Digital Society
https://doi.org/10.1007/s44206-024-00101-6

ORIGINAL PAPER

Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies

Damian Eke[1] · Bernd Stahl[1]

Received: 20 June 2023 / Accepted: 26 February 2024

Abstract

Addressing ethical concerns is among the fundamental motivations for the development of policies and regulations for data and digital technologies. In the last few years, the European Commission has issued a number of policies, regulations and legislative proposals for socially desirable and legally compliant data governance for technologies which have ethical implications. What is not obvious, however, is whether and in what way ethics are included explicitly in the way these policies and regulations are created and implemented to address data governance challenges. Given the increasing amount of available digital data, its use for AI and other purposes and the growing amount of regulatory activity around data, this paper explores the role ethics plays in these documents. We examined eight of these documents to map the ethical concerns and justifications underlining their provisions, the ethical principles they promote and the implementation approaches recommended. Our analysis shows that the current EU data governance policy landscape can be read from an ethical perspective as being grounded in ethical thinking, typically expressed in terms of human rights, aware of likely concerns, based on well-established principles and in the process of being codified in regulation, legislation and institutions. However, the practical implementation of these principles, for instance how conflicts among these principles can be resolved, remain unclear.

Keywords Data governance · Ethics · Technology · EU data regulations · Human rights

✉ Damian Eke
damian.eke@nottingham.ac.uk

[1] School of Computer Science, University of Nottingham, Nottingham, UK

Published online: 04 March 2024

1 Introduction

On 9 March 2021, the European Commission presented visions outlining the pathway to Europe's digital transformation by 2030 in line with the EU's values. The overall goal of this policy programme as stated in its Explanatory Memorandum is to reinforce the EU's digital leadership and promote human centred, inclusive and sustainable digital policies empowering citizens and businesses (Proposal for a DECISION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Establishing the 2030 Policy Programme "Path to the Digital Decade", 2021). In addition to this the Commission proposed an inter-institutional solemn declaration on digital rights and principles for the digital decade (European Commission, 2022). This is a proposal to ensure that the EU's digital transformation puts people and their rights at the centre, supports solidarity and inclusion, increases safety, security and empowers individuals, fosters citizens participation, ensures freedom and promotes sustainability. Underlying the EU's digital strategy are proposed regulations and a strong commitment to be consistent with existing policy and regulatory provisions (such as 2019 Strategy for Shaping Europe's digital future, the Data Governance Act, the Digital Services Act, the GDPR, the Digital Markets Act and the Cybersecurity Strategy).

These policy and regulatory documents are set to shape the foundations of responsible data governance for digital technologies in Europe. All digital technologies rely on digital data. Data is processed by these technologies and is typically a result of this processing. Data to a large extent determines what digital technologies do and how they do it. Data is thus also important with regards to the ethical and social benefits of digital technologies as well as the issues, concerns and problems they raise. The importance of data in the digital age is hard to deny. It is recognised by organisations that rely on and make use of data as well as by governments, regulators and administrators who aim to ensure that data is used appropriately for purposes that are beneficial.

This paper analyses major policy and regulatory documents aimed at shaping the future of the EU's digital economy. The aim is to answer the question of which role ethics plays in current European digital policies and regulations and which wider ethical implications such regulations imply. As stakeholders explore ways of providing harmonised understanding of these policies and regulations and how it applies to their processes, it is critical to identify the ethical principles underlying them. By answering this question, we shed light on the broader context of ethics in data-related policies and regulations which is often hidden from sight because of the dense technical language of policy and regulation. It also provides an understanding of the role that data policies and regulations have in broader policy and political contexts. These questions are of academic interest for a range of disciplines that focus on data and digital technologies, ranging from computer science to information systems. They are also important for disciplines that are interested in the reflection of digital technologies, such as philosophy of technology and science and technology studies. In addition, the topic discussed in this paper is of high relevance to both theory and practise for different entities, disciplines and

innovations. A better understanding of the underlying ethical assumptions and implied ethical intentions of EU policy and regulation can help ensure consistency of different regulatory regimes and approaches and facilitate a more detailed debate about such topics. This paper acknowledges that non-EU policies and regulations shaped by different ethical justifications, values and principles may likely affect data sharing from the EU. However, the focus of this paper is the EU data ecosystem and the policies and regulations shaping it. The justification of this focus on the EU is its strong emphasis on values and the fact that it is often referred to as a "community of values" (see section on data and digital ethics in Europe, below. The (self-) perception of the EU as being value-driving calls for a scrutiny of the nature of those values and how they are embedded in legislation and regulation, thus rendering the EU a good subject for the investigation of underlying ethical aspects of data-related regulatory systems.

The article is organised as follows. We begin with a brief overview of the academic discussion of data and digital ethics that highlights some of the key topics and issues of the field. This introduction sets the scene for an outline of the chosen methodology of a structured reading of current policy and regulation. Our findings are described in the subsequent section which provides the basis for the discussion. We conclude by highlighting key insights and suggesting how these ideas can be taken further.

2 Data and Digital Ethics in Europe

Given our interest in the ethics of data as expressed or implied in EU policy and regulation, we start with an introduction of the key concepts. This will include a brief overview of data and digital ethics which is then followed by a discussion of the relationship between ethics and human rights.

2.1 Data and Digital Ethics

The discussion of the ethical aspects of digital technologies is almost as old as these technologies themselves (Weizenbaum, 1977; Wiener, 1954). The increasing capabilities of these technologies have changed possible concerns over time and the academic discourse has developed accordingly (Dreyfus, 1972, 1992). By the 1980s digital technologies had developed to the point where their societal importance warranted a recognisable field or discourse. Ethical issues of these technologies were discussed under headings such as computer ethics (Bynum, 2010), information ethics (Floridi, 1999), or cyberethics (Baird et al., 2000). The increasing use of digital technologies for personal purposes, notably in the form of social networks, led to another wave of concerns. Most recently the success and expected impact of artificial intelligence (AI) technologies (particularly generative AI systems) have further boosted the visibility of the topic and size of the discourse (Coeckelbergh, 2020; Dignum, 2019; Eke, 2023; Stahl & Eke, 2024).

While the content of these various streams of the discussion of ethics of digital technologies has been informed by technical capabilities, one can observe

a significant amount of consistency across discourses, e.g. in the case of computer ethics and ethics of AI (Stahl, 2021). A systematic review of the literature published between 2003 and 2012 on the ethics of digital technologies (Stahl et al., 2016) showed a remarkable amount of continuity in terms of topics raised, theoretical approaches and possible solutions. The issues identified in this study can provide a good starting point for this article, as they have been validated as having a high level of visibility for at least a decade and can be hypothesised to retain their relevance until now. The top 10 issues that were identified are: privacy, professionalism and work-related issues, autonomy, agency, trust, issues related to specific technologies, consent, identity, inclusion and digital divide, and security.

The recognition that many of these issues are directly related to data is not new and led to the development of discourse on 'data ethics' (Floridi & Taddeo, 2016; Metcalf et al., 2016; Zwitter, 2014). This discussion was driven by the phenomenon of 'big data' (Boyd & Crawford, 2012; Kitchin & McArdle, 2016) which promised new opportunities as well as new challenges. It currently appears that the discourse on data ethics was eclipsed by the discourse on ethics of AI. At its core, however, this is likely to be a relatively minor shift in terminology which has little relevance to the content of the debate. The reason for the ascendance of the ethics of AI debate was in particular the success of machine learning and most currently successful machine learning techniques require large data sets. It is widely accepted that the availability of big data sets was one of the preconditions of the success of AI (Bengio et al., 2021; Hall & Pesenti, 2017).

In parallel to the academic debate on the various manifestations of digital technology, the data they use and the ethical and social implications these can have, there has been an active policy debate. Without being able to engage in much detail with the complex question of the relationship between ethics, policy and the law, it is probably fair to say that ethical concerns were one of the main reasons why policymakers engaged with the topic of digital technology and, more recently data, to ensure that such issues are addressed in a suitable manner. The most visible ethical issue, namely privacy, has consequently had the most visible consequences in policy and law, namely data protection. Privacy as an ethical issue with legal implications can be traced back to the 19th century (Warren & Brandeis, 1890). Its translation into legally enforceable principles can be observed from the 1970s and formal data protection legislation has developed since the 1980s.

Our starting point is thus that ethical concerns are one cause of the development of policy and regulation. What is not obvious, however, is whether and in what way ethical concerns are included explicitly in the way policy and regulation are created and implemented. Given the increasing amount of available digital data, its use for AI and other purposes and the growing amount of regulatory activity around data, it is thus worth asking which role ethics plays in policy and regulation. We are particularly interested in the answer to this question from an EU perspective. This is motivated by the explicit moral claims that the EU upholds (the EU as being founded on values[1]) coupled with the various regulatory interventions concerning

[1] https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en.

data that the EU is currently proposing. We aim to answer this question by undertaking a discourse analysis of current regulatory texts and proposals as described in the following section.

2.2 Ethics and Human Rights in Technology

The European Union is sometimes referred to as a union of values. These are defined in the Treaty on the European Union (TEU).[2] Article 2 of the TEU states that

> The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.

These values are ethical values that are codified in the legal text of the TEU and elsewhere in the legal framework that governs the EU. The most prominent location where they are spelled out in more detail is the Charter of Fundamental Rights of the European Union.[3] This charter sits at the top of the hierarchy of EU legislations followed by 'ordinary legislations (Regulations and Directives). The European Declaration on Digital Rights and Principles for the Digital Decade 2022 reaffirms this by also declaring that "EU is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity".[4] Most importantly, this declaration was emphatic in amplifying key digital rights that need to be upheld as a way forward for the digital transformation in Europe. These include; the right to digital education, training and skills, to fair and just working conditions, to digital public services online, a fair, safe, protected, secure, and inclusive access to digital environment.

In this paper, it is important we offer some distinction between 'human rights' and 'Fundamental Rights'. Whereas fundamental rights and human rights show large overlaps in substance (they both protect rights to not to be discriminated against, freedom of expression, access to an independent or impartial court, privacy, and so forth), the terms are of a different origin, and more importantly, raise different bifurcations as to their applicability. Fundamental rights entail subjective rights which are accepted in a specific legal system and approved by that legal system's statutes. Fundamental rights and human rights diverge at the point where fundamental rights are specific to and can be invoked in a particular legal system by those to whom the law applies (e.g., citizen rights such as voting rights of the EU Charter can only be invoked by EU citizens; the right to privacy can be invoked by any person residing on EU territory). By contrast, human rights have world-wide acceptance and belong to all human beings—irrespective of for instance their nationality, race, gender, birth (e.g. the UN Charter of Human

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016M/TXT.
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.
[4] https://ec.europa.eu/newsroom/dae/redirection/document/94370.

Rights), or of where they reside. Mcgregor et al. (2019) have pointed out a number of situations where fundamental rights can be invoked in the application of algorithms.

From the perspective of an article that aims to look at ethical topics covered in legal and policy-related texts, this focus on constitutional and human rights law raises the question of the relationship between ethics and constitutional values including human rights. This is a difficult question that would call for a more detailed analysis of jurisprudential history than the current article can offer.

For the purposes of this article, it may suffice that we see ethics and human rights as distinct but complementary (World Economic Forum, 2019). Human rights typically refer to the role of citizens but also non-citizens within a society. Ethics is broader and can include questions that pertain only to a single individual with no relevance to anybody else, just as it can cover the distant future, neither of which tend to be the subject of human rights. In addition, ethics has various different layers, not all of which are visible in human rights. Ethics covers questions of good or bad, right or wrong on different levels. This starts with the individual act, thought or intention which can be deemed to be good or bad. Ethics also looks at the rules according to which such judgments can be made. On the next level of abstract, ethics explores the justifications that can be used to develop or review these rules. This is the level where much academic philosophical ethics is discussed (Stahl, 2012). A key characteristic of ethics is that much of it is contested. There are few moral certainties about what is right and wrong or which theoretical approaches can provide the best perspective on ethical questions.

Human rights have different characteristics. They are substantive, which means that they define certain rights which people have or ought to have, such as the right to life, freedom of expression, respect for privacy, right to education and many more. Human rights law does not tend to worry about the provenance of these rights but focuses on their definition and offers established mechanisms of enforcing them.

One can thus interpret human rights as a (temporary) agreement on the (moral) rights enshrined in the relevant document, notably the UN's Declaration of Human Rights or the EU's Charter of Fundamental Rights. This status has advantages from the perspective of people seeking to find appropriate ways of dealing with technology that potentially raise ethical concerns. One key advantage is that human rights are well-described and established and therefore do not require their development from first principles. In addition, human rights are embedded in legal systems and can be enforced through existing structures.

This may explain why much recent work on ethics of technology relies heavily on human rights as the fundamental normative basis. A good example with strong links to data governance is the ethics of AI debate. Much of this is framed in terms of the impact of AI on human rights (Access Now, 2018; Fjeld et al., 2020; Latonero, 2018). This approach is heavily adopted by political bodies that look at potential regulation and legislation of technology, such as the Council of the European Union (2020) and the European Commission (2021) but also by other international bodies such as the United Nations (Guterres, 2020), UNESCO (2020) or the OECD (2019).

The conclusions one can draw from this brief discussion of the relationship of ethics and human rights for this article is that human rights can be included in any discussion of ethical questions but that ethics is potentially broader and may cover questions such as the justification of ethical positions that are less obviously covered in human rights discourses. Having clarified this point, we are now in a position to explain how we undertook the analysis of recent European initiatives on data governance.

3 Methodology

In order to come to a better understanding of the role of ethics in current EU data governance-related policies and regulations, we first had to identify which policies currently exist that relate to data. We decided to focus on those initiatives that are already well developed and where there is either existing European legislation or manifest proposals for legislation. We started from the International Association of Privacy Professionals overview of current data initiatives.[5] We furthermore remained open to ongoing discussions of EU data governance policy, by scanning media and public data governance discussions. As a result of these scanning exercises, we identified the following documents that were analysed in detail:

EU governance document	Type	Status
EU General Data Protection Regulation (GDPR)	Regulations	Applies since 25 May 2018
EU Strategy for Data (SfD)	Policy	In operation
EU Data Governance Act (DGA)	Regulation	applicable across the EU from 24 September 2023
EU Data Act (DA)	Regulation	Applicable from early to mid- 2025
EU e-Privacy Directive (ePD)	Directive	Adopted in 2002 and revised in 2009
EU Cybersecurity Strategy for the Digital Decade (CS)	Policy	In operation
EU Digital Markets Act (DMA)	Regulation	Applicable from May 2023
EU Digital Services Act (DSA)	Regulation	Came into effect on 25 August 2023, for very large online platforms and very large online search engines. It becomes fully applicable to other entities on 17 February 2024.

The analysis aimed to identify the role of ethics in these documents. This included obvious and explicit references to ethics but also less obvious and implicit uses of ethical concepts or ideas. We therefore made use of thematic analysis, a widely-used approach to analysing qualitative data (Aronson, 1995; Braun & Clarke, 2006; Miles & Huberman, 1994). We used NVivo (server version 12) as a software tool to implement the analysis

We started out the thematic analysis by identifying the main analysis topics which were defined as top level nodes. These were ‘ethical concerns’ which

[5] https://iapp.org/media/pdf/resource_center/recent_eu_data_initiatives_in_context_infographic.pdf.

captured ethics-related reasons for developing and implementing data governance policies and regulations. Secondly, we defined 'ethical justifications' to capture those references to ethics that provide the overall rationale for instituting the policy. Thirdly, we defined a node called 'implementation' where we collected ethics-related aspects of implementing policies. Fourthly, we tried to identify specific ethical positions in a node named 'principles'. And, finally, we defined a node on 'recommendations' where we collected ethics-related practical implications of the policy. This initial top list of nodes developed during the analysis process. Where clearly identifiable themes emerged from the data or where we identified topics, concepts and concerns that play a visible role in the broader discourse, we created sub-nodes. For example, we created codes such as 'fairness' or 'consent' as sub-nodes under 'principles' or 'fraudulent practices' and 'general risks to rights and freedoms' as sub-nodes under 'ethical concerns'.

All coding was undertaken by the first author with the second author reviewing the coding progress and development of the coding structure. This approach to data analysis led to the following findings.

4 Findings

The empirical analysis of the eight major EU data-related documents provides insights that we now present. First, we present the ethical justifications given as the underlying rationale for the creation of these data governance documents. Part of this is related to a number of identified ethical concerns evident in the documents. Then we discuss the ethical principles promoted by these documents shaped mainly by EU socio-cultural contexts, expectations, interests and narratives. Finally, we present a number of implementation approaches that align with ethical considerations.

4.1 Ethical Concerns and Justifications

These data governance documents pointed out a number of ethical concerns that needed to be addressed. For instance, the overall intention is to use these governance mechanisms to address socio-cultural, economic, legal and technical concerns. Some of these ethical concerns include the evident discriminatory effects of digital data processing. As the EU strategy for data (section 4) observed; "*since increasingly large amounts of data are generated by consumers when they use IoT devices and digital services, consumers may be faced with risks of discrimination, unfair practices and lock-in effects*". This is directly related to critical risks to human rights and freedoms as recognised in the EU GDPR that large scale data processing particularly via technologies may result in discriminatory effects (GDPR, article 22). In these documents it was clear that these risks to human rights can occur mostly when data is unlawfully accessed (DA and CS). The risk of unlawful access is made more possible through cloud and edge computing services.

Data processing is generally recognised in these documents as an activity that raises concerns related to *fraudulent or abusive practices* (DGA, article 11). These

practices may include; *identity theft, damage to the reputation and economic theft*. These documents highlight the role availability of diverse digital technologies play not only in optimally maximising data for the benefit of society but also in amplifying these concerns and challenges. Also among these concerns is the disproportionate government access to data which can lead to possible abuses (EU SfD, section 6). The underlying point here is that an unbalanced government access to data, particularly personal data, gives governments powers that can be abused. Such powers can also be used by large corporations against smaller entities and this creates *contractual imbalances*. As the EU Data Act (article 13) highlighted, such contractual imbalances harm micro, small and medium-sized enterprises without a meaningful ability to negotiate the conditions for access to data. The accumulation of big data by Big Tech companies and other large-scale businesses reinforces imbalances in bargaining power or creates market imbalances that can be detrimental to legitimate interests of SMEs and this is of great concern according to the EU strategy for data. Imbalances related to access to and use of data can lead to 'unfair contracts' that harms the weaker contractual party and ultimately impedes the use of data by both contractual parties (EU DA chapter IV).

The EU Digital Markets Act (DMA) article 4 also observed that certain features of digital platforms can "lead in many cases to serious imbalances in bargaining power and, consequently, to unfair practices and conditions for business users as well as end users of core platform services". This implies that market processes, particularly when gatekeepers (providers of platforms and services) are involved, often lead to weak contestability and unfair practices. Providers of core platform providers are considered gatekeepers when they operate one or more gateways to customers and have significant impact on the internal market and are likely to have the power to set commercial conditions in a unilateral and often detrimental manner for both businesses and end users. Governance mechanisms are therefore required to safeguard the fairness and contestability of core platform services provided by gatekeepers.

Another critical concern identified by these governance documents is *the risk of data breach*. As the GDPR (art 33, 34) highlights; in the case of personal data breach, lack of appropriate and timely solution may result in physical, material or non-material damage to persons such as loss of control over their personal data or limitation of their rights. Article 4 of the ePrivacy Directive also raised the possibility of personal data breach through the use of electronic services. As the EU Cybersecurity Strategy observed, "hundreds of millions of records are lost each year through data breaches". Related to this are concerns about *security*. It is estimated that two out of five EU online users have experienced security-related problems and three out of five feel unable to protect themselves (EU CS, section 1).

The EU Strategy for Data (SfD, section 4) further highlights that despite the recorded benefits of open data initiatives in Europe, many data-driven companies are not sufficiently incentivised to share data. There is an evident *lack of trust* between entities that the data will not be used in line with contractual agreements, imbalances in negotiating power, the fear of misappropriation of the data by third parties and lack of legal clarity. These form a major part of the underlying ethical concerns that inform the EU data governance landscape.

The EU Digital Services Act (DSA) observed that online data processing activities expose Union citizens to *risks and harm online*—from the spread of illegal content and activities to limitations to express themselves and other societal harms. Illegal content is defined as information that is *"either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that relates to activities that are illegal such as the sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the non-authorised use of copyright protected material or activities involving the infringements of consumer protection law"* (EU DSA article 12). The wording of this article such as 'illegal hate speech' seems to suggest that there is a form of hate speech that can be considered legal. However, the point to be made here is that data processing activities on digital services can directly put individuals at risk or directly harm people.

A number of ethical justifications for the current EU data governance frameworks emerge from the above concerns (see Fig. 1). Data processing (collection, cleaning, storage, sharing, use and deletion) present technical, legal, organisational and socio-cultural challenges. Data processing significantly challenges the fundamental rights of natural persons as well as the rights of legal entities. There are individual as well as collective risks involved when data is processed; harm to individuals can occur (e.g discrimination, identity theft, fraud) and the legitimate interests of legal entities can be severely jeopardised (e.g unfair contracts). Thus, these documents aim at ensuring fairness in the allocation of value among data actors in the data economy (Data Act); protection of the rights of data subjects (GDPR), contribute to the emergence of pools of data made available on the basis of data altruism (DG Act) and leverage on a thriving data ecosystem to ensure that data is generated and used with the interests of individuals in focus and in accordance with "European values, fundamental rights and rules" (EU SfD, section 1). The strategy for data consistently emphasises the role EU values (revolving around the idea of the individual first) play in shaping the governance framework that are considered fair, practical and clear. Therefore, the paramount importance of the interests of the individual rather than the collective is central to the EU data governance mechanism.

These documents are therefore created to mitigate risks to persons, and ensure greater balance in the distribution of the value from data in alignment with the new wave of non-personal and industrial data and increasing proliferation of technological tools and services.

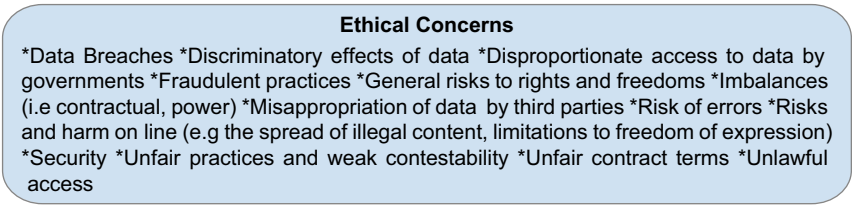

Fig. 1 Ethical concerns identified in EU data-related regulations and policies

4.2 Underlying Ethical Principles

As these documents clearly indicate, European values, contexts and expectations should be at the core of data processing pipelines and workflows. Thus, principles such as *autonomy* and *consent* are promoted. This highlights the understanding that data-driven technologies can promote or hinder human autonomy. Digital technologies are often designed with *dark patterns* (manipulative design patterns that influence users to make certain choices) that can subvert or impair human autonomy, decision-making and choice by pushing, coercing or deceiving people into making decisions on data disclosure transactions which often have negative consequences (EU DA). Dark patterns and other manipulative designs compromise ethical and legal requirements like autonomy and consent. That is why consent is provided as a major legal basis for data processing (GDPR arts 6 and 9). The EU DMA (article 5) reiterated the importance of consent as the basis for processing data generated through digital platforms. The intent is to ensure that human participants can freely participate in data processing activities with full information about what it entails to take part. This is called *informed consent* which is a critical principle for the promotion of human autonomy and the right to self-determination and a reflective action against dark patterns. At the foundation of this principle is the concept of *human agency*; a term that denotes the manifestation of the capacity to act (Schlosser, 2015). For the Data Governance Act (section 23), data processing activities ought to "enhance individual agency and the individuals' control over the data pertaining to them". Human agency includes the right of data subjects to take informed data disclosure and control decisions with appropriate knowledge of the potential risks and benefits involved. As the ePrivacy Directive provided, the obligation to inform service users of the purposes of which their personal data are collected should be imposed on the party collecting the data. Indeed, the Directive prohibits personal data processing without consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1) of the directive.

There is an acknowledgment in these governance documents that the human person has an intrinsic value with *fundamental rights* including the *right to data protection and privacy, confidentiality, and intellectual property rights*. The confidentiality of data and other electronic communications was emphasised by the e-Privacy directive. The principle of human rights underscores all the documents reviewed. The intent of Directive/95/46/ec and the GDPR is to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data within the European Union. Other governance documents also reinforce the objective to respect the fundamental rights as contextualised in European values including the right to privacy, the protection of personal data, the freedom to conduct business, the right to property and the integration of all persons irrespective of demographic differences. The EU Cybersecurity Strategy was clear in stating that effective governance mechanisms protect and promote human rights and fundamental freedoms online. The Data Act and the EU Strategy for Data share similar perspectives but the Data Act expands this to include the right of children as vulnerable consumers of IoTs and the right of digital technology users (even through

nominated third parties) to access and use their data. The focus on human rights re-emphasises the risks big data processing presents to human rights. The involvement of malleable, ubiquitous and pervasive technologies exacerbates these risks. These documents promote the rights of individuals as well as legal entities. That means that legal entities should also remain free to negotiate the precise conditions for making data available in their contractual relationships (DA, article 13).

The GDPR provides the data subject with a number of data protection and privacy rights which are taken as fundamental human rights (GDPR, articles 12–23). These include the right of access to their data, the right to rectification of errors in personal data, the right to erasure of the right to be forgotten, the right to restrict the processing of their personal data and the right to data portability. Particularly where personal data is involved, privacy-preserving techniques (e.g anonymisation, pseudonymisation, differential privacy, generalisation, or suppression, encryption and randomisation) are encouraged to preserve the ethical principles of privacy and confidentiality of the data subjects. Most notably, the other documents are not in conflict with these provisions of the GDPR. The right to portability is prominent in the Data Act (article 29) that seeks to facilitate the portability of the user's data to third parties. This right ensures that natural persons are treated as persons with intrinsic value with the right to self-determination; as a person that has autonomy/control over personal data.

Although the general idea is to preserve the rights of natural persons, the provision of secure processing environments is also crucial in ensuring 'trust among the different actors of European data ecosystems' (EU Strategy for Data, section 4). These governance mechanisms are also aimed at fostering *trust* between and among relevant data processing stakeholders (e.g public and private sectors as well as data subjects). As regards publicly held data, the EU Data Governance Act highlights that relevant stakeholder (including companies and data subjects) should be able to trust that, the re-use of certain categories of protected data in a way that respects their rights and interests. Protected data in this sense also includes non-personal data that can jeopardise public policy objectives. On the level of personal data, the EU SfD (section 1) observes that citizens will only trust and embrace data-driven innovations "if they are confident that any personal data sharing … will be subject to full compliance with the EU's strict data protection rules". Closely related to trust is the principle of *transparency*. These governance mechanisms provide legal clarity, certainty and transparency on legally enforceable rights and ethical obligations and responsibilities for all relevant stakeholders (GDPR, Data Act and Data Governance Act). This principle requires that information regarding data processing activities be made accessible, easy to comprehend and in clear and plain language. From data generation, storage and application to access controls (including data requests made by public sector bodies as is in the Data Act), transparency is an important principle to ensure trust as well as fairness.

Many aspects of data processing including but not limited to data sharing, data generation via digital products and services, data access controls give rise to questions of *fairness* in the digital economy; between users and designers or service providers as well as between large corporations and SMEs (DA, DGA, GDPR). First the GDPR was clear in stating that data processing activities must be lawful

and fair. Fairness as a principle will be a counter to possibilities of power imbalances, unfair contractual terms and discriminatory or biased decisions. There is an acknowledgement that conditions for data processing can be prejudiced and discriminatory. Therefore, the Data Governance Act (article 5) provides that conditions should be non-discriminatory, proportionate and objectively justified, while not restricting competition

Fairness in this sense is different from the *FAIR data principle* also promoted by the EU data governance documents. Making data FAIR means making data Findable, Accessible, Interoperable and Reusable (Wilkinson et al., 2016). The central idea here is not to create new standards for FAIR but to maximise existing standards and infrastructure to increase the findability, accessibility, interoperability and reusability of data (EU SfD, section 5). As an important element of FAIR, interoperability was emphasised in these documents as a critical element of ensuring trust and fostering the individuals' control of their data. It helps data sharing within and between sectors of the economy and the common EU data spaces and facilitates switching between data processing services (EU DA, article 3).

The EU Data Governance Act (article 15) furthers a principle called '*data altruism'*. This refers to data being made available by individuals or companies voluntarily for the common good. An example of this can be found in projects like *OpenSchufa* where people could share their personal credit score in order to study discriminatory effects in the scoring system. However, provisions must be made to ensure that data provided altruistically should be used for the common good and risks to the data providers mitigated. The concept of common good is also promoted by the EU Strategy for Data (section 4). The argument is that since data is created by society, they should be available for the *common good* including combating emergencies, addressing public health concerns, improving public services, tackling environmental degradation and climate change and efficient fight against crime. In this sense, the EU data governance mechanism documents aimed at ensuring the availability, quality and usability of data contribute to sustainability of private and public sector systems as well as environmental sustainability (EU SfD, section 5).

Furthermore, the reviewed documents promote the principle of *empowerment*. The underlying rationale is evident in EU SfD's statement that the EU can become a leading role model for a society empowered by data to make better decisions (section 1). This points to empowering individuals to be in control of the 'why', 'what' and 'how' of their data as well as businesses and the public sector (SfD, sections 3, 4, 5 and 7). Data-driven technologies and systems therefore ought to be designed to offer a very high degree of robustness not only to avoid errors but to withstand manipulation and address identifiable risks to all stakeholders. There were also strong requirements for the principle of *necessity*. Together with the principle of *proportionality*, the principle of necessity interrogates those intending to intervene or restrict a person's exercise of fundamental rights (e.g privacy) by the use of certain technologies as to why such intervention or restriction is necessary. Art. 6 of the GDPR highlights the importance of these principles and emphasises that necessity shall be justified only on the basis of objective evidence. Necessity is fundamental when accessing the lawfulness of personal data processing and is often the first criterion to consider before assessing the proportionality of the limitation.

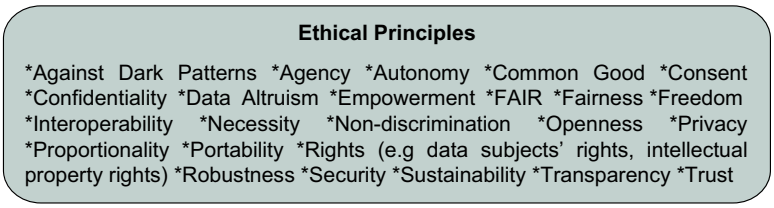

Fig. 2 Ethical principles promoted in EU data-related regulations and policies

These principles promoted by EU data-related policies and regulations (see Fig. 2) align with prevalent European ethical positions, most especially the primal importance of protecting the fundamental rights of the individual. The individual is a person with agency and autonomy and should be treated without discrimination. Data processing should be able to occur in a manner that ensures that the individual's rights are protected including the rights to consent and to fair and transparent decisions. Data processing entities ought to guard against dark patterns that can hinder empowerment of natural persons and the fostering of the common good. Data processing activities can only achieve this by being transparent, fair, open, secure, sustainable, trustworthy and FAIR.

4.3 Implementation/Recommendation

To address the identified ethical concerns and to achieve the ethical principles that align with European values and laws, these governance documents have provided a number of implementation approaches (see Fig. 3). For instance, the GDPR (article 32) provides that data processing entities adopt a number of technical and organisational measures or safeguards that includes; data protection impact assessment, identification of lawful basis for processing data (including but not limited to consent), pseudonymisation, anonymisation, encryption and specific rules clauses and agreements. In addition to this, each member state is expected to have a competent supervisory authority to ensure enforcement and possible resolution of breaches and conflicts. Supervisory authorities are encouraged to establish data protection certification mechanisms (article 42). Associations or bodies representing

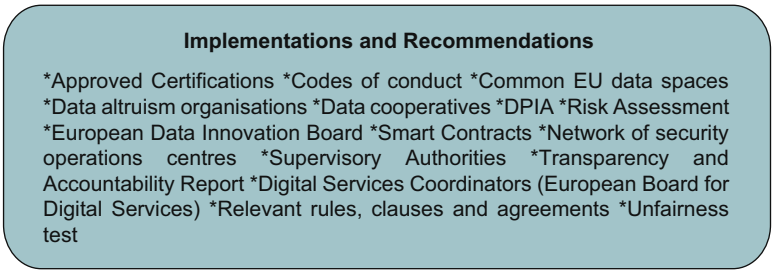

Fig. 3 Approaches to implementing identified ethical principles

categories of controllers or processors are encouraged to draw up codes of conduct to facilitate the effective application of the provisions of the regulation bearing in mind the diverse nature of data processing in different sectors. These implementation approaches provided by the GDPR are intended to promote a mixture of ethical, legal and technical principles; lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); accountability.

To unlock the value of data generated by connected objects in Europe and address the imbalances of power between SMEs and big tech companies, the EU Data Act proposes an *unfairness test* (DA, article 13). Contractual clauses that do not pass the unfairness test will not be binding on SMEs. In addition to this, article 34 proposes that the Commission shall develop and recommend non-binding model contractual terms on data access, sharing and use to enable parties negotiate fairer and more balanced terms and conditions. Another implementation approach provided by this regulation is smart *contracts* (article 30) which can facilitate interoperability and portability and prevent unauthorised access to data and ensure respect for user's rights including intellectual property rights. As defined by the Act, *Smart* contract is a computer program stored in an electronic ledger system and the outcome of the execution of the program or contract is recorded on the ledger. The essential requirements and harmonised standards of smart contracts for data sharing are detailed in this Act, but what is not clear is the ethical implication of this automated (blockchain) process especially as it relates to responsibility: who is responsible in cases of mistakes?

As a regulation that is focused on personal and non-personal data held by public sector bodies, the Data Governance Act created a robust mechanism for re-use of data based on the principles of transparency and proportionality. It does not specifically create the right to re-use but provides a harmonised set of conditions and requirements for re-use and sharing such data (DGA, chapter ii and iii). In chapter two, Member States are encouraged to establish single contact points that can support researchers and tech-driven businesses to identify and be able to request for the re-use of relevant data. Chapter three focuses on data sharing services (intermediation services between data holders and potential data users or between data subjects looking to make their data available and potential data users; and data cooperatives services). This chapter creates a notification mechanism where notifications are submitted to a Member State's competent authority who ensures that services are non-discriminatory, fair, transparent and compliant with available regulations. Most notably, the DGA facilitates data altruism as an efficient way of gathering data for the common good. To ensure that trust in the operations of organisations engaged in data altruism is established, the DGA opens up the possibility of these organisations registering as 'Data Altruism Organisations' (DGA, chapter iv). This implementation approach also involves the creation of a common EU data altruism consent form which can reduce the cost of collecting consent as well as facilitate efficient portability of data. This Act also created the European Data Innovation Board as an expert group that can ensure harmonised requests for re-use and notification mechanisms as well as advise the international cross- sectoral standardisation requests (DGA, chapter vi).

To address cybersecurity issues that can undermine fundamental rights and interests of natural persons, the Cybersecurity Strategy proposes to build a network of security operations centres across the EU (CS, section 1.2). The proposed national and sectoral networks require cross-border cooperation to create collective knowledge and to share best practices. Whereas this is a technical implementation approach, it has ethical implications. Increased collaboration and cooperation in the building of a robust cybersecurity architecture will mitigate risks to data breaches which in turn increases the safety and trustworthiness of the data processing ecosystem.

The EU DSA provided a number of implementation approaches to ensure that the risks and harms online are mitigated. First it preserves the prohibition of general monitoring of users from the e-Commerce directive in the bid to maintain a fair balance of fundamental rights of users online (DSA, article 7). Other obligations include that very large online platforms have the obligation to conduct risk assessments for 'systemic risks stemming from the functioning and use of their services in the Union' (article 26) and to take reasonable and effective steps to mitigate identified risks (article 27) and also submit to external independent audits (article 28). The DSA also provides for the establishment of competent digital services coordinators (article 38), the European Board for digital services (article 47) and the obligation to submit a transparency and accountability report annually (article 13). It is made clear that providers of intermediary services should not be subject to a monitoring obligation with respect to obligations of a general nature but does not affect specific orders given by national authorities in accordance with their national regulations. They have the obligation to moderate activities in a way that is socially acceptable, ethically responsible and legally compliant. The competent authorities and digital services coordinators are responsible for the application and enforcement of the regulation while the European Board for Digital Services serves as an independent advisory group of Digital Services Coordinators. The annual transparency report should be able to detail content moderation activities. However, the Act noted that the obligation to submit such a report does not apply to micro- or small enterprises so as to avoid disproportionate burdens on these entities.

Finally, the central proposal in the EU Strategy for Data (section 3) is the creation of the common EU data spaces in strategic economic sectors and domains of public interest. These sectoral spaces include; Industrial & Manufacturing data space, Green Deal data space, Mobility, Health, Energy, Agriculture, Public administration and Skills data spaces. This data ecosystem approach acknowledges the diverse nature, origins and applications of data. The intent is to provide a common governance mechanism, concepts and models in a way that can optimally maximise the data for the entire ecosystem and also the citizens. Data spaces will be complemented by sectoral policies and other measures (data sharing tools, architectures, infrastructures and governance mechanisms) across the data value chain. It is also hoped that structured data spaces with clearly defined infrastructures can facilitate interoperability, portability and security of data and "keep the EU at the forefront of the data-agile economy, while respecting and promoting the fundamental values that are at the foundation of European Societies" (EU SfD, section 1). The critical question then is, what is the implication of these findings that highlight

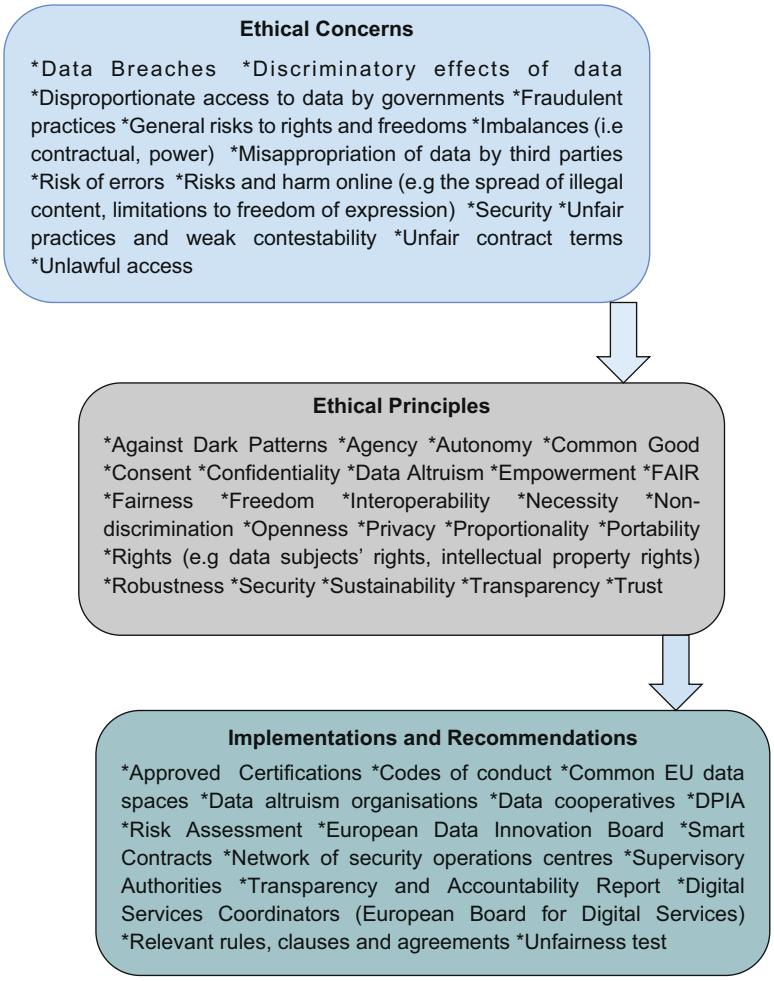

Fig. 4 Overview of ethical concerns, principles and implementation approaches identified in EU data-related regulations and policies

the Overview of ethical concerns, principles and implementation approaches identifiable in EU data-related policies and regulations (see Fig. 4)?

5 Discussion and Conclusion

This paper takes an approach that inverts the logic of much of the research on ethics of technology. The typical logic is that ethical concerns of a particular technology or application are identified and evaluated. Where they are deemed to be sufficiently serious mitigation strategies are proposed. These often include policy, regulatory or legislative interventions that can then be implemented. The example of privacy and

data protection may be instructive here. While the right to privacy has first been stipulated in the 19th century (Warren & Brandeis, 1890), the finer detail of the threats that novel information technologies posed to this right only became clearer in the second half of the 20th century. This led to the development of the ethically motivated fair information principles that inspired subsequent legislation including the GDPR. We can thus see a process of formalisation and codification of ethical concerns leading to policy and regulation. In this paper we aim to reverse the view and start with existing and emerging policy, legislation and regulation to understand the underlying ethical positions.

The analysis of the current EU data policy and regulatory landscape provided in the preceding sections does indeed provide some indications of ethical assumptions and positions that underpin the foundation of this landscape. The extraction of ethical issues and concerns as shown above indicates a clear focus on the protection of the individual citizen and consumer. Citizens are to be protected from harm that may occur due to data breaches, fraud, misappropriation of data, unfair contracts and other harms that may arise in the digital space. These concerns do not indicate a specific ethical theory that is consistently applied. The protection of individual citizens and consumers is compatible with most established ethical theories including Kantian deontology or utilitarian consequentialism.

A similar statement can be made about the principles that inform the legislation. Mid-level principles are the bedrock of much current ethics-related practice. This is likely to be driven by the success of biomedical ethics (Beauchamp & Childress, 2009) which sidestepped traditional debates in philosophical ethics about the respective merits of ethical theories and instead focused on ostensibly uncontroversial principles, notably beneficence, nonmaleficence, respect for autonomy and justice. These principles have not only inspired the development and institutionalisation of biomedical research ethics, but they have also been increasingly adapted and adopted by ethical approaches to data and technology (Jobin et al., 2019) as prominently exemplified by the EU's High Level Expert Group on AI (AI HLEG, 2019).

The principles identified in our analysis of EU data policy explicitly include some of the traditional biomedical principles such as autonomy and closely related ones like consent which is often derived from autonomy or fairness which is often used synonymously to justice. The set of principles that we identified is, however, broader than the biomedical principles and covers some that are specifically geared to the use in data-related environments, such as interoperability, portability, transparency or the FAIR principles that were developed specifically for data. In addition, there are other principles that are arguably mostly consistent with biomedical ethics, such as empowerment, proportionality, or sustainability. These principles appear to be capable of being supported from a range of ethical positions. They are furthermore largely unproblematic and not contested per se. The ranking of these principles would be challenging and it is not clear how conflicts between them could be evaluated. They are nevertheless useful proxies to guide data-related policy insofar as they implement or instantiate various human rights.

The final set of findings, the recommendations and implementation proposals follow this logic and propose mechanisms that will allow realising the principles

and address the issues and concerns. By their very nature they sit on a different level and spell out mechanisms that can be used consistently across uses of data, such as codes of conduct, the implementation of DPIAs, networks of competence centres or certifications. These mechanisms will in many cases require the existence of bodies or organisations to provide or certify them, such as a digital services coordinator, a European data innovation board or other supervisory authorities.

One can thus draw a line from the issues via the principles to the implementation proposals. At the same time, a slightly different interpretation is possible. The ethical issues we identified are predominantly those that affect the individual. This is not surprising, as the individual human being has traditionally been the focus of European ethical thinking as well as human rights legislation. The protection of individuals from data-related harm is therefore justifiably at the core of the current EU data policy landscape. At the same time, however, one can observe an increasing level of interest in questions that are not exclusively focused on individual risks and harms. It is a well-established critique of the current tech landscape that it has given rise to monopolies and oligopolies that allow the extraction of value from data for the benefit of few, notably the large tech companies (Zuboff, 2019). In Europe this dominance of the tech companies which are mostly US-based is further embedded in concerns about the ability to control the use of data, a topic sometimes discussed under the heading of digital sovereignty. Looking at the proposals in the current EU data policy landscape, one can identify several that are clearly aimed at addressing this concern. This includes the idea of data cooperatives which also informs the developing EU data spaces. While such more community-oriented policies can be justified from the traditional individual-centric ethical perspectives, they may also point to a growing influence of more communitarian ethical thinking. If this interpretation proves to be appropriate, then one could expect in future to see a stronger emphasis on positive human rights, i.e. rights to solidarity that also form part of the EU's Charter of Fundamental Rights. Such developments would be interesting to follow if they start to cover topics that are currently under-developed in policy, such as the impact of data on working conditions, collective bargaining etc. The impact of data-driven technologies on the future of work is well-covered in the ethics of technology debate (Willcocks, 2020), but currently does not seem to filter through to policy development.

Our analysis thus shows that the current EU data governance policy landscape can be read from an ethical perspective as being grounded in ethical thinking, typically expressed in terms of human rights, aware of likely concerns, based on well-established principles and in the process of being codified in regulation, legislation and institutions. At present this reading is not easy to realise, however. In our analysis we focused on some of the most high-profile policy-related documents. We realise that there are many more documents of relevance to the EU data governance policy world. Accessing this world is not trivial, as there is no platform where individuals and organisations can find harmonised or streamlined information or interpretation on the detail of policy, its interpretation and implementation. One reason why this is problematic from an ethical perspective, in addition to the obvious problem of implementing policy where the exact content of the policy is not clear, is that it offers little guidance on dealing with value conflicts. Our analysis

has shown the numerous principles that guide EU data governance. These values can and often do conflict with one another. An obvious example would be data protection, for example in the case of medical research data, which can clash with openness, transparency and FAIR principles (Starkbaum & Felt, 2019). In the GDPR, limitations in the case of conflicts of rights and interests can sometimes be justified where such limitation is necessary, proportionate, and if no other reasonable alternatives to achieve purpose are present. While this ethical-legal approach aims to balance conflicting rights, what constitutes 'necessary' and 'proportional' continues to be unclear in cases of new forms of research data and technologies. Additionally, the applicability of established approaches under the new regulations remains uncertain. Such value conflicts call for mechanisms to contextualise and relate the different values, a task that philosophical ethics can address, but for which there is currently no mechanism or approach with regards to EU data governance.

A further limitation of this landscape is its EU focus. While policy and legislation are by nature usually tied to jurisdiction, the same cannot be said for data. The technical data infrastructure is largely global and while governments can influence how data transcends borders, much data flow is international. A better understanding of the ethical underpinnings of data governance therefore calls for an analysis of data governance policies beyond the EU which in practice would greatly complicate the work, not just because of language barriers and the fundamental difference in understanding, interpreting and implementing policies, but also because it would likely include other values that are more prominent outside of the EU. However, such an international analysis at least across key data processing countries and legal systems (e.g. USA, China) would be helpful in better understanding the relationship between data governance regimes which, in turn, would be helpful in negotiating principles of international data governance. Another useful exercise for further research is to unpack or make explicit the types of implicit philosophical assumptions the European Commission has in the governance of data and technologies. Identifying and mapping the normative assumptions or ethical traditions or theories behind these regulations can provide greater insights into their meaning and interpretations.

Finally, we concede that this textual analysis of the ethics of data governance policy can only be the starting point of trying to understand the landscape. At the moment we are witnessing much experimentation with data governance structures and approaches in the EU. Our analysis has shown that these are based on ethical underpinnings, but it says nothing about how these ethical underpinnings play out in practice and whether the policies will have the consequences they are aiming for. We therefore believe that empirical research is called for to understand the social reality of data governance practice that is guided by EU policies to understand whether and to what degree ethical principles are realised and whether agents in the data governance space agree with them, comply with them or maybe ignore or sidestep them.

A further area for empirical research would be the socio-political context of the policies and regulations that drive the EU's approach to data. The texts we analysed do not appear in a vacuum but are the results of social interaction and political

negotiation. In this paper we have taken the documents for granted, but a further analysis is called for that could explore why are topics portrayed as they are, how they were drafted, what the origins of the ideas and concepts are that are enshrined in them etc. This could also include the use of critical theory to better understand power relationships, partial interests, silenced voices etc (Iliadis & Russo, 2016)

We believe that such research is urgently called for due to the importance of data and data governance. We agree with the assumption that data and the current and emerging digital technologies that are based on and make use of data have huge potential to improve human lives. They can also have highly undesirable consequences. Data governance will play a key role in encouraging the former and avoiding the latter. Data governance is normative, i.e. it guides behaviour. An understanding of the underlying ethical drives and justification is therefore important to ensure that it leads to desirable consequences. Technical and legal work on data governance should therefore be accompanied by ethical reflection. We hope that this article can serve as a step in this accompaniment and that it has demonstrated that data governance policy is neither a purely technical nor a pure policy activity and can benefit from active ethically informed reflection.

Author Contributions D.E.: Conceptualisation, data collection and analysis; writing—original draft/review and editing; B.S.: Conceptualisation, data analysis, writing—original draft/review and editing.

Funding This work was supported by the UKRI Technology Mission Fund under the EPSRC grant ref *EP/Y009800/1*.

Data Availability The data that support the findings of this study including the Nvivo coding book and the full Nvivo project are available at Nottingham Research Data Management Repository DOI: 10.17639/nott.7382.

Declarations

Informed Consent Not applicable.

Competing Interests The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Access Now. (2018). *Human rights in the age of artificial intelligence*. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

AI HLEG. (2019). *Ethics guidelines for trustworthy AI*. European Commission - Directorate-General for Communication. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Aronson, J. (1995). A pragmatic view of thematic analysis. *The Qualitative Report*, *2*(1), 1–3.

Baird, R. M., Ramsower, R. M., & Rosenbaum, S. E. (Eds.). (2000). *Cyberethics: Social and moral issues in the computer age (contemporary issues (prometheus)): Social & moral issues in the computer age*. Prometheus.

Beauchamp, T. L., & Childress, J. F. (2009). *Principles of biomedical ethics* (6th ed.). OUP.

Bengio, Y., Lecun, Y., & Hinton, G. (2021). Deep learning for AI. *Communications of the ACM*, *64*(7), 58–65. https://doi.org/10.1145/3448250

Boyd, D., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society*, *15*(5), 662–679. https://doi.org/10.1080/1369118X.2012.678878

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Bynum, T. W. (2010). The historical roots of information and computer ethics. In L. Floridi (Ed.), *The Cambridge handbook of information and computer ethics* (pp. 20–38). Cambridge University Press.

Coeckelbergh, M. (2020). *AI Ethics*. The MIT Press.

Council of the European Union. (2020). *Presidency conclusions—The charter of fundamental rights in the context of artificial intelligence and digital change* (No. 11481/20). https://www.consilium.europa.eu/media/46496/st11481-en20.pdf

Dignum, V. (2019). *Responsible artificial intelligence: How to develop and use AI in a responsible way* (1st ed. 2019 ed). Springer.

Dreyfus, H. L. (1972). *What computers can't do: A critique of artificial reason*. Harper & Row.

Dreyfus, H. L. (1992). *What computers still can't do: A critique of artificial reason* (Rev. ed.).

Eke, D. O. (2023). ChatGPT and the rise of generative AI: Threat to academic integrity? *Journal of Responsible Technology*, *13*, 100060.

European Commission. (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence—Annexes to the proposal* (COM(2021) 206 final). European Commission. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

European Commission. (2022, January 26). *Commission puts forward declaration on digital rights and principles for everyone in the EU*. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_452

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., & Srikumar, M. (2020). *Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI*. https://dash.harvard.edu/handle/1/42160420

Floridi, L. (1999). Information ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology*, *1*(1), 33–52.

Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A*, *374*(2083), 20160360. https://doi.org/10.1098/rsta.2016.0360

Guterres, A. (2020). *The highest aspiration—A call to action for human rights*. Unitted Nations. https://www.un.org/sg/sites/www.un.org.sg/files/atoms/files/The_Highest_Asperation_A_Call_To_Action_For_Human_Right_English.pdf

Hall, W., & Pesenti, J. (2017). *Growing the artificial intelligence industry in the UK*. Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf

Iliadis, A., & Russo, F. (2016). Critical data studies: An introduction. *Big Data and Society*, *3*(2), 2053951716674238.

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

Kitchin, R., & McArdle, G. (2016). What makes big data, big data? Exploring the ontological characteristics of 26 datasets. *Big Data and Society*, *3*(1), 2053951716631130. https://doi.org/10.1177/2053951716631130

Latonero, M. (2018). *Governing artificial intelligence: Upholding human rights & dignity*. Data&Society. https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf

McGregor, L., Murray, D. & Ng, V. (2019). International human rights law as a framework for algorithmic accountability. *International & Comparative Law Quarterly*, *68*(2), 309–343.
Metcalf, J., Keller, E. F., & boyd, d. (2016). *Perspectives on big data, ethics, and society.* Council for Big Data, Ethics, and Society. http://bdes.datasociety.net/wp-content/uploads/2016/05/Perspectives-on-Big-Data.pdf
Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. SAGE.
OECD. (2019). *Recommendation of the council on artificial intelligence* [OECD Legal Instruments]. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
Proposal for a DECISION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the 2030 Policy Programme "Path to the Digital Decade", no. COM/2021/574 final (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0574
Schlosser, M. (2015). Agency. [Online] Available from: https://plato.stanford.edu/entries/agency/?trk=public_post_comment-text [Accessed 02/03/2024].
Stahl, B. C. (2012). Morality, ethics, and reflection: A categorization of normative IS research. *Journal of the Association for Information Systems*, *13*(8), https://aisel.aisnet.org/jais/vol13/iss8/1
Stahl, B. C., Timmermans, J., & Mittelstadt, B. D. (2016). The ethics of computing: A survey of the computing-oriented literature. *ACM Computing Surveys*, *48*(4), 55:1–55:38. https://doi.org/10.1145/2871196
Stahl, B. C. (2021). From computer ethics and the ethics of AI towards an ethics of digital ecosystems. *AI and Ethics*, *2*, https://doi.org/10.1007/s43681-021-00080-1
Stahl, B. C., & Eke, D. (2024). The ethics of ChatGPT – Exploring the ethical issues of an emerging technology. *International Journal of Information Management*, *74*, 102700.
Starkbaum, J., & Felt, U. (2019). Negotiating the reuse of health-data: Research, big data, and the European general data protection regulation. *Big Data and Society*, *6*(2), 2053951719862594. https://doi.org/10.1177/2053951719862594
UNESCO. (2020). *First draft of the recommendation on the Ethics of Artificial Intelligence* (SHS/BIO/AHEG-AI/2020/4 REV.2). https://unesdoc.unesco.org/ark:/48223/pf0000373434
Warren, S. D., & Brandeis, L. D. (1890). Right to privacy. *Harvard Law Review*, *4*, 193.
Weizenbaum, J. (1977). *Computer power and human reason: From judgement to calculation* (New ed.). W.H.Freeman & Co Ltd.
Wiener, N. (1954). *The human use of human beings*. Doubleday.
Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., ... & Mons, B. (2016). The FAIR guiding principles for scientific data management and stewardship. *Scientific Data*, *3*(1), 160018.
Willcocks, L. (2020). Robo-Apocalypse cancelled? Reframing the automation and future of work debate. *Journal of Information Technology*, *35*(4), 286–302. https://doi.org/10.1177/0268396220925830
World Economic Forum. (2019). Responsible use of technology [White paper]. WEB. http://www3.weforum.org/docs/WEF_Responsible_Use_of_Technology.pdf
Zuboff, P. S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (1st ed.). Profile Books.
Zwitter, A. (2014). Big data ethics. *Big Data and Society*, *1*(2), 2053951714559253.