Opinion of the Data Ethics Commission

Executive Summary

daten ethik kommission

Opinion of the Data Ethics Commission

daten
ethik
kommission

Contents

The full version of the Opinion can be downloaded from ***www.datenethikkommission.de****.*

Guiding motifs

Our society is experiencing profound changes brought about by digitalisation. Innovative data-based technologies may benefit us at both the individual and the wider societal levels, as well as potentially boosting economic productivity, promoting sustainability and catalysing huge strides forward in terms of scientific progress. At the same time, however, digitalisation poses risks to our fundamental rights and freedoms. It raises a wide range of ethical and legal questions centring around two wider issues: the role we want these new technologies to play, and their design. If we want to ensure that digital transformation serves the good of society as a whole, both society itself and its elected political representatives must engage in a debate on how to use and shape data-based technologies, including artificial intelligence (AI).

Germany's Federal Government set up the Data Ethics Commission *(Datenethikkommission)* on 18 July 2018. It was given a one-year mandate to develop ethical benchmarks and guidelines as well as specific recommendations for action, aiming at protecting the individual, preserving social cohesion, and safeguarding and promoting prosperity in the information age. As a starting point, the Federal Government presented the Data Ethics Commission with a number of key questions clustered around three main topics: algorithm-based decision-making (ADM), AI and data. In the opinion of the Data Ethics Commission, however, AI is merely one among many possible variants of an algorithmic system, and has much in common with other such systems in terms of the ethical and legal questions it raises. With this in mind, the Data Ethics Commission has structured its work under two different headings: **data** and **algorithmic systems** (in the broader sense).

In preparing its Opinion, the Data Ethics Commission was inspired by the following **guiding motifs**:

- Ensuring the human-centred and value-oriented design of technology
- Fostering digital skills and critical reflection in the digital world
- Enhancing protection for individual freedom, self-determination and integrity
- Fostering responsible data utilisation that is compatible with the public good
- Introducing risk-adapted regulation and effective oversight of algorithmic systems
- Safeguarding and promoting democracy and social cohesion
- Aligning digital strategies with sustainability goals
- Strengthening the digital sovereignty of both Germany and Europe.

1

General ethical and legal principles

Humans are morally responsible for their actions, and there is no escaping this moral dimension. Humans are responsible for the goals they pursue, the means by which they pursue them, and their reasons for doing so. Both this dimension and the societal conditionality of human action must always be taken into account when designing our technologically shaped future. At the same time, the notion that technology should serve humans rather than humans being subservient to technology can be taken as incontrovertible fact. Germany's constitutional system is founded on this **understanding of human nature**, and it adheres to the tradition of Europe's cultural and intellectual history.

Digital technologies have not altered our ethical framework – in terms of the basic values, rights and freedoms enshrined in the German Constitution and in the Charter of Fundamental Rights of the European Union. Yet the new challenges we are facing mean that we need to reassert these values, rights and freedoms and perform new balancing exercises. With this in mind, the Data Ethics Commission believes that the following ethical and legal principles and precepts should be viewed as indispensable and socially accepted benchmarks for action.

Human dignity
Human dignity is a principle that presupposes the unconditional value of every human being, prohibiting such practices as the total digital monitoring of the individual or his or her humiliation through deception, manipulation or exclusion.

Self-determination
Self-determination is a fundamental expression of freedom, and encompasses the notion of informational self-determination. The term "digital self-determination" can be used to express the idea of a human being a self-determined player in a data society.

Privacy
The right to privacy is intended to preserve an individual's freedom and the integrity of his or her personal identity. Potential threats to privacy include the wholesale collection and evaluation of data about even the most intimate of topics.

Security
The principle of security relates not only to the physical and emotional safety of humans but also to environmental protection, and as such involves the preservation of vitally important assets. Guaranteeing security entails compliance with stringent requirements, e. g. in relation to human/machine interaction or system resilience to attacks and misuse.

Democracy

Digital technologies are of systemic relevance to the flourishing of democracy. They make it possible to shape new forms of political participation, but they also foster the emergence of threats such as manipulation and radicalisation.

Justice and Solidarity

In view of the vast amounts of power being accumulated using data and technologies, and the new threats of exclusion and discrimination, the safeguarding of equitable access and distributive justice is an urgent task. Digitalisation should foster participation in society and thereby promote social cohesion.

Sustainability

Digital developments also serve sustainable development. Digital technologies should contribute towards achieving economic, ecological and social sustainability goals.

Ethics cannot be equated on a one-to-one basis with the law. In other words, not everything that is relevant from an ethical perspective can and should be enshrined in legislation; conversely, there are provisions of the law that are motivated purely by pragmatic considerations. Nevertheless, the law must, at all times, be heedful of the potential ethical implications of the legal provisions in force, as well as living up to ethical standards. The Data Ethics Commission holds the view that **regulation is necessary, and cannot be replaced by ethical principles**. This is particularly true for issues with heightened implications for fundamental rights that require the central decisions to be made by the democratically elected legislator. Regulation is also an essential basis for building a system where citizens, companies and institutions can trust that the transformation of society will be guided by ethical principles.

At the same time, regulation must not unduly inhibit technological and social innovation and dynamic market growth. Overly rigid laws that attempt to regulate every last detail of a situation may place a stranglehold on progress and increase red tape to such an extent that innovation by German companies can no longer keep pace with the rate of technological development on the international stage.

Yet legislation is only one of a range of tools that can be used to lend tangible shape to ethical principles. The **synergistic use of various governance instruments** at different levels (multi-level governance) is vital in view of the complexity and dynamism of data ecosystems. These instruments include not only legislative measures and standardisation, but also various forms of co-regulation or self-regulation. Technology and technological design can moreover function as governance instruments themselves, and the same applies to business models and options for steering the economy. Governance in the broader sense also encompasses policy-making decisions in the fields of education and research. It is important to consider each of the aforesaid governance instruments not only in a national context, but also (and in particular) in their **European and international** contexts.

In the view of the Data Ethics Commission, all of the key questions presented by the Federal Government belong to one of two different perspectives: questions that concentrate mainly on data (the **"data perspective"**) and questions that are primarily focused on algorithmic systems (the **"algorithms perspective"**). These two perspectives should not be regarded as competing views or two sides of the same coin; instead, they represent two different **ethical discourses, which both complement each other and are contingent upon each other**. These different ethical discourses are typically also reflected in different governance instruments, including in different acts of legislation.

2

Data

The **data perspective** focuses on digital data, which are used for machine learning, as a basis for algorithmically shaped decisions, and for a plethora of further purposes. This perspective considers data primarily with a view to their **origin** and to the potential **impact** their processing may have on certain parties who are involved with the data, such as by being the data subject, as well as on society at large. From an ethical and legal point of view, it is important to identify **standards for data governance**; typically, however, **rights** that parties involved with the data can enforce against others will play an even more significant role. A central distinction in this context is that between personal and non-personal data, since it determines whether the provisions of data protection law apply.

General standards for data governance

In the opinion of the Data Ethics Commission, responsible data governance must be guided by the following data ethics principles:

- **Foresighted responsibility:** Possible future cumulative effects, network effects and effects of scale, technological developments and changing actor constellations must be taken into account when gauging the potential impact of collecting, processing and forwarding data on individuals or the general public.
- **Respect for the rights of the parties involved:** Parties who have been involved in the generation of data – whether as data subjects or in a different role – may have rights in relation to such data, and these rights must be respected.
- **Data use and data sharing for the public good:** As a non-rivalrous resource, data can be duplicated and used in parallel by many different individuals for many different purposes, thereby furthering the public good.
- **Fit-for-purpose data quality:** Responsible use of data includes ensuring a high level of data quality that is fit for the relevant purpose.
- **Risk-adequate level of information security:** Data are vulnerable to external attacks, and it is difficult to recover them once they have gone astray. The standard of information security applied must therefore be commensurate with the potential for risk inherent to the situation in question.
- **Interest-oriented transparency:** Controllers must be prepared and in a position to account for their data-related activities. This requires appropriate documentation and transparency and, if necessary, a corresponding liability regime in place.

Data rights and corresponding obligations

For self-determined navigation in the data society, parties must have, and be able to enforce, certain data-related rights against others. First and foremost among these rights are those relating to an individual's **personal data**, which derive from the right to informational self-determination that is enshrined as a fundamental right, and which are guaranteed by the applicable data protection law. Digital self-determination in the data society also includes the self-determined economic exploitation of one's own data, and it includes self-determined management of **non-personal data**, such as non-personal data generated by one's own devices. The Data Ethics Commission takes the view that, in principle, a right to digital self-determination in the data society also applies to companies and **legal entities** and – at least to some extent – to groups of persons (collectives).

Data are often generated with contributions from different parties who are acting in different roles – be it as the data subject, be it as the owner of a data-generating device or be it in yet another role. In the opinion of the Data Ethics Commission such contributions to the generation of data should not lead to exclusive ownership rights in data, but rather to **data-specific rights of co-determination and participation**, which in turn may lead to corresponding obligations on the part of other parties. The extent to which an individual should be entitled to data rights of this kind, and the shape they should take, depends on the following general factors:

a) the nature and scope of that party's **contribution to data generation**,

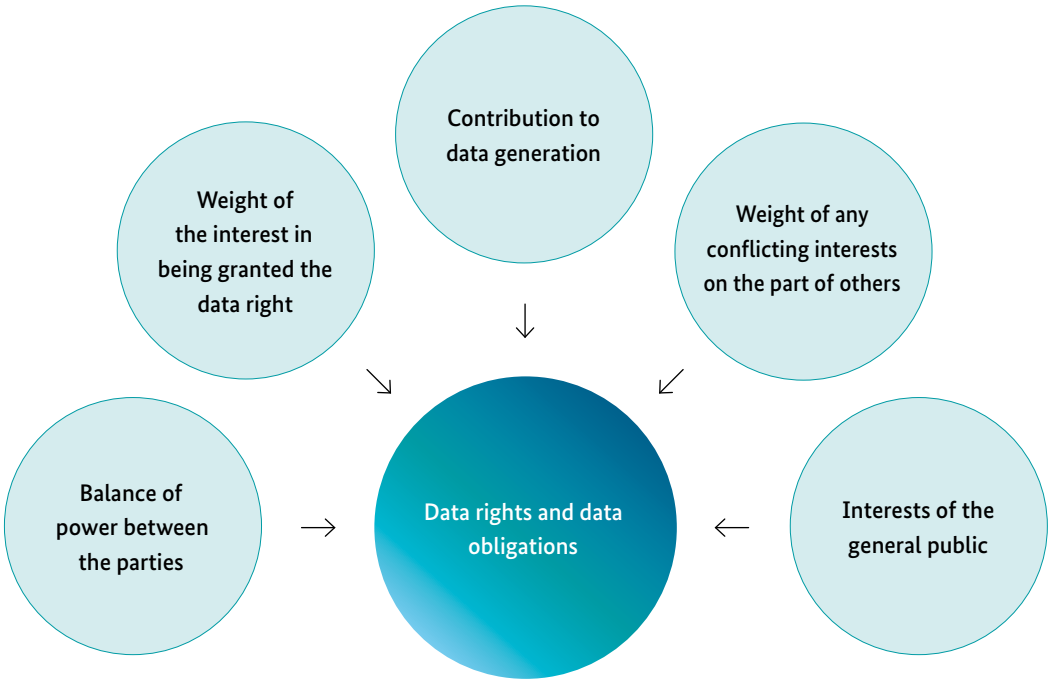
b) the **weight of that party's legitimate interest** in being granted the data right,

c) the weight of any possibly **conflicting interests** on the part of the other party or of third parties, taking into account any potential compensation arrangements (e.g. protective measures, remuneration),

d) the **interests of the general public**, and

e) the **balance of power** between the parties involved.

Figure 1:
Factors for the shaping of data rights and data obligations



Data rights may allow their holders to pursue a number of different goals, in particular the following:

- requiring that a controller **desist from data use** (up to a right to require erasure of the data),
- requiring that a controller **rectify the data**,
- requiring that a controller grant **access to data** (up to full data portability), or
- requiring an **economic share** in profits derived with the help of the data.

For each type of data right (desistance, rectification, access, economic share) there exists a **separate set of conditions** defining, e.g., what counts as a party's legitimate interest in being granted the data right. For determining whether a party has a right to require desistance from a particular data use, key considerations include the potential for harm associated with said use and the circumstances under which the party in question had contributed to generating the data. Potential for harm may also be relevant when a request is made to rectify data, but the benchmark is lower in this respect. Where a party requests access to data, there is a graded spectrum of interests that count as a legitimate interest to be granted such access, which is particularly relevant within existing value creation systems. Only under very narrowly defined conditions may a party have an independent claim to an economic share in profits derived by others. The **rights granted to data subjects** under the EU's General Data Protection Regulation (GDPR) are a particularly important manifestation of these data rights, aimed specifically at protecting the natural persons to whom the data pertain; they are also to some extent a standardised manifestation given that they hinge on the qualification of data as personal data.

Considering these principles, the Data Ethics Commission wishes to submit the following key recommendations for action:

Standards for the use of personal data

1

The Data Ethics Commission recommends that **measures be taken against ethically indefensible uses of data**. Examples of these uses include total surveillance, profiling that poses a threat to personal integrity, the targeted exploitation of vulnerabilities, addictive designs and dark patterns, methods of influencing political elections that are incompatible with the principle of democracy, vendor lock-in and systematic consumer detriment, and many practices that involve trading in personal data.

2

Data protection law as well as other branches of the legal system (including general private law and unfair commercial practices law) already provide for a range of instruments that can be used to prevent such ethically indefensible uses of data. However, in spite of the widespread impact and enormous potential for harm, too little has been done to date in terms of harnessing the power of these instruments, particularly against the market giants. The various factors contributing to this **enforcement gap** must be tackled systematically.

3

As well as steps to make front-line players (e.g. supervisory authorities) more aware of the existing options, there is an urgent need for the **legislative framework in force to be fleshed out more clearly and strengthened in certain areas**. Examples of recommended measures include the blacklisting of data-specific unfair contract terms, the fleshing out of data-specific contractual duties of a fiduciary nature, new data-specific torts, the blacklisting of certain data-specific unfair commercial practices and the introduction of a much more detailed legislative framework for profiling, scoring and data trading.

4

In order to allow supervisory authorities to take action more effectively, these authorities need significantly better human and material resources. Attempts should be made to strengthen and formalise cooperation between the different data protection authorities in Germany, thereby ensuring the uniform and coherent application of data protection law. If these attempts fail, consideration should be given to the **centralisation of market-related supervisory activities** within a federal-level authority that is granted a broad mandate and that cooperates closely with other specialist supervisory authorities. The authorities at *Land* level should remain responsible for supervisory activities relating to the public sector, however.

5

The Data Ethics Commission believes that **"data ownership"** (i.e. exclusive rights in data modelled on the ownership of tangible assets or on intellectual property) would not solve any of the problems we are currently facing, but would create new problems instead, and **recommends refraining from their recognition**. It also advises against granting to data subjects copyright-like rights of economic exploitation in respect of their personal data (which might then be managed by collective societies).

6

The Data Ethics Commission also argues that **data should not be referred to as 'counter-performance'** provided in exchange for a service, even though the term sums up the issue in a nutshell and has helped to raise awareness among the general public. Regardless of the position that data protection authorities and the European Court of Justice will ultimately take with regard to the prohibition under the GDPR of 'tying' or 'bundling' consent with the provision of a service, the Data Ethics Commission believes that consumers must be offered **reasonable alternatives** to releasing their data for commercial use (e.g. appropriately designed **pay options**).

7

Stringent requirements and limitations should be imposed on the use of data for **personalised risk assessment** (e.g. the "black box" premiums in certain insurance schemes). In particular, the processing of data may not intrude on intimate areas of private life, there must be a clear causal relationship between the data and the risk, and the difference between individual prices charged on the basis of personalised and non-personalised risk assessments should not exceed certain percentages (to be determined). There should also be stringent requirements in respect of transparency, non-discrimination and the protection of third parties.

8

The Data Ethics Commission advises the Federal Government not to consider the issues falling under the heading of **"digital inheritance"** as having been settled by the Federal Court of Justice's 2018 ruling. The ephemeral spoken word is being replaced in many situations by digital communications that are recorded more or less in their entirety, and the possibility that these records will be handed over to a deceased's heirs adds a whole new dimension of privacy risk. A range of mitigating measures should be taken, including the imposition of new obligations on service providers, quality assurance standards for digital estate planning services and national regulations on post-mortem data protection.

9

The Data Ethics Commission recommends that the Federal Government should invite the social partners to work towards a common position on the legislative provisions that should be adopted with a view to **stepping up the protection of employee data**, based on examples of best practices from existing collective agreements. The concerns of individuals in non-standard forms of employment should also be taken into account during this process.

10

In view of the benefits that could be gained from **digitalising healthcare**, the Data Ethics Commission recommends swift expansion of digital infrastructures in this sector. The expansion of both the range and the quality of digitalised healthcare services should include measures to better allow patients to exercise their rights to informational self-determination. Measures that could be taken in this respect include the introduction and roll-out of an electronic health record, building on a participatory process that involves the relevant stakeholders, and the further development of procedures for reviewing and assessing digital medical apps in the insurer-funded and consumer-funded health markets.

11

The Data Ethics Commission calls for action against the significant enforcement gap that exists with regard to statutory **protection of children and young people** in the digital sphere. Particular attention should be paid to the development and mandatory provision of technologies (including effective identity management) and default settings that not only guarantee reliable protection of children and young people but that are also family-friendly, i.e. that neither demand too much of parents or guardians nor allow or even encourage excessive surveillance in the home environment.

12

Standards and guidelines on the handling of the personal data of **vulnerable and care-dependent persons** should be introduced to provide greater legal certainty for professionals in the care sector. At the same time, consideration should be given to clarifying in the relevant legal provisions on living wills that these may also include dispositions with regard to the future processing of personal data as far as such processing will require the care-dependent person's consent (e.g. for dementia patients who will not be in a position to provide legally valid consent).

13

The Data Ethics Commission believes that a number of binding requirements should be introduced to ensure the **privacy-friendly design of products and services**, so that the principles of privacy by design and privacy by default (which the GDPR imposes on controllers) will already be put into practice upstream, by manufacturers and service providers themselves. Such requirements would be particularly important with regard to consumer equipment. In this context, standardised icons should also be introduced so that consumers are able to take informed purchase decisions.

14

Action must also be taken at a number of different levels to provide manufacturers with adequate **incentives to implement features of privacy-friendly design**. This includes effective legal remedies that can be pursued against parties along the entire distribution chain to ensure that also manufacturers can be held accountable for inadequate application of the principles of privacy by design and privacy by default. Consideration should also be given, in particular, to requirements built into tender specifications, procurement guidelines for public bodies and conditions for funding programmes. The same applies to **privacy-friendly product development**, including the training of algorithmic systems.

15

While debates on data protection tend (quite rightly) to centre around natural persons, it is important not to ignore the fact that **companies and legal persons must also be granted protection**. The almost limitless ability to pool together individual pieces of data can be used as a means of obtaining a comprehensive picture of a company's internal operating procedures, and this information can be passed on to competitors, negotiating partners, parties interested in a takeover bid and so on. This poses a variety of threats – *inter alia* to the digital sovereignty of both Germany and Europe – in view of the significant volumes of data that flow to third countries. Many of the Data Ethics Commission's recommendations for action therefore also apply on a *mutatis mutandis* basis to the data of legal persons. The Data Ethics Commission believes that action must be taken by the Federal Government to **step up the level of data-related protection afforded to companies**.

Improving controlled access to personal data

16

The Data Ethics Commission identifies enormous potential in the use of data for research purposes that serve a public interest (e.g. to improve healthcare provision). Data protection law as it currently stands acknowledges this potential, in principle, by granting far-reaching privileges for the processing of personal data for research purposes. Uncertainty persists, however, in particular as regards the scope of the so-called research privilege for secondary use of data, and the scope of what counts as "research" in the context of product development. The Data Ethics Commission believes that appropriate **clarifications in the law** are necessary to rectify this situation.

17

The fragmentation of research-specific data protection law, both within Germany itself and among the EU Member States, represents a potential obstacle to data-driven research. The Data Ethics Commission therefore recommends that **research-specific regulations should be harmonised**, both between federal and *Land* level and between the different legal systems within the EU. Introducing a notification requirement for research-specific national law could also bring some improvement, as could the establishment of a European clearing house for cross-border research projects.

18

In the case of research involving particularly sensitive categories of personal data (e.g. health data), **guidelines** should be produced with information for researchers on how to obtain consent in a legally compliant manner, and **innovative consent models should be promoted and explicitly recognised by the law**. Potential options include the development and roll-out of digital consent assistants or the recognition of so-called meta consent, alongside further endeavours to clarify the scope of the research privilege for secondary use of data.

19

The Data Ethics Commission supports, in principle, the move towards a **"learning healthcare system"**, in which healthcare provision is continuously improved by making systematic and quality-oriented use of the health data generated on a day-to-day basis, in keeping with the principles of evidence-based medicine. If further progress is made in this direction, however, greater efforts must be made at the same time to protect data subjects against the significant potential for discrimination that exists when sensitive categories of data are used; this might involve **prohibiting the exploitation of such data** beyond the defined range of purposes.

20

The development of procedures and standards for data **anonymisation** and **pseudonymisation** is central to any efforts to improve controlled access to (formerly) personal data. A legal presumption that, if compliance with the standard has been achieved, data no longer qualify as personal, or that "appropriate safeguards" have been provided in respect of the data subject's rights, would improve legal certainty by a long way. These measures should be accompanied by rules that – on pain of criminal penalty – prohibit the de-anonymisation of anonymised data (e.g., because new technology becomes available that would allow the re-identification of data subjects) or the reversal of pseudonymisation, both in the absence of narrowly defined grounds for doing so. Also research in the field of **synthetic data** shows enormous promise, and more funding should be funnelled into this area.

21

Fundamentally speaking, the Data Ethics Commission believes that **innovative data management and data trust schemes** hold great potential, provided that these systems are designed to be robust, suited to real-life applications and compliant with data protection law. A broad spectrum of models falls under this heading, ranging from dashboards that perform a purely technical function (**privacy management tools**, PMT) right through to comprehensive data and consent management services (**personal information management services**, PIMS). The underlying aim is to empower individuals to take control over their personal data, while not overburdening them with decisions that are beyond their capabilities. The Data Ethics Commission recommends that research and development in the field of data management and data trust schemes should be identified as a funding priority, but also wishes to make it clear that adequate protection of the rights and legitimate interests of all parties involved will require additional **regulatory measures at EU level**. These regulatory measures would need to secure central functions without which operators cannot be active, since their scope for action would otherwise be very limited. On the other hand, it is also necessary to protect individuals against parties that they assume to be acting in their interests, but that, in reality, are prioritising their own financial aims or the interests of others. In the event that a feasible method of protection can be found, data trust schemes could serve as vitally important mediators between data protection interests and data economy interests.

22

As far as the right to **data portability** enshrined in Article 20 GDPR is concerned, the Data Ethics Commission recommends that industry-specific codes of conduct and standards on data formats should be adopted. Given that the underlying purpose of Article 20 GDPR is not only to make it more straightforward to change provider, but also to allow other providers to access data more easily, it is important to evaluate carefully the market impact of the existing right to portability and to analyse potential mechanisms by which it can be prevented that a small number of providers increase yet further their market power. Until the findings of this evaluation are available, expansion of the scope of this right (for example to cover data other than data provided by the data subject, or real-time porting of data) would seem premature and not advisable.

23

In certain sectors, for example messenger services and social networks, **interoperability or interconnectivity obligations** might help to reduce the market entry barriers for new providers. Such obligations should be designed on an asymmetric basis, i.e. the stringency of the regulation should increase in step with the company's market share. Interoperability and interconnectivity obligations would also be a prerequisite for building up or strengthening, within and for Europe, certain basic services of an information society.

Debates around access to non-personal data

24

Access by European companies to appropriate non-personal data of appropriate quality is a key factor for the growth of the European data economy. In order to benefit from enhanced **access to data**, however, stakeholders must have a sufficient degree of data-awareness and have the data skills that are necessary to make use of the data. Also, access to data proves to be disproportionately advantageous to stakeholders that have already built up the largest reserves of data and that have the best data infrastructures at hand. The Data Ethics Commission therefore wishes to stress that the factors referred to should always receive due attention when discussing whether and how to improve data access, in keeping with the **ASISA principle** *(Awareness – Skills – Infrastructures – Stocks – Access)*.

25

The Data Ethics Commission therefore supports the efforts already initiated at European level to promote and improve **data infrastructures** in the broadest sense of the term (e. g. platforms, standards for application programming interfaces and other elements, model contracts, EU support centre), and recommends to the Federal Government that these efforts should continue to be matched by corresponding efforts at national level. It would also be advisable to set up an ombudsman's office at federal level to provide assistance and support in relation to the negotiation of data access agreements and dispute settlement.

26

The Data Ethics Commission ascribes enormous importance to a holistically conceived, sustainable and strategic **economic policy** that outlines effective methods of preventing not only the exodus of innovative European companies or their acquisition by third-country companies, but also an excessive dependence on third-country infrastructures (e. g. server capacities). A balance must be struck in this context between much-needed international cooperation and networking on the one hand, and on the other a resolute assumption of responsibility for sustainable security and prosperity in Europe against the backdrop of an ever-evolving global power dynamic.

27

Also from the perspective of boosting the European data economy, the Data Ethics Commission does not see any benefit in introducing new exclusive rights ("data ownership", "data producer right"). Instead, it recommends affording **limited third-party effects to contractual agreements** (e. g. to restrictions on data utilisation and onward transfer of data by a recipient). These third-party effects could be modelled on the new European regime for the protection of trade secrets. The Data Ethics Commission also recommends the adoption of legislative solutions enabling European companies to cooperate in their use of data, for example by using data trust schemes, without running afoul of anti-trust law (**"data partnerships"**).

28

The data accumulated in existing value creation systems (e. g. production and distribution chains) are often of enormous commercial significance, both inside and outside that value creation system. In many cases, however, the provisions on data access that appear in the contractual agreements concluded within a value creation system are unfair and/or inefficient, or lacking entirely; in certain cases, there is no contractual agreement at all. Efforts must therefore be made to **raise awareness among businesses** in sectors far outside what is commonly perceived as the "data economy", and to provide practical guidance and support (e. g. model contracts).

29

The Data Ethics Commission furthermore recommends cautious **adaptations of the current legislative framework**. The first stage in this process should be to make explicit reference in Section 311 of the [German] Civil Code (*Bürgerliches Gesetzbuch*, BGB) to the special relationship that exists between a party that has contributed to the generation of data in a value creation system and the controller of the data, clarifying that such parties may have certain quasi-contractual duties of a fiduciary nature. These duties should normally include a duty to enter into negotiations about fair and efficient data access arrangements. Consideration should also be given to whether additional steps should be taken, which could range from blacklisting particular contract terms also for B2B transactions, to formulating default provisions for data contracts, to introducing sector-specific data access rights.

30

The Data Ethics Commission believes that **open government data (OGD) concepts** hold enormous potential, and recommends that these concepts should be built on and promoted. It also recommends a series of measures to promote a **shift in mindset among public authorities** (something that has not yet fully taken place) and to make it easier in practice to share data on the basis of OGD concepts. These measures include not only the establishment of the relevant **infrastructures** (e.g. platforms), but also harmonisation and improvement of the existing **legal framework** that is currently fragmented and sometimes inconsistent.

31

Nevertheless, the Data Ethics Commission identifies a degree of tension between efforts to promote OGD (relying on principles such as "open by default" and "open for all purposes"), and efforts to enhance data protection and the protection of trade secrets (with legally enshrined concepts such as "privacy by default"). The Data Ethics Commission submits that, in cases of doubt, **priority should be given to the duty of protecting** individuals and companies who have entrusted their data to the State (often without being given any choice in the matter, e.g. tax information). The State must deliver on this duty by implementing a range of different measures, which may include technical as well as legal safeguards against misuse of data.

32

In particular, it would be beneficial to develop **standard licences and model terms and conditions** for public-sector data sharing arrangements, and to make their use mandatory (at least on a sector-specific basis). These standard licenses and model terms and conditions should include clearly defined safeguards for the rights of third parties who are affected by a data access arrangement. Provision should also be made against data being used in a way that ultimately harms public interests, and also against still greater accumulation of data and market power on the part of the big players (which would be likely to undermine competition) and against the taxpayer having to pay twice.

33

As regards **open-data concepts in the private sector**, priority should be given to **promoting and supporting voluntary data-sharing arrangements**. Consideration must be given not only to the improvement of infrastructures (e.g. data platforms), but also to a broad range of potential incentives; these might include certain privileges in the context of tax breaks, public procurement, funding programmes or licensing procedures. Statutory data access rights and corresponding obligations to grant access should be considered as fall-back options if the above measures fail to deliver the desired outcomes.

34

Generally speaking, the Data Ethics Commission believes that a cautious approach should be taken to the introduction of statutory data access rights; ideally such rights should be developed only on a **sector-by-sector basis**. Sectors in which the level of demand should be analysed include the media, mobility or energy sectors. In any case, before a statutory data access right or even a disclosure obligation is introduced, a full impact assessment needs to be carried out, examining and weighing up against each other all possible implications; these include implications for data protection and the protection of trade secrets, for investment decisions and the distribution of market power, as well as for the strategic interests of German and European companies compared to those of companies in third countries.

35

The Data Ethics Commission recommends considering enhanced obligations of private enterprises to grant access to data **for public interest and public-sector purposes** (Business-to-Government, B2G). A cautious and sector-specific approach is, however, recommended in this respect as well.

3

Algorithmic systems

The **algorithms perspective** focuses on the architecture of data-driven algorithmic systems, their dynamics and the systems' impacts on individuals and society. The ethical and legal discourse in this area typically centres around the relationship between humans and machines, with a particular focus on automation and the outsourcing of increasingly complex operational and decision-making processes to "autonomous" systems enabled by AI. The algorithms perspective differs from the data perspective in that the data processed by the system might have no connection whatsoever with the persons affected by it; in particular, individuals may suffer ethically indefensible implications even if all of the data used (e.g. to train an algorithmic system) are non-personal. The current debates on "algorithmic oversight" or liability for AI are of central importance in this respect.

General standards for algorithmic systems

The Data Ethics Commission distinguishes between three different levels of algorithmic involvement in human decision-making, based on the distribution of tasks between the human and the machine in the specific case in question:

a) **algorithm-based** decisions are human decisions based either in whole or in part on information obtained using algorithmic calculations,

b) **algorithm-driven** decisions are human decisions shaped by the outputs of algorithmic systems in such a way that the human's factual decision-making abilities and capacity for self-determination are restricted,

c) **algorithm-determined** decisions trigger consequences automatically; no provision is made for a human decision in the individual case.

In the opinion of the Data Ethics Commission, the following principles should be observed to ensure the responsible use of algorithmic systems.

- **Human-centred design:** Systems must be centred around the human who uses them or who is affected by their decisions; they must prioritise his or her fundamental rights and freedoms, basic needs, physical and emotional well-being and skills development.

- **Compatibility with core societal values:** The process of system design must take account of the system's impact on society as a whole, and in particular its effects on the democratic process, on the citizen-centred nature of state action, on competition, on the future of work and on the digital sovereignty of Germany and Europe.

- **Sustainability:** Considerations relating to the availability of human skills, participation, environmental protection, sustainable resource management and sustainable economic activity are becoming increasingly important factors in the design and use of algorithmic systems.

- **Quality and performance:** Algorithmic systems must work correctly and reliably so that the goals pursued with their help can be achieved.

- **Robustness and security:** Robust and secure system design involves not only making the system secure against external threats, but also protecting humans and the environment against any negative impacts that may emanate from the system.

- **Minimisation of bias and discrimination:** The decision-making patterns upon which algorithmic systems are based must not be the source of systematic bias or the cause of discriminatory decisions.

- **Transparent, explainable and comprehensible systems:** It is vitally important to ensure not only that the users of algorithmic systems understand how these systems function and can explain and control them, but also that the parties affected by a decision are provided with sufficient information to exercise their rights properly and challenge the decision if necessary.

- **Clear accountability structures:** Questions of the allocation of responsibility and accountability including possible liability arising with the use of algorithmic systems must be unambiguously resolved.

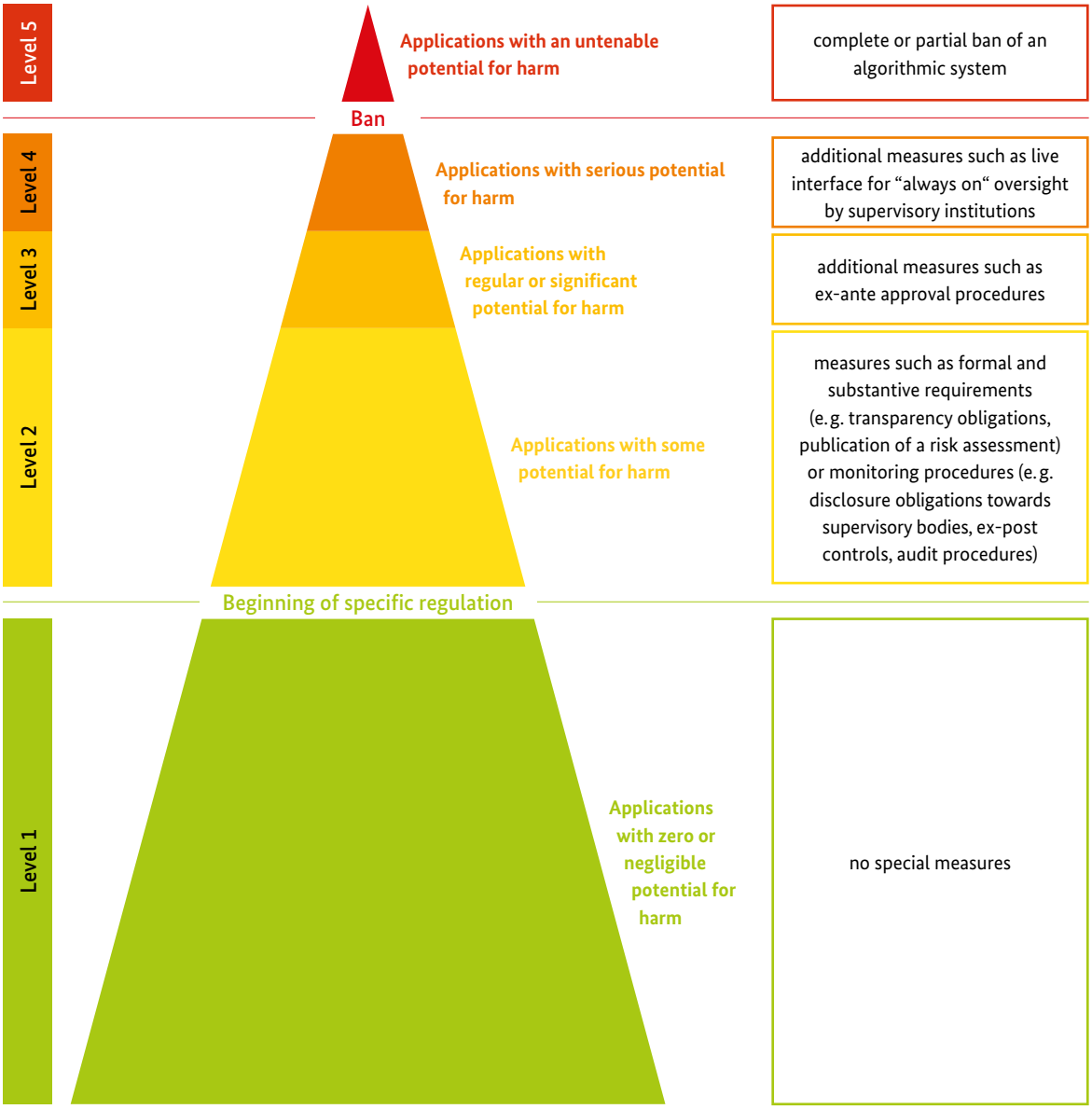
System criticality

The level of **criticality of an algorithmic system** dictates the specific requirements it must meet, in particular with regard to transparency and oversight. System criticality is determined by assessing an algorithmic system's potential for harm, on the basis of a two-pronged investigation into the **likelihood that harm will occur** and the **severity of that harm**.

The **severity** of the harm that could potentially be sustained, for example as a result of a mistaken decision, depends on the significance of the legally protected rights and interests affected (such as the right to privacy, the fundamental right to life and physical integrity, the prohibition of discrimination), the level of potential harm suffered by individuals (including non-material harm or loss of utility that are hard to calculate in monetary terms), the number of individuals affected, the total figure of the harm potentially sustained and the overall harm sustained by society as a whole, which may go well beyond a straightforward summation of the harm suffered by individuals. The **likelihood** that harm will be sustained is also influenced by the properties of the system in question, in particular the role of the algorithmic system components in the decision-making process, the complexity of the decision, the effects of the decision and the reversibility of these effects. The severity and likelihood of the predicted harm may also be contingent on whether the algorithmic systems are operated by the State or by private enterprises and, particularly in a business context, on the market power wielded by the system's operator.

In conclusion, the Data Ethics Commission wishes to make the following recommendations for action on the basis of these principles:

Figure 2:
Criticality pyramid and risk-adapted regulatory system for the use of algorithmic systems



Risk-adapted regulatory approach

36

The Data Ethics Commission recommends adopting a **risk-adapted regulatory approach** to algorithmic systems. The principle underlying this approach should be as follows: the greater the potential for harm, the more stringent the requirements and the more far-reaching the intervention by means of regulatory instruments. When assessing this potential for harm, the **sociotechnical system as a whole** must be considered, or in other words all the components of an algorithmic application, including all the people involved, from the development phase – for example the training data used – right through to its implementation in an application environment and any evaluation and adjustment measures.

37

The Data Ethics Commission recommends that the potential of algorithmic systems to harm individuals and/or society should be determined uniformly on the basis of a **universally applicable model**. For this purpose, the legislator should develop a **criteria-based assessment scheme** as a tool for determining the criticality of algorithmic systems. This scheme should be based on the general ethical and legal principles presented by the Data Ethics Commission.

38

Among other things, the **regulatory instruments and the requirements that apply to algorithmic systems** should include corrective and oversight mechanisms, specifications of transparency, explainability and comprehensibility of the systems' results, and rules on the allocation of responsibility and liability for using the systems.

39

The Data Ethics Commission believes that a useful first stage in determining the potential for harm of algorithmic systems is to distinguish between **five levels of criticality**. Applications that fall under the lowest of these levels (Level 1) are associated with zero or negligible potential for harm, and it is unnecessary to carry out special oversight of them or impose requirements other than the general quality requirements that apply to products irrespective of whether they incorporate algorithmic systems.

40

Applications that fall under Level 2 are associated with **some potential for harm**, and can and should be regulated on an as-needs basis; regulatory instruments used in this connection may include ex-post controls, an obligation to produce and publish an appropriate risk assessment, an obligation to disclose information to supervisory bodies or also enhanced transparency obligations and access rights for individuals affected.

41

In addition, the introduction of licensing procedures may be justified for applications that fall under Level 3, which are associated with **regular** or **significant potential for harm**. Applications that fall under Level 4 are associated with **serious potential for harm**; the Data Ethics Commission believes that these applications should be subject to enhanced oversight and transparency obligations. These may extend all the way through to the publication of information on the factors that influence the algorithmic calculations and their relative weightings, the pool of data used and the algorithmic decision-making model; an option for "always-on" regulatory oversight via a live interface with the system may also be required.

42

Finally, a complete or partial ban should be imposed on **applications with an untenable potential for harm** (Level 5).

43

The Data Ethics Commission believes that the measures it has proposed should be implemented in a new EU Regulation on algorithmic systems enshrining general **horizontal requirements (Regulation on Algorithmic Systems, EU-ASR)**. This horizontal regulation should incorporate the fundamental requirements for algorithmic sytems that the Data Ethics Commission developed. In particular, it should group together general substantive rules – informed by the concept of system criticality – on the admissibility and design of algorithmic systems, transparency, the rights of individuals affected, organisational and technical safeguards and supervisory institutions and structures. This horizontal instrument should be fleshed out in **sectoral instruments** at EU and Member State level, with the concept of system criticality once again serving as a guiding framework.

44

The process of drafting the EU-ASR (as recommended above) should incorporate a debate on how best to demarcate the respective scopes of this Regulation and the **GDPR**. A number of factors should be taken into account in this respect; firstly, algorithmic systems may pose specific risks to individuals and groups even if they do not involve the processing of personal data, and these risks may relate to assets, ownership, bodily integrity or discrimination. Secondly, the regulatory framework introduced for the future horizontal regulation of algorithmic systems may need to be more flexible and risk-adapted than the current data protection regime.

Instruments

45

The Data Ethics Commission recommends the introduction of a **mandatory labelling scheme** for algorithmic systems of enhanced criticality (Level 2 upwards). A mandatory scheme of this kind would oblige operators to make it clear whether (i.e. when and to what extent) algorithmic systems are being used. Regardless of system criticality, operators should always be obliged to comply with a mandatory labelling scheme if there is a risk of confusion between human and machine that might prove problematic from an ethical point of view.

46

An individual affected by a decision should be able to exercise his or her right to "meaningful **information** about the logic involved, as well as the scope and intended consequences" of an algorithmic system (cf. GDPR) not only in respect of fully automated systems, but also in situations that involve any kind of **profiling**, regardless of whether a decision is taken on this basis later down the line. The right should also be expanded in the future to apply to the algorithm-based decisions themselves, with differing levels of access to these decisions according to system criticality. These measures may require the clarification of certain legislative provisions or a widening of regulatory scope at European level.

47

It certain cases, it may be appropriate to ask the operator of an algorithmic system to provide an **individual explanation** of the decision taken, in addition to a general explanation of the logic (procedure) and scope of the system. The main objective should be to provide individuals who are affected by a decision with comprehensible, relevant and concrete information. The Data Ethics Commission therefore welcomes the work being carried out under the banner of "Explainable AI" (efforts to improve the explainability of algorithmic systems, in particular self-learning systems), and recommends that the Federal Government should fund further research and development in this area.

48

In view of the fact that, in certain sectors, society as a whole may be affected as well as its individual members, also particular **parties who are not individually affected** by an algorithmic system should be entitled to access certain types of information about it. It is likely that rights of this kind would be granted primarily for journalistic and research purposes; in order to take due account of the operator's interests, they would need to be accompanied by adequate protective measures. The Data Ethics Commission believes that consideration should also be given to the granting of unconditional rights to access information in certain circumstances, in particular when algorithmic systems with serious potential for harm (Level 4) are used by the State.

49

It is appropriate and reasonable to impose a legal requirement for the operators of algorithmic systems with at least some potential for harm (Level 2 upwards) to produce and publish a proper **risk assessment**; an assessment of this kind should also cover the processing of non-personal data, as well as risks that do not fall under the heading of data protection. In particular, it should appraise the risks posed in respect of self-determination, privacy, bodily integrity, personal integrity, assets, ownership and discrimination. It should encompass not only the underlying data and logic of the model, but also methods for gauging the quality and fairness of the data and the model accuracy, for example the bias or the rates of (statistical) error (overall or for certain sub-groups) exhibited by a system during forecasting/category formation.

50

To provide controllers and processors with greater legal clarity, further work must be done in terms of fleshing out the requirements to **document and log** the data sets and models used, the level of granularity, the retention periods and the intended purposes. In addition, operators of sensitive applications should be obliged in future to document and log the program runs of software that may cause lasting harm. The data sets and models used should be described in such a way that they are comprehensible to the employees of supervisory institutions carrying out oversight measures (as regards the origin of the data sets or the way in which they are pre-processed, for example, or the optimisation goals pursued using the models).

51

System operators should be required by the standard-setting body to guarantee a minimum level of **quality, from both a technical and a mathematical-procedural perspective**. The procedural criteria imposed must ensure that algorithmically derived results are obtained in a correct and lawful manner. For this purpose, quality criteria could be imposed, in particular as regards corrective and control mechanisms, data quality and system security. For example, it would be appropriate to impose quality criteria on the relationship between algorithmic data processing outcomes and the data used to obtain these outcomes.

52

The Data Ethics Commission believes that a necessary first step is to clarify and flesh out in greater detail the scope and legal consequences of Article 22 GDPR in relation to the use of algorithmic systems in the context of human decision-making. As a second step, the Data Ethics Commission recommends the introduction of additional **protective mechanisms for algorithm-based and algorithm-driven decision-making systems**, since the influence of these systems in real-life settings may be almost as significant as that of algorithm-determined applications. The prohibitory principle followed to date by Article 22 GDPR should be replaced by a more flexible and risk-adapted regulatory framework that provides adequate guarantees as regards the protection of individuals (in particular where profiling is concerned) and options for these individuals to take action if mistakes are made or if their rights are jeopardised.

53

Consideration should be given to expanding the **scope of anti-discrimination legislation** to cover specific situations in which an individual is discriminated against on the basis of automated data analysis or an automated decision-making procedure. In addition, the legislator should take effective steps to prevent **discrimination on the basis of group characteristics** which do not in themselves qualify as protected characteristics under law, and where the discrimination often does not currently qualify as indirect discrimination on the basis of a protected characteristic.

54

In the case of algorithmic systems with regular or significant (Level 3) or even serious potential for harm (Level 4), it would be useful – as a supplement to the existing regulations – for these systems to be covered by **licensing procedures or preliminary checks** carried out by supervisory institutions, in the interests of preventing harm to individuals who are affected, certain sections of the population or society as a whole.

Institutions

55

The Data Ethics Commission recommends that the Federal Government should expand and realign the competencies of existing supervisory institutions and structures and, where necessary, set up new ones. Official supervisory tasks and powers should primarily be entrusted to the **sectoral supervisory authorities** that have already built up a wealth of expert knowledge in the relevant sector. Ensuring that the competent authorities have the financial, human and technical **resources** they need is a particularly important factor in this respect.

56

The Data Ethics Commission also recommends that the Federal Government should set up a **national centre of competence for algorithmic systems**; this centre should act as a repository of technical and regulatory expertise and assist the sectoral supervisory authorities in their task of monitoring algorithmic systems to ensure compliance with the law.

57

The Data Ethics Commission believes that initiatives involving the development of technical and statistical **quality standards for test procedures and audits** (differentiated according to critical application areas if necessary) are worthy of support. Test procedures of this kind – provided that they are designed to be adequately meaningful, reliable and secure – may make a vital contribution to the future auditability of algorithmic systems.

58

In the opinion of the Data Ethics Commission, particular attention should be paid to innovative forms of **co-regulation and self-regulation**, alongside and as a complement to forms of state regulation. It recommends that the Federal Government should examine various models of co-regulation and self-regulation as a potentially useful solution in certain situations.

59

The Data Ethics Commission believes that an option worth considering might be to require operators by law (inspired by the "comply or explain" regulatory model) to sign a declaration confirming their willingness to comply with an **Algorithmic Accountability Code**. An independent commission with equal representation – which must be free of state influence – could be set up to develop a code of this kind, which would apply on a binding basis to the operators of algorithmic systems. Appropriate involvement of civil society representatives in the drafting of this code must be guaranteed.

60

Voluntary or mandatory evidence of protective measures in the form of a specific **quality seal** may also serve as a guarantee to consumers that the algorithmic system in question is reliable, while at the same time providing an incentive for developers and operators to develop and use reliable systems.

61

The Data Ethics Commission takes the view that companies and authorities operating critical algorithmic systems should be obliged in future to appoint a **contact person**, in the same way that companies of a specific size are currently obliged to appoint a data protection officer. Communications with the authorities should be routed through this contact person, and he or she should also be subject to a duty of cooperation.

62

To ensure that official audits of algorithmic systems take due account of the interests of civil society and any companies affected, suitable **advisory boards should be set up within the sectoral supervisory authorities**.

63

In the opinion of the Data Ethics Commission, technical standards adopted by **accredited standardisation organisations** are a generally useful measure, occupying an intermediate position between state regulation and purely private self-regulation. It therefore recommends that the Federal Government should engage in appropriate efforts towards the development and adoption of such standards.

64

The system of granting **competitors, competition associations or consumer associations the right to file an action** has been an important feature of the German legal landscape for many years, and could play a key role in civil society oversight of the use of algorithmic systems. In particular, private rights of this kind could allow civil society players with a legitimate mandate to enforce compliance with legal provisions in the area of contract law, fair trading law or anti-discrimination law, without needing to rely on the authorities to take action and without needing to wait for individuals to authorise them.

Special topic: Algorithmic systems used by media intermediaries

65

Given the specific risks posed by media intermediaries that act as **gatekeepers to democracy**, the Data Ethics Commission recommends that options should be examined for countering these risks, also with regard to influencing EU legislation (→ see Recommendation 43 above). A whole gamut of risk mitigation measures should be considered, extending through to ex-ante controls (e.g. in the form of a licensing procedure).

66

The national legislator is under a constitutional obligation to protect the democratic system from the dangers to the free, democratic and pluralistic formation of opinions that may be created by providers that act as gatekeepers by establishing a binding normative framework for **media**. The Data Ethics Commission believes that the small number of operators concerned should be obliged to use algorithmic systems that allow users (at least as an additional option) to access an unbiased and balanced selection of posts and information that embodies pluralism of opinion.

67

The Federal Government should consider measures that take due account of the risks typically encountered in the media sector in respect of all media intermediaries and also in respect of providers that do not act as gatekeepers or whose systems are associated with a lower potential for harm. These measures might include mechanisms for **enhancing transparency** (for example by ensuring that information is available about the technical procedures used to select and rank news stories, **introducing labelling obligations for social bots**) and establishing a right to post countering responses on timelines.

Use of algorithmic systems by state bodies

68

The State must, in the interests of its citizens, make use of the best available technologies, including algorithmic systems, but must also exercise particular prudence in all of its actions in view of its obligation to preserve fundamental rights and act as a role model. As a general rule, therefore, the use of algorithmic systems by public authorities should be assessed on the basis of the criticality model as **particularly sensitive**, entailing at the very least a comprehensive risk assessment.

69

In the areas of **law-making** and the **dispensation of justice**, algorithmic systems may at most be used for peripheral tasks. In particular, algorithmic systems must not be used to undermine the functional independence of the courts or the democratic process. By way of contrast, enormous potential exists for the use of algorithmic systems in connection with **administrative** tasks, in particular those relating to the provision of services and benefits. The legislator should take due account of this fact by giving the green light to a greater number of partially and fully automated administrative procedures. Cautious consideration should therefore be given to expanding the scope of both Section 35a of the German Administrative Procedures Act (*Verwaltungsverfahrensgesetz*, VwVfG) (which is couched in overly restrictive terms) and the corresponding provisions of statutory law. All of these measures must be accompanied by adequate steps to protect citizens.

70

Decisions taken by the State on the basis of algorithmic systems must still be **transparent**, and it must still be possible to provide **justifications** for them. It may be necessary to clarify or expand the existing legislation on freedom of information and transparency in order to achieve these goals. Furthermore, the use of algorithmic systems does not negate the principle that decisions made by public authorities must generally be justified individually; on the contrary, this principle may impose limits on the use of overly complex algorithmic systems. Finally, greater priority should be accorded to open-source solutions, since the latter may significantly enhance the transparency of government actions.

71

From an ethical point of view, there is no general right to non-compliance with rules and regulations. At the same time, however, automated "total" enforcement of the law raises a number of different ethical concerns. As a general rule, therefore, systems should be designed in such a way that a human can override **technical enforcement** in a specific case. The balance struck between the potential transgression and the automated (and perhaps preventive) enforcement measure must at all times meet the requirements of the proportionality principle.

Liability for algorithmic systems

72

Liability for damages, alongside criminal responsibility and administrative sanctions, is a vital component of any ethically sound regulatory framework for algorithmic systems. It is already apparent today that algorithmic systems pose challenges to liability law as it currently stands, *inter alia* because of the complexity and dynamism of these systems and their growing "autonomy". The Data Ethics Commission therefore recommends that the current provisions of liability law should undergo in-depth checks and (where necessary) revisions. The scope of these checks and revisions should not be restricted on the basis of too narrowly defined technological features, such as machine learning or artificial intelligence.

73

The proposal for a future system under which legal personality would be granted to high-autonomy algorithmic systems, and the systems themselves would be liable for damages (**"electronic person"**), should **not be pursued further**. As far as this concept is, by some protagonists, based on a purported equivalence between human and machine it is ethically indefensible. And as far as it boils down to introducing a new type of company under company law it does not, in fact, solve any of the pertinent problems.

74

By way of contrast, if harm is caused by autonomous technology used in a way functionally equivalent to the employment of human auxiliaries, the operator's liability for making use of the technology should correspond to the otherwise existing vicarious **liability regime of a principal for such auxiliaries** (cf. in particular Section 278 of the German Civil Code). For example, a bank that uses an autonomous system to check the creditworthiness of its customers should be liable towards them to at least the same extent that it would be had it used a human employee to perform this task.

75

As the debate currently stands, it appears highly likely that appropriate amendments will need to be made to the **Product Liability Directive** (which dates back to the 1980s), and a connection established to new product safety standards; in addition, certain changes may need to be made to the rules relating to **fault-based liability** and/or new bases of **strict liability** may need to be introduced. In each case, it will be necessary to determine the liability regime that is most appropriate for particular types of products, digital content and digital services, and the exact shape that this regime should take (once again depending on the criticality of the relevant algorithmic system). Consideration should also be given to innovative liability concepts currently being developed at European level.

4

A European path

The Data Ethics Commission examined a great many different questions in the course of its work, and discussions on these questions have raised new ones in turn; this alone should serve to indicate that this Opinion can serve only as one out of many building blocks in the larger edifice of a **debate on ethics, law and technology** that will continue for many years to come. The Data Ethics Commission takes the view that it is important to remember that ethics, law and democracy must serve as a shaping force for change, both in the broader sense and more specifically in the field of technology. To achieve this goal, interdisciplinary discourse in politics and society is required, and care must be taken to ensure that any rules and regulations adopted are open enough to retain their regulatory clout and their ability to adapt, even in the face of fast-paced changes to technologies and business models. These rules and regulations must be enforced effectively by means of appropriate instruments, procedures and structures, and these latter must make it possible to intervene promptly in response to infringements or undesirable developments.

In the global contest for future technologies, Germany and Europe are being confronted with value systems, models of society and cultures that differ widely from our own. The Data Ethics Commission supports the **"European path"** that has been followed to date: the defining feature of European technologies should be their consistent alignment with European values and fundamental rights, in particular those enshrined in the European Union's Charter of Fundamental Rights and the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms.

The Data Ethics Commission believes that the State has a particular responsibility to develop and enforce ethical benchmarks for the digital sphere that reflect this value system. In order to deliver on this promise to citizens, it must act from a position of political and economic strength on the global stage; excessive dependence on others turns a nation into a rule taker rather than a rule maker, resulting in the citizens of this nation being subject to requirements imposed by players elsewhere in the world, or by private corporations that are, for the most part, exempt from democratic legitimacy and oversight. Embarking on **efforts to safeguard the digital sovereignty of Germany and Europe in the long term** is therefore not only a politically far-sighted necessity, but also an expression of ethical responsibility.

Members of the Data Ethics Commission

Co-Spokespersons

Prof. Dr Christiane Wendehorst

- Professor of Civil Law at the University of Vienna
- Co-Head of the Department of Innovation and Digitalisation in Law at the University of Vienna
- President of the European Law Institute (ELI)

Prof. Dr Christiane Woopen

- Professor for Ethics and Theory of Medicine and Head of the Research Unit Ethics at the University Clinic of Cologne
- Executive Director of the Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres) at the University of Cologne
- Chair of the European Group on Ethics in Science and New Technologies (EGE)

Members

Prof. Dr Johanna Haberer

- Professor of Christian Media Studies at Friedrich Alexander University Erlangen Nuremberg (FAU)
- Director of the Institute for Practical Theology at Friedrich Alexander University Erlangen Nuremberg (FAU)

Prof. Dr Dirk Heckmann

- Full Professor of Law and Security of Digitization at the Technical University of Munich (TUM)
- Director at the Bavarian Research Institute for Digital Transformation
- Judge at the Bavarian Constitutional Court

Marit Hansen

- Data Protection Commissioner of Land Schleswig-Holstein
- Head of Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Independent Centre for Privacy Protection Schleswig-Holstein)

Prof. Ulrich Kelber

- Federal Commissioner for Data Protection and Freedom of Information
- Honorary Professor at Bonn-Rhein-Sieg University of Applied Sciences (H-BRS)

Prof. Dieter Kempf

- President of the Federation of German Industries (BDI)
- Honorary Professor at Friedrich Alexander University Erlangen Nuremberg (FAU)

Prof. Dr Mario Martini

- Professor of Public Administration, Public Law, Administrative Law and European Law at the German University of Administrative Sciences Speyer (DUV Speyer)
- Head of the Programme Area "Transformation of the State in the Digital Age" and Deputy Director of the German Research Institute for Public Administration (FÖV)

Klaus Müller

- Executive Director of the Federation of German Consumer Organisations (vzbv)
- Lecturer at Heinrich Heine University Düsseldorf (HHU)

Paul Nemitz

- Principle Advisor at the European Commission, Directorate-General for Justice and Consumers

Prof. Dr Sabine Sachweh

- Professor for Applied Software Engineering at Dortmund University of Applied Sciences and Arts (FH Dortmund)
- Spokesperson and Board Member of the Institute for the Digital Transformation of Application and Living Domains (IDiAL) at Dortmund University of Applied Sciences and Arts (FH Dortmund)
- Co-Spokesperson of the "Digitalisation and Education for the Elderly" Advisory Council at the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth

Christin Schäfer

- Founder and Managing Director of the company acs plus, a data science boutique
- Advisor of the Big Data Analytics Research Group at the German Economic Institute in Cologne (IW Köln)

Prof. Dr Rolf Schwartmann

- Professor of Civil Law and Economic Law at Cologne University of Applied Sciences (TH Köln)
- Head of the Research Centre for Media Law at Cologne University of Applied Sciences (TH Köln)
- Chairman of the German Association for Data Protection and Data Security (GDD)

Prof. Dr Judith Simon

- Professor for Ethics in Information Technology at the University of Hamburg (UHH)

Prof. Dr Wolfgang Wahlster

- Professor of Computer Science, Chair for Artificial Intelligence, Saarland University
- CEO/CEA of the German Research Center for Artificial Intelligence (DFKI)
- Head of the Steering Committee for the AI Standardisation Roadmap at the German Institute for Standardization (DIN)

Prof. Dr Thomas Wischmeyer

- Assistant Professor (Tenure Track) for Public Law and Information Law at the University of Bielefeld

Current as of: 10 October 2019

Imprint

Berlin, October 2019

Opinion of the Data Ethics Commission

Publisher
Data Ethics Commission of the Federal Government
Federal Ministry of the Interior, Building and Community
Alt-Moabit 140, 10557 Berlin
Federal Ministry of Justice and Consumer Protection
Mohrenstraße 37, 10117 Berlin

E-mail
datenethikkommission_gs@bmi.bund.de
datenethikkommission_gs@bmjv.bund.de

Website
www.datenethikkommission.de

Design
Atelier Hauer + Dörfler GmbH, Berlin

Photo credits
p. 28: BMI (group photo), Studio Wilke (Christiane Wendehorst), Reiner Zensen (Christiane Woopen), BPA/Kugler (Ulrich Kelber)
p. 29: Christian Kruppa (Dieter Kempf), vzbv/Gert Baumbach (Klaus Müller), Markus Mielek (Sabine Sachweh),TH Köln/Schmülgen (Rolf Schwartmann), UHH/Nicolai (Judith Simon), Jim Rakete (Wolfgang Wahlster)

Printing
Brandenburgische Universitätsdruckerei und Verlags-gesellschaft Potsdam mbH (bud)

The full version of the Opinion can be downloaded from **www.datenethikkommission.de**.