Opinion of the German Data Ethics Commission

Christiane Wendehorst
Co-Chair of the Data Ethics Commission
Data Ethics Commission

- Established in mid 2018 with the mission to develop, within one year, an ethical and regulatory framework for data, ADM and AI
- Co-chaired by Christiane Wendehorst and Christiane Woopen
- Opinion presented in Berlin on 23 October 2019
- Includes ethical guidelines and 75 concrete recommendations for action regarding data and algorithmic systems
What is Data Ethics?

Data

Ethics of handling personal data

Ethics of handling data in general (including non-personal data)

Ethics of handling data and data-driven technologies (including algorithmic systems, such as AI)

Ethics of the digital transformation in general (including issues such as the platform economy or the future of work)

Data-driven technologies (such as AI)

Wider framework
Introduction
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.
General ethical principles
General ethical principles

Human dignity
Autonomy
Privacy
Security
Democracy
Justice and Solidarity
Sustainability
Technological Foundations
• Main mission to ‘de-mystify’ the technology and do away with popular misconceptions that may be inspired by science fiction rather than by science

• Not everything that may be considered ‘data’ is useful, ‘data quality’ is not absolute but relative (dependent on the concrete purpose), …

• Not useful to quarrel about the proper definition of ‘Artificial Intelligence’, ethical and legal implications may follow more from the existence of an ‘algorithmic system’ rather than on how the algorithms are created
Multi-Level-Governance of Digital Ecosystems
Education and Upskilling

Corporate Governance

Ethics-by-Design

Getting Civil Society involved

Regulation, Co- and Self-Regulation

Fostering R&D
Data perspective and algorithms perspective

Data rights and data obligations

Requirements for algorithmic systems
Data
Data Governance Principles

• In line with the Principles under Article 5 of the GDPR, but apply to personal as well as non-personal data

• Stress the potential of data use and data sharing for the common good

• Recognise that there may, under certain circumstances, also be an ethical imperative to use data
Data rights and corresponding data obligations

- Rights vis-à-vis a controller of data, aimed at access, desistance, rectification or at receiving an economic share
- Inspired by ALI-ELI Principles
- No plea for “data ownership”
- Data subjects’ rights under the GDPR as a particularly important manifestation
Ethical imperatives to use data

Illustration:

A hospital is experiencing an outbreak of a multi-resistant pathogen. It wants to analyse the health data of patients who have recently become infected, as a basis for pinpointing the inpatients that might benefit most from a move to another hospital. Under these circumstances, the hospital has a general obligation to provide new patients with the best possible protection against infection by taking all available and reasonable precautions to this end. This may include the use of health data belonging to patients who have already been infected.
Rights to require desistance from data use

Illustration:

The non-personal data collected by sensors in modern agricultural machinery (relating to soil quality, weather, etc.) are used by manufacturers as a basis for many of the services they provide (precision farming, predictive maintenance, etc.). If the manufacturers were to forward these data to potential investors or lessors of land, however, the latter would be given information that might prove harmful to a farmer if negotiations over the land were to take place in the future.
Rights to request access to data

Illustrations:

A smart tractor has been damaged in an accident. The manufacturer’s authorized repair shop offers repair only at a very high price. In order for the farmer to have a second opinion from an independent repair shop, access to data about the tractor held by the manufacturer would be required.

A supplier manufactures the engines for the tractors. It would be extremely useful for the supplier to have access to certain tractor data so that it can verify and constantly improve the quality of its engines. These data are stored in the manufacturer’s cloud, however, and the latter is unwilling to allow the supplier to access them.
Standards for the Use of Personal Data

• Recommendations for **measures against ethically indefensible uses of data and against the existing enforcement gap**, including by fleshing out and strengthening the existing legal framework (e.g. concerning **profiling and trade in data**)

• Recommendations with regard to **specific contexts**: data as “counter-performance”, personalised risk assessment, digital inheritance

• Recommendations with regard to specific groups of data subjects: **employees, patients, minors, vulnerable adults**

• Better implementation of privacy by design
Improving controlled access to personal data

• Better legal certainty for researchers (clarification and harmonisation of the law, innovative forms of consent, etc.)
• Fostering progress with anonymisation, pseudonymisation and synthetic data
• Innovative data management and data trust schemes as the way forward
• Duty to provide for interoperability/interconnectivity in particular sectors (by way of asymmetrical regulation)
Debates around access to non-personal data

- **ASISA-Principle** (*Awareness – Skills – Infrastructures – Stocks – Access*): Investing in awareness raising, data infrastructures, and practical support
- Cautious adaptations of the current legislative framework (*limited third party effects of data contracts, facilitating data pooling, rights in co-generated data etc*) and possibly further legislative measures
- Fostering **open data in the public sector** (open government data) while improving protection of third parties
- Open data in the private sector: incentives for **voluntary data sharing**, cautious approach to statutory duties, mainly on a sector-by-sector basis
Algorithmic Systems
Algorithmic Systems

• AI only as a subset of algorithmic systems

• Differentiation of algorithm-based, -driven and -determined decisions

• General requirements for algorithmic systems
A risk-based regulatory framework

• „Criticality pyramid“: different levels of potential for harm (risk)

• No need for any regulation with regard to most algorithmic systems

• Ban on systems involving an untenable potential for harm
No need for any additional regulation with regard to the vast majority of algorithmic systems

Illustration for level 1: The algorithms used in a drinks vending machine do have a certain potential for harm, since a user could, for example, not receive any goods and lose his or her money. However, this potential for harm does not exceed the threshold for specific potential for harm within the algorithm context. It is sufficient here to rely on the general mechanisms which oblige contractual partners to fulfil their contractually undertaken performance obligations or manufacturers to produce devices which function properly.
Illustration for level 2: Dynamic pricing (for example based on the criteria of supply and demand) in e-commerce, which however does not involve any personalised pricing, for the most part has a low potential for harm but one which does exceed the relevance threshold, for example concerning covert discrimination.

Illustration for level 3: Algorithms for setting personalised prices (i.e. setting a price based on criteria which are tailored to the individual customer and usually estimate their maximum personal willingness to pay) involve appreciable potential for harm, for example concerning the discrimination of particularly vulnerable groups. At best, it should be possible to use them only after they have undergone a licensing procedure.

Illustration for level 4: Algorithmic systems, for example of players with huge market power, which are used to determine the creditworthiness of an individual consumer or company must be classified as Level 4. Whether a person receives a loan or not can have a decisive bearing on that person’s fate. The high level of system criticality is also justified by the market concentration with few providers and the tendency for a lender to rely on the judgment of a particular player.
Illustration: Lethal autonomous weapons are often seen as a “red line”, as machines should not be allowed to kill people. However, that can apply only on the basis that they are algorithm-determined killings. Where lethal autonomous weapons simply provide human soldiers with support in recognising objects or are merely used to keep a missile on track in the face of crosswinds, an ethical “red line” is not being crossed.
A risk-based regulatory framework

- Horizontal Regulation at EU level and sector specific legislation at both EU and national levels
Instruments

Depending on the level of criticality:

- **Labelling** requirements, **information** duties, and duties to **explain**
- **Risk assessment**, documentation and logging
- Ensuring **quality** from a technical and mathematical-procedural perspective
- Ex-post control – **licensing** procedures – continuous audits up to ‘always on’ **oversight** via a live interface
- Individual protection even below the level of Article 22 GDPR
- Rethinking **anti-discrimination law**
Institutions

- **Sectoral supervisory** authorities should normally be in charge (but be better equipped, and have advisory councils representing civil society and a diverse range of players)
- Support to be provided by **national centre of competence at federal level**
- Technical standards, **co-regulation and self-regulation**
- **Algorithmic Accountability Codex**
- **Quality seals**
- **Contact persons** in companies and government authorities
- Rights to file an action on the part of competitors and consumer organisations
Algorithmic systems used by media intermediaries

- Enhanced responsibilities on the part of media intermediaries functioning as ‘gatekeepers to democracy’
- Need for a binding normative framework for the media, including the obligation of ‘gatekeepers’ to offer an alternative channel with a balanced and unbiased portfolio of news items etc
- Labelling duties with regard to social bots and other measurers to enhance transparency
Use of algorithmic systems by state bodies

• Particular sensitivity and **enhanced criticality**
• Different situation for **law-making and dispensation of justice** on the one hand and **administration** on the other
• **Transparency and explainability** requirements
• Ethical and legal **limits to automated ‘total’ enforcement**
Liability for algorithmic systems

• Existing liability regimes need a ‘digital fitness check’ and may have to be reconsidered
• No recognition of ‘electronic personhood’
• Operators’ liability along the lines of vicarious liability of principals for their auxiliaries
A European Path
A European path

• Data Ethics Commission supports the ‘European path’ of consistent alignment of technology with European values and fundamental rights

• Data Ethics Commission sees efforts to ensure Europe’s ‘digital sovereignty’ as part of European leaders’ ethical responsibility
Opinion of the
German Data Ethics Commission

Christiane Wendehorst
Co-Chair of the Data Ethics Commission