 16 (2017), p. 18–84.

Ehmann, Eugen/*Selmayr*, Martin (ed.), Datenschutz-Grundverordnung, Kommentar, 2nd ed., Munich, 2018.

Ernst, Christian, Algorithmische Entscheidungsfindung und personenbezogene Daten, JZ 2017, p. 1026–1036.

Fanta, Alexander, Österreichs Jobcenter richten künftig mit Hilfe von Software über Arbeitslose, netzpolitik.org of 13/10/2018.

Federal Cartel Office, Joint Guidelines on the new transaction value thresholds for merger control rules in Germany and Austria – public consultation, press release of 14/5/2018, Bonn.

Floridi, Luciano/*Cowls*, Josh/*Beltrametti*, Monica/*Chatila*, Raja, et al., AI4People - An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, Minds & Machines 28 (2018), p. 689–707.

Franck, Lorenz, Das System der Betroffenenrechte nach der Datenschutz-Grundverordnung (DS-GVO), RDV 2016, p. 111–119.

Future of Life Institute, Asilomar AI Principles, https://futureoflife.org/ai-principles (25/10/2018).

Gasser, Tom Michael, Fundamental and Special Legal Questions for Autonomous Vehicles, in: Maurer, Markus/Gerdes, J. Christian/Lenz, Barbara et al. (ed.), Autonomous Driving: Technical, Legal and Social Aspects, Ladenburg, 2015, p. 523–551.

Gersdorf, Hubertus/*Paal*, Boris P. (ed.), Beck'scher Online-Kommentar Informations- und Medienrecht, 22nd ed. (status: 1/8/2018), Munich, 2018.

Grabitz, Eberhard/*Hilf*, Meinhard/*Nettesheim*, Martin (ed.), Das Recht der Europäischen Union, EUV/AEUV, loose-leaf collection (status: 65th updated information) vol. 1, Munich, 2018.

Härting, Niko/*Schneider*, Jochen, Das Ende des Datenschutzes – es lebe die Privatsphäre, Eine Rückbesinnung auf die Kern-Anliegen des Privatsphärenschutzes, CR 2015, p. 819–827.

Herberger, Maximilian, "Künstliche Intelligenz" und Recht, Ein Orientierungsversuch, NJW 2018, p. 2825–2829.

Hoeren, Thomas/*Niehoff*, Maurice, KI und Datenschutz – Begründungserfordernisse automatisierter Entscheidungen, RW 9 (2018), p. 47–66.

Hoffmann-Riem, Wolfgang, Verhaltenssteuerung durch Algorithmen, Eine Herausforderung für das Recht, AöR 142 (2017), p. 1–42.

Hoffmann-Riem, Wolfgang/*Schmidt-Aßmann*, Eberhard/*Voßkuhle*, Andreas (ed.), Grundlagen des Verwaltungsrechts vol. I, Methoden, Maßstäbe, Aufgaben, Organisation, 2nd ed., Munich, 2012.

Hölters, Wolfgang (ed.), Aktiengesetz, 3rd ed., Munich, 2017.

Jellinek, Georg, Gesetz und Verordnung, Staatsrechtliche Untersuchungen auf rechtsgeschichtlicher und rechtsvergleichender Grundlage, Tübingen, 1919 (1887).

Kastl, Graziana, Algorithmen – Fluch oder Segen?, GRUR 2015, p. 136–141.

Kieck, Annika, Zum Verhältnis von Datenschutz- und Kartellaufsicht, PinG 2017, p. 67–72.

Kiefer, Günther, Die Beleihung, (K)ein unbekanntes Wesen?, NVwZ 2011, p. 1300–1303.

Kloepfer, Michael, Umweltrecht, 4th ed., Munich, 2016.

Kolain, Michael, Data Protection Impact Assessment (Art. 35 GDPR) as a Tool of Privacy Regulation, Issue Paper 18-15-5, Korea Legislation Research Institute, Sejong-si, 2018.

Körber, Torsten, Das Bundeskartellamt auf dem Weg zur Digitalagentur?, WuW 2018, p. 173.

Kühling, Jürgen/*Buchner*, Benedikt (ed.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2nd ed., Munich, 2018.

Kühling, Jürgen/*Martini*, Mario/*Heberlein*, Johanna/*Kühl*, Benjamin, et al., Die DSGVO und das nationale Recht, Erste Überlegungen zum nationalen Regelungsbedarf, Münster, 2016.

Kulartz, Hans-Peter/*Kus*, Alexander/*Portz*, Norbert/*Prieß*, Hans-Joachim (ed.), Kommentar zum GWB-Vergaberecht, 4th ed., Cologne, 2016.

Lepa, Manfred, Verfassungsrechtliche Probleme der Rechtsetzung durch Rechtsverordnung, AöR 105 (1980), p. 337–369.

von Lewinski, Kai/*de Barros Fritz*, Raphael, Arbeitgeberhaftung nach dem AGG infolge des Einsatzes von Algorithmen bei Personalentscheidungen, NZA 2018, p. 620–625.

Ludwig, Kristiana, Mehr Arbeit fürs Kartellamt, Süddeutsche Zeitung Online of 21/11/2016.

Martini, Mario, Normsetzungsdelegation zwischen parlamentarischer Steuerung und legislativer Effizienz – auf dem Weg zu einer dritten Form der Gesetzgebung?, AöR 133 (2008), p. 155–190.

– Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts, JA 2009, p. 839–845.

– Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, p. 1017–1025.

– Blackbox Algorithmus, Grundfragen einer Regulierung Künstlicher Intelligenz, New York et al., 2019.

Martini, Mario/*Botta*, Jonas, Iron Man am Arbeitsplatz? – Exoskelette zwischen Effizienzstreben, Daten- und Gesundheitsschutz, Chancen und Risiken der Verschmelzung von Mensch und Maschine in der Industrie 4.0, NZA 2018, p. 625–637.

Martini, Mario/*Kühl*, Benjamin, Staatliches Informationshandeln, Jura 2014, p. 1221–1236.

Maurer, Markus/*Gerdes*, J. Christian/*Lenz*, Barbara/*Winner*, Hermann (ed.), Autonomes Fahren: Technische, rechtliche und gesellschaftliche Aspekte, Berlin, 2015.

McNamara, Andrew/*Smith*, Justin/*Murphy-Hill*, Emerson, Does ACM's Code of Ethics Change Ethical Decision Making in Software Development?, ESEC/FSE '18, November 4–9, 2018, Lake Buena Vista, FL, USA.

Mittelstadt, Brent Daniel/*Allo*, Patrick/*Taddeo*, Mariarosaria/*Wachter*, Sandra/*Floridi*, Luciano, The ethics of algorithms, Mapping the debate, Big Data & Society 2016, p. 1–21.

Müller-Hengstenberg, Claus D./*Kirn*, Stefan, Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems – Rechtliche Konsequenzen der "Verselbstständigung" technischer Systeme, MMR 2014, p. 307–313.

Nowak, Eric/*Rott*, Roland/*Mahr*, Till, Wer den Kodex nicht einhält, den bestraft der Kapitalmarkt?, Eine empirische Analyse der Selbstregulierung und Kapitalmarktrelevanz des Deutschen Corporate Governance Kodex, ZGR 2005, p. 252–279.

Paal, Boris P./*Pauly*, Daniel A. (ed.), Datenschutz-Grundverordnung - Bundesdatenschutzgesetz, 2nd ed., Munich, 2018.

Pasquale, Frank, The Black Box Society, The Secret Algorithms That Control Money and Information, Cambridge, 2015.

Pluta, Werner, Algorithmus schreibt wissenschaftliches Buch, golem.de of 16/4/2019.

Podszun, Rupprecht/*Schwalbe*, Ulrich, Digitale Plattformen und GWB-Novelle: Überzeugende Regeln für die Internetökonomie?, NZKart 2017, p. 98–106.

Posser, Heinrich/*Wolff*, Heinrich Amadeus (ed.), Beck'scher Online-Kommentar VwGO, 47th ed. (status: 1/10/2018), Munich.

Reichwald, Julian/*Pfisterer*, Dennis, Autonomie und Intelligenz im Internet der Dinge, CR 2016, p. 208–212.

Reisman, Dillon/*Schultz*, Jason/*Crawford*, Kate/*Whittaker*, Meredith, Algorithmic Impact Assessments, A practical framework for public agency accountability, April 2018.

Rohde, Noëlle, Gütekriterien für algorithmische Prozesse, Eine Stärken- und Schwächenanalyse ausgewählter Forderungskataloge, Gütersloh, 2018.

Ruffert, Matthias, Rechtsquellen und Rechtsschichten des Verwaltungsrechts, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (ed.), Grundlagen des Verwaltungsrechts vol. I, Methoden, Maßstäbe, Aufgaben, Organisation, 2nd ed., Munich, 2012, p. 1163–1256.

Saurer, Johannes, Die Mitwirkung des Bundestages an der Verordnungsgebung nach § BIMSCHG § 48b BImSchG, NVwZ 2003, p. 1176–1182.

Schack, Haimo, Internationales Zivilverfahrensrecht, Mit internationalem Insolvenz- und Schiedsverfahrensrecht, 7th ed., Munich, 2017.

Schmid, Alexander, Pflicht zur „integrierten Produktbeobachtung" für automatisierte und vernetzte Systeme, CR 2019, p. 141–147.

Schmidt am Busch, Birgit, Die Beleihung, Ein Rechtsinstitut im Wandel, DÖV 2007, p. 533–542.

Schweighofer, Erich/*Sorge*, Christoph/*Borges*, Georg/*Schäfer*, Christoph, et al., Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, report of the specialist group of Legal Informatics of the Corporation for Informatics (registered association) on behalf of the Council of Experts for Consumer Affairs, Berlin, October 2018.

Schwintowski, Hans-Peter, Wird Recht durch Robotik und künstliche Intelligenz überflüssig?, NJOZ 2018, p. 1601–1609.

Spranger, Tade Matthias/*Wegmann*, Henning, Öffentlich-rechtliche Dimensionen der Robotik, in: Beck, Susanne (ed.), Jenseits von Mensch und Maschine, Ethische und rechtliche Fragen zum Umgang mit Robotern, Künstlicher Intelligenz und Cyborgs, Baden-Baden, 2012, p. 105–118.

Tene, Omer/*Polonetsky*, Jules, Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property 11 (2013), p. 239–273.

Tufekci, Zeynep, Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency, Colorado Technology Law Journal 13 (2015), p. 203–218.

Tutt, Andrew, An FDA for Algorithms, A New Agency, Administrative Law Review 69 (2017), p. 83–123.

Veil, Winfried, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip, Eine erste Bestandsaufnahme, ZD 2015, p. 347–353.

Wachter, Sandra/*Mittelstadt*, Brent, A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI, Columbia Business Law Review 2019, p. 1–84 of the type script.

Wachter, Sandra/*Mittelstadt*, Brent/*Floridi*, Luciano, Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation, International Data Privacy Law 7 (2017), p. 76–99.

Weinzierl, Quirin, Warum das Bundesverfassungsgericht Fußballstadion sagt und Soziale Plattformen trifft, JuWissBlog No. 48/2018 of 24/5/2018.

Weiß, Wolfgang, Dezentrale Agenturen in der EU-Rechtsetzung, EuR 2016, p. 631–666.

Whittaker, Meredith/*Crawford*, Kate/*Dobbe*, Roel/*Fried*, Genevieve, et al., AI Now Report 2018, December 2018.

Wirth, Christian/*Kolain*, Michael, Privacy by BlockchainDesign: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data, in: Prinz/Hoschka (ed.), Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies, Amsterdam 2018.

Wischmeyer, Nils, Der Computer, der mich einstellte, brand eins of 4/12/2017.

Wischmeyer, Thomas, Regulierung intelligenter Systeme, AöR 143 (2018), p. 1–66.

Zweig, Katharina Anna, Wo Maschinen irren können, working paper of the Bertelsmann-Stiftung, Gütersloh, 2018.

About the author

Prof. Dr. Mario Martini holds the Chair of Administrative Science, Constitutional Law, Administrative Law and European Law at the German University of Administrative Sciences Speyer and is head of the program "Transformation of the State in the Digital Age" at the German Research Institute for Public Administration, Fellow at the Center for Advanced Internet Studies and a member of the Federal Government's Data Ethics Commission. Until April 2010, he held a chair in constitutional and administrative law at the Ludwig Maximilian University in Munich. Mario Martini habilitated at the Bucerius Law School (2006) and received his PhD from the Johannes Gutenberg University in Mainz (2000). His research focuses in particular on the internet, data protection, media and telecommunications law, law and economics as well as open government and artificial intelligence.

Recent publications:

1. Monographs

- Blackbox Algorithmus – Grundfragen eine Regulierung künstlicher Intelligenz, Springer, 2019, 423 p.
- Zwischen Agora und Arkanum: die Innenministerkonferenz als Gegenstand des Informationsrechts, Duncker & Humblot, Berlin 2018, 284 p.
- Die Landarztquote - verfassungsrechtliche Zulässigkeit und rechtliche Ausgestaltung, Duncker & Humblot, 235 Seiten, 2017 (with Jan Ziekow).
- Verwaltungsprozessrecht und Allgemeines Verwaltungsrecht - eine systematische Darstellung in Text-Bild-Kombination, Vahlen, München, 2017, 243 p.

2. Articles

- Facebook, die Lebenden und die Toten – Der digitale Nachlass aus telekommunikations- und datenschutzrechtlicher Sicht, JZ 2019, p. 235-241 (with Thomas Kienle).
- Subsumtionsautomaten ante portas? - Zu den Grenzen der Automatisierung in verwaltungsrechtlichen (Rechtsbehelfs-)Verfahren, DVBl 2018, p. 1128-1138 (with David Nink).
- Iron Man am Arbeitsplatz? - Exoskelette zwischen Effizienzstreben, Daten- und Gesundheitsschutz: Chancen und Risiken der Verschmelzung von Mensch und Maschine in der Industrie 4.0, NZA 2018, p. 625-637 (with Jonas Botta).
- Das neue Sanktionsregime der DSGVO – ein scharfes Schwert ohne legislativen Feinschliff (with David Wagner und Michael Wenzel), Teil 1: VerwArch 2018, p. 163-189, Teil 2: VerwArch 2018, p. 296-335.
- Art. 91c Abs. 5 GG und das neue Zugangsregime zur digitalen Verwaltung – Quantensprung oder zu kurz gesprungen?, ZG 32 (2017), p. 193-227 (with Cornelius Wiesner).
- Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, p. 1251-1259 (with Quirin Weinzierl).