A Discussion on Ethical Cybersecurity Issues in Digital Service Chains

Frédéric Tronnier(✉), Sebastian Pape, Sascha Löbner, and Kai Rannenberg

Goethe University, Frankfurt, Germany
{frederic.tronnier,sebastian.pape,sascha.loebner,
kai.rannenberg}@m-chair.de

Abstract. Enabling cybersecurity and protecting personal data are crucial challenges in the development and provision of digital service chains. Data and information are the key ingredients in the creation process of new digital services and products. While legal and technical problems are frequently discussed in academia, ethical issues of digital service chains and the commercialization of data are seldom investigated. Thus, based on outcomes of the Horizon2020 PANELFIT project, this work discusses current ethical issues related to cybersecurity. Utilizing expert workshops and encounters as well as a scientific literature review, ethical issues are mapped on individual steps of digital service chains. Not surprisingly, the results demonstrate that ethical challenges cannot be resolved in a general way, but need to be discussed individually and with respect to the ethical principles that are violated in the specific step of the service chain. Nevertheless, our results support practitioners by providing and discussing a list of ethical challenges to enable legally compliant as well as ethically acceptable solutions in the future.

Keywords: Data protection · GDPR · Cybersecurity · Ethical issues · Digital service chain

1 Introduction

Information and data, including personal data, are the main drivers of the constantly advancing digitalization and digital economy. In this economy, traditional product and service chains are supplemented and replaced by digital service chains that transform the way products and services are created, processed, distributed and experienced. Products, services and processes are increasingly being connected to create new insights and information from data. With these drivers, ethical and legal issues are arising on the appropriate protection of individuals and their data. While the legislative response in Europe through the General Data Protection Regulation (GDPR) is widely regarded as a major step towards the protection of data subjects and (their) personal data, ethical issues remain. The GDPR

Supported by H2020 Science with and for Society Programme [GRANT AGREEMENT NUMBER – 788039 – PANELFIT].

J. Kołodziej et al. (Eds.): Cybersecurity of Digital Service Chains, LNCS 13300, pp. 222–256, 2022.
https://doi.org/10.1007/978-3-031-04036-8_10

aims to give individuals the control over (their) personal data by laying down a set of rules clarifying how personal data may be used by individuals and organizations. Compliance with data protection regulation does however not automatically equal ethical organizational procedures. With respect to research projects, the European Commission defines this point accurately as: "the fact that your research is legally permissible does not necessarily mean that it will be deemed ethical" [23, p. 4]. We argue that the same holds for the development of products and services in digital service chains where ethical issues are rarely discussed.

Ethical issues concerning data and cybersecurity are often – and rightly so – discussed from the perspective of individuals as they are likely to be the stakeholders suffering from them. However, in this work, we aim to discuss ethical issues from the perspective of both, individuals and organisations, using the framework of digital service chains as a point of reference. As ethical issues arise due to the different needs and interests of various stakeholders, individuals, data subjects, small and multinational organizations as well as states and state agencies, ethical issues need to be discussed with all stakeholders in mind.

The objective of this work is therefore to cluster existing ethical issues with regards to cybersecurity and data commercialization in the different phases or steps of digital service chains. Our objective is not to define the "right decision" for stakeholders in an ethical issue, but rather collect a list of such issues arising in digital service chains. We imagine that service providers in the chain can go through that collection and identify ethical issues, which are relevant to their services, too. To a certain degree, we follow the call from Schoentgen and Wilkinson [77] to expand the ethics debate on recent technologies.

The structure of this work is as follows: In section two related work on digital service chains, cybersecurity, and data commercialization is provided. As there exist numerous ethical issues, we concentrate on the most pressing or timely ones, based on the methodology outlined in the third section. The fourth section discusses ethical issues following the framework of a digital service chain. The results are then discussed in a separate section. The last section concludes this work and identifies opportunities for future work.

2 Background and Related Work

The following subsections provide an introduction to the topics relevant for this work. In the first subsection, the topics of cybersecurity and data protection are established. As multiple ethical issues in digital service chains relate to the selling and purchasing of data, we define the term of data commercialization in the subsequent section before outlining digital service chains themselves. Fundamental ethical principles are then introduced before giving an overview on related work on ethics in cybersecurity in research.

2.1 Cybersecurity and Information Security

Cybersecurity, often also called IT security or ICT security before "cyberspace" became a popular term, refers to the safeguarding of individuals, organizations

and society of cyber risks. As computer and information systems are increasingly relied on as the backbone of organizations and the daily working environment of large parts of the workforce, ensuring cybersecurity is a crucial factor for organisations and individuals alike. With the advancement of the internet, new wireless network standards and technologies such as "internet of things", "smart devices" or connected vehicles, the importance of ensuring cybersecurity is only increasing. The primary focus of cybersecurity is often described as the provision of confidentiality, integrity, and availability of data, also called the CIA-triad. In this context, confidentiality aims to prevent data and information from unauthorized access while integrity aims to maintain the accuracy and consistency of data and information in all stages of the processing of the data. Lastly, availability encompasses the consistent accessibility of data and information for all authorized entities. Integrity and availability are then also considered relevant for the systems handling the data. Cybersecurity can be seen as a significant aspect of the broader concept of information security. Information security, the protection of information and data, encompasses both non-technical and technical aspects, whereby cybersecurity solely focuses on the technical aspects of it. For instance, the creation of shredding or recycling procedures of printed information would fall under the domain of information security but does not fall under the domain of cybersecurity. In this work, we address information security in general, as the management of information security includes the management of cybersecurity and offers a more holistic approach to study ethical issues of cybersecurity in digital service chains.

To ensure information security, it is essential to understand the different types of vulnerabilities that can lead to information disclosure or the disruption of services in a system. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) define a vulnerability in ISO/IEC 27005:2018 as *"weakness of an asset or control (3.1.12) that can be exploited so that an event with a negative consequence occurs"* [25].

Such vulnerabilities were classified in ISO/IEC 27005 into their related asset types: hardware, software, network, personnel, physical site and organizational site. Here, vulnerabilities may not only be caused by insecure or unprotected hardware or software but also by the susceptibility of external factors such as humidity for hardware, natural disasters for a physical site or a lack of security training for personnel. A wide range of causes for vulnerabilities exist that need to be individually evaluated [84]. As the definition of a vulnerability also relates the concept of threats, it is necessary to define a threat in the context of information security. According to the European Union Agency For Cybersecurity (ENISA), a threat may be defined as: *"Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service"* [19]. A plethora of different threats exists for which various possible classification schemes exist[1].

[1] For an overview of threat types, see the threat classification model of the Horizon2022 CyberSANE project: https://www.cybersane-project.eu/taxonomy-of-threat-landscape/.

2.2 Data Commercialization

According to the European Commission, in 2019, *"the value of the European Data Market is expected to reach 77.8 billion Euro, with a growth rate of 97% in 2018, and at an average rate of 4.2% out to 2020"* [58, p. 67][2] In 2025, *"...the Data Market will amount to more than 82 billion Euro in the EU27, against 60.3 billion Euro in 2018 (a 6.5% CAGR 2020–2025)..."* [58, p. 41]. The same estimate predicts that, if policy and legal framework conditions for the data economy are put in place in time, its value will increase to EUR 680 billion by 2025 for the EU28 (550 billion for the EU27), representing 4.2% (4.0%) of the overall EU GDP for a baseline scenario. Still, the term 'data commercialisation' is one that causes diverging reactions among different stakeholders in the environment of data protection and ICT research. While some people regard it as a reality that is indeed lawful - whether commercially and/or socially desirable or not -, others assess it to be unlawful, unethical and unacceptable for personal data in general. This could be explained by the fact that there does not exist one generally approved definition of the term. As the lawfulness of commercialising and processing data highly depends on its specification, it is crucial to define the context first. Hereby, one should differentiate between:

- The type of data, that is either personal or non-personal data [14, p. 4–5];
- The amount of data, that is either multiple data records in a database or individual data records;
- The source of the data, that is either collected by the data controller, by a third party or publicly available data;
- The form of commercialisation, that is the licensing or granting access of data.

In order to discuss ethical considerations on this subject in the context of this work, the commercialization of data is defined as: the processing of personal data as regulated under the GDPR, in the form of licensing by granting third parties access to collected personal data for a monetary profit. While it is assumed that personal data possesses economic value that may be transferred between parties, the specifics of the commercialisation of data however may differ, depending on the licensor, licensee and the purpose of the data.

Ethical Considerations on Data Commercialization: The commercialisation of data does not only create issues and gaps through unclear or missing regulation but also needs to be reviewed from an ethical perspective. The European Commission states in a non-guiding document on Ethics and Data Protection (2018) for researchers that: "...the fact that your research is legally permissible does not necessarily mean that it will be deemed ethical". So also ethical requirements need to be met for the commercialisation of data. The GDPR already encompasses some ethical aspects such as transparency and accountability in the relations between data subjects, data controllers, and data processors. The GDPR also aims to foster the societal interest to protect data and ensure privacy, for instance in Art.

[2] Disaggregated data can be found at The European Data Market Monitoring Tool: http://datalandscape.eu/european-data-market-monitoring-tool-2018.

57(1)(b), stating that public authorities must "promote public awareness" on the aspects of data processing. Moreover human dignity and personal autonomy are moral values, covered by constitutions and laws that need to be respected through the protection of data, also when data is being commercialised.

However, several ethical issues and questions arise when looking at the commercialisation of data, as defined in this document. Should it be possible to renounce fundamental rights to allow for data altruism? How can data indeed be ethically commercialised if the ownership of data is not defined? Unless an established pricing mechanism for personal data is developed, fair data markets that ensure an adequate remuneration of individuals relinquishing their personal data are unlikely to occur. As long as privacy is not transparently priced, individuals are not aware of the value of their personal data, do not know whether they are getting a fair deal if they accept to monetise their data, and remain unaware of their market power. This demonstrates that legal and ethical issues are closely connected and that the commercialisation of data needs to be reviewed with both, ethical and legal issues in mind.

2.3 Digital Service Chains

The book "Service Chain Management" by [86] provides a comprehensive introduction to the topic and defines the sub-category of digital service chains. The authors state that digital service chains "depend on the digital transportation and processing of information from "raw" inputs to "finished" outputs delivered over bandwidth-rich computer networks to a variety of computationally powerful consumer devices" [86]. Digital service chains are therefore comparable to traditional service chains and consist of the steps outlined in Table 1.

Table 1. Examplary digital service chains, adapted from [86]

Content creation	Aggregation	Distribution	Data transport	Digital experience
Software	Software suites	J2EE, .Net, Application servers	Cables, Wireless	Terminals and mobile devices
Advertising	Combining personal data	Ad-networks	Cables, Wireless	Terminals and mobile devices

The first step, Content Creation, is defined as a process through which software, music, art or other services are created. While [86] defines this step as an intense human process, we argue that this step could also take place automatically, given the emergence of new technologies and services that allow the creation of other goods and services without the need of a human. Examples of this are ML/AI algorithms that can create music, texts, or software on their own [31,61].

In the second step, Aggregation, data and information are aggregated from different sources, for instance from multiple data subjects or platforms. In the

third step, Distribution, the data is placed on a suitable platform, using a distribution system, to be delivered to the respective users or customers. This could for instance be advertising servers at a social media organization or application servers for a software solution. In the fourth step, Data Transport, the data is transported to users or customers using fixed or wireless network solutions. Lastly and in the fifth step, Digital Experience, the service or product is experienced by customers or users, using mobile or stationary devices.

Digital service chains have been researched extensively from a technological perspective [20] and also with respect to cybersecurity. Repetto et al. [74] argue that traditional security models are not suitable anymore for increasingly agile service chains and develop a reference architecture to manage cybersecurity in digital service chains. Concrete use cases of such a framework are detailed in [75]. However, in both articles, there is no consideration of how to ensure that the deployed services consider potential ethical issues.

2.4 Ethics in Cybersecurity

When discussing ethical issues relating to cybersecurity and the commercialization of data, ethical issues need to be discussed first. Vallor et al. [85] argue that "ethical issues are at the core of cybersecurity practices" as they retain "the ability of human individuals and groups to live well". Research on ethics in cybersecurity has been an emerging topic [67] with a particular focus on ethics in cybersecurity in the context of AI [82]. Manjikian [55] provides an comprehensive introduction to the topic. A variety of ethical frameworks and approaches towards ethics in cybersecurity exists. Formosa et al. [28] distinguish the existing approaches into two categories:

- The first category applies moral theories such as utilitarianism, consequentialism, deontological, and virtue ethics. The authors state that this approach may lead to conflicting results, depending on the moral or ethical theory applied.
- The objective of the second category is "to develop a cluster of mid-level ethical principles for cybersecurity contexts" [28].

Based on the shortcomings of existing approaches, the authors develop a new framework, depicted in Fig. 1. The ethical principles depicted in Fig. 1 will be utilized when discussing the ethical issues relating to digital service chains identified in this work.

In the following sections the framework will be used as a point of reference on which ethical issues in digital service chains and with regard to the commercialization of data are to be clustered upon. The five basic principles of cybersecurity ethics, adapted from [28] are the following:

- **Non-maleficence:** The technologies, services, and products envisioned and implemented in the digital service chains do not to intentionally harm users or make their lives worse.
- **Beneficence:** The technologies, services and products envisioned and implemented in the digital service chains should be beneficial for humans, that is, improve users overall live.

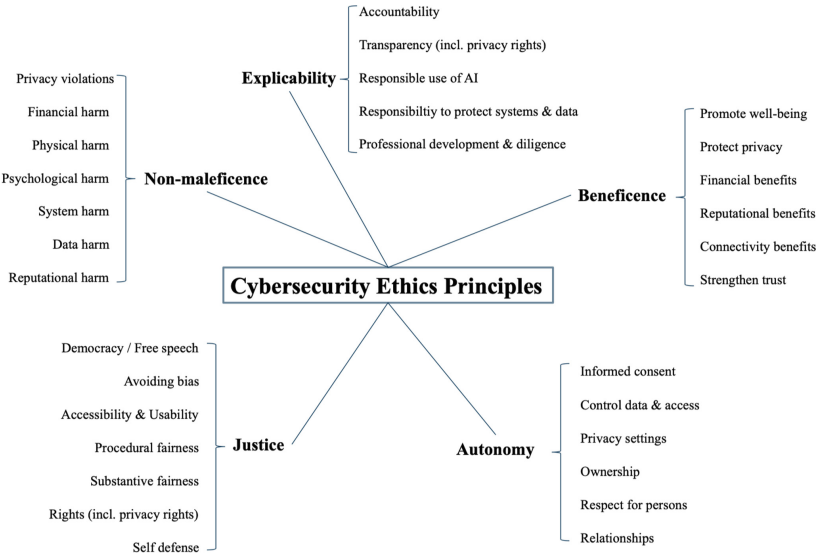

Fig. 1. Five cybersecurity ethics principles adopted from Formosa et al. [28]

- **Autonomy:** The technologies, services and products envisioned and implemented in the digital service chains should retain users' autonomy. That is, users are able to make informed decisions on how these services and products impact their lives and how they may use them.
- **Justice:** The technologies, services, and products envisioned and implemented in the digital service chains should not discriminate or undermine solidarity between users. Instead, fairness and equality are to be promoted.
- **Explicability:** The technologies, services, and products envisioned and implemented in the digital service chains are to be transparent. Users are to be able to understand them and know which entities are responsible and accountable for them.

2.5 Related Work

While a plethora of research on technology-related ethical issues exists, research on ethics in cybersecurity and digital service chains is less omnipresent.

Ethical issues in cybersecurity are often studied in the domain of academic research, in which ethical standards are to be met by researchers when working with data. Macnish and van der Ham [51] investigate different ethical issues and discuss the difference between ethical issues in research and practice using two case studies. The authors find that researchers are able to draw on feedback from research ethics committees, an option that is not available to practitioners. The authors advocate for a stronger focus and discussions on ethical topics in computer science courses. The book of Manjikian [55] provides an extensive introduction into the topic of cybersecurity ethics. The author introduces

several concepts and ethical frameworks and applies them to multiple issues in cybersecurity, such as data piracy and military cybersecurity. Finally, the author discusses codes of ethics for cybersecurity. While the author follows a comparable approach to this work, the ethical issues discussed in this work were identified through a different structure, expert workshops and encounters, and take place in a particular setting, the focus on digital service chains and the commercialization of data.

Similarly, the interdisciplinary book of Christen et al. [13] discusses various topics of ethics in cybersecurity. Here, van de Poel [72] analyses values and value conflicts in cybersecurity ethics, clustering them into security, privacy, fairness and accountability. The author identifies and discusses several value conflicts, not only between security and privacy, but also between privacy and fairness or accountability. The chapter of Loi and Christen [50] discusses several ethical frameworks for cybersecurity and creates a first methodology for the assessment of ethical issues. The methodology follows the privacy framework of Nissenbaum [68] that views privacy as contextual integrity and extends it with "social norms and expectations affecting all human interactions that are constitutive of an established social practice" [50]. When discussing ethical issues in the context of business, the book focuses more on specific domains, such as healthcare, or on ensuring cybersecurity for businesses (see [59,80]).

Mason [56] discusses policy for personal data as an overarching framework in a socio-technical system. He focuses on respect for persons and the maintenance of individual dignity. In the same manner, Nabbosa and Kaar [63] investigate ethical issues of digitalization with a strong focus on the economics of personal data. They conclude that user's awareness to data privacy needs to be strengthened and the control over the data needs to be shifted back to the users, but this cannot be done by regulation alone and all shareholders should take responsibility. Schoentgen and Wilkinson [77] present several ethical frameworks and investigate the implementation of ethics by governments and companies. Royakkers et al. [76] focus on ethical issues emerging from the Internet of Things, robotics, biometrics, persuasive technology, platforms, and augmented and virtual reality. They connect the presented ethical issues with values set out in international treaties and fundamental rights.

Hagendorff [33] analyzes 22 guidelines for ethical artificial intelligence and also investigates to what extent these were implemented in practice. His conclusion is that artificial intelligence ethics are failing in many cases. Mostly, because there are neither consequences for a company not following the guidelines nor for the individual developer not implementing them when developing a new service.

However, none of this work has a specific focus on the digital service chains and maps the ethical challenges to its corresponding phases.

3 Methodology

The methodology of this work is based on a two-step approach. Starting point for the identification and analysis of ethical, and also legal, issues was a workshop with four legal and four industry experts from Spain, Finland, England,

the Netherlands, Germany, and France, which took place on 3 June 2019 in Bilbao, Spain. The workshop, corresponding to work-package 3 of the Horizon2020 PANELFIT project[3], was structured into four sessions:

- Ownership of Data
- Usage of External Databases
- Monetising Internal Databases
- Good Commercialisation Governance

Each of the experts was asked to give a short presentation on one of the topics, followed by a discussion with all attendees (experts and present projects partners). Based on the results of the workshop, several attendants have also produced academic papers on the commercialisation of data, leading to a special issue in the European Review of Private Law.[4] While the workshop focused primarily on legal issues and gaps in the GDPR relating to the commercialization of data, the workshop also raised first ethical issues that have been subsequently expanded on in a second workshop on 28^{th} of June 2021 in an online event. Similarly, the workshop was structured into four sessions:

1. Data Altruism
2. The value of data
3. A pricing mechanism for data
4. Data as payment for a service

Again, experts on ethics and information privacy were asked to give short presentations on the topics, whereby the topics were first chosen by a larger set of experts on ethics, chosen by the PANELFIT project consortium, via mail correspondence, based on their topicality and priority. Based on the conducted workshops, the previously mentioned topics that relate to ethical consideration on the commercialization of data are discussed in this work. Two additional workshops, following the same structure as outlined above, were held regarding ethical and legal issues of cybersecurity specifically, corresponding to work-package 4 of the PANELFIT project.

In a second step, a literature review was conducted on ethics in cybersecurity and digital service chains in particular to elaborate further on the issues identified through the workshops and encounters. The objective was twofold. Firstly, to identify possible ethical issues that were not voiced, or not of concern, in the workshops and encounters. Secondly, to analyze the previously identified issues in detail and in particular in the context of digital service chains.

[3] The PANELFIT project (Participatory Approaches to a New Ethical and Legal Framework for ICT) aims to reduce ethical and legal issues with regards to the European data protection regulation. To this end, the project develops openly accessible guidelines that help stakeholders overcome such issues in various areas, including the processing of data in ICT and the provision of cybersecurity. PANELFIT is a related project of GUARD.

[4] Volume 29, Issue 5 (p. 699–830), 2021 of the European Review of Private Law. kluwerlawonline.com/journalIssue/European+Review+of+Private+Law/29.5/19933.

4 Ethical Issues

The following section provides a discussion on the ethical issues that have been identified through the methodology defined in the prior section. All ethical issues are structured into the five steps of a digital value chain. Ethical issues are furthermore structured to firstly provide the context of the issue. Next, the ethical issues itself is defined and, where applicable, examples are provided. Lastly, a risk assessment and the possible impact are discussed in detail.

4.1 Content Creation

Overall, this section is structured using the CRISP-DM framework [90]. Regarding the business understanding we start by discussing the ethical issue of different definitions of fairness that were provided by a variety of machine learning researches. Then we discuss the issue of data altruism for data acquisition. Regarding data understanding we investigate examples for common biases that can occur and should be solved in the phase of data preparation.

Selecting the "Right" Definition for Fairness
Context: It is obvious that a user will expect a fair design of an AI model. But how to achieve such a fair model is not an easy task for the developers as fairness is not clearly defined and may differ between users, developers and the context of a service. In this paragraph we will have a closer look on different fairness definitions and the problem of selecting the "right" definition for fairness.

Ethical Issues: Although the GDPR states in Article 5 and 14 that personal data should be processed lawfully, transparent and fairly, a clear definition of fairness is not trivial. Malgieri [53] argue that fairness is a substantial balancing of the interested parties that are predominantly data controllers and data subjects. They further declare that fairness is separated from lawfulness and transparency by not being a legal construct. In their opinion, fairness aims to mitigate situations of unfair imbalances, the data subject feels vulnerable.

Kusner et al. [45] declare that the classic fairness criteria such as demographic fairness or statistical parity are limited because they ignore the discrimination of subgroups or the individual level. Therefore, Kusner et al. [45] introduce the principle of counterfactual fairness that is achieved when individuals and their structural counterfactual part are equally treated.

Zafar et al. [91] introduce another definition of fairness that is based on the principles of disparate treatment[5] and disparate impact[6]. They line out that maximizing fairness under accuracy constraints is a major issue when designing AI applications. Especially if the sensitive attribute in the training set is very high this can lead to unacceptable performance with regard to the business objectives.

[5] Disparate treatment: A decision making process, e.g. a classification suffers if it is built on a subject's sensitive attributes [4].

[6] Disparate impact: A decision making process suffers if subgroups with certain sensitive attributes are hurt [4].

Example: A well known example for the problem of choosing the right definition of fairness is the discussion about the risk assessment tool Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) that predicts the risk of a defendant committing a misdemeanor or felony within 2 years, from 2016. In a detailed analysis the investigative news organization ProPublica claimed the model to be unfair as under their definition of fairness the model was found to be biased against black citizens [2]. On the opposite side, the developing company Northpoint argued that their definition of fairness holds including more standard definitions of fairness [17,21].

Risk Assessment and Discussion: While we have included only a limited selection of fairness definitions, this already demonstrates that there is not one ethically correct definition of fairness. In general, two different types of fairness can be identified, that are the fairness of a group and the fairness of individuals and subgroups. While Zafar et al. [91] show one way to weight these definitions, Selbst et al. [79] argue that a social concept such as fairness cannot be resolved by mathematical definitions because fairness is procedural, contextual and contestable. Moreover, also Mehrabi et al. [57] provide a taxonomy for fairness to avoid bias in AI systems. Finally, this argumentation shows that whether an algorithm is fair or not can barely be assessed by a programmer alone and will always require a diverse team as controlling instance, defining a definition that fits the specific requirements of the service and its users.

Data Altruism

Context: During multiple encounters and workshops, the notion of data altruism was raised as a pressing issue that needs consideration when discussing the commercialization of data. Data altruism refers to the instances in which data is voluntarily made available for organizations or individuals to (re)use without compensation. Such instances may be for the common good, for scientific research or the improvement of public services, as stated in the proposal for the European Data Governance Act (DGA) [1]. Data altruism is related to the concept of data solidarity and particularly crucial for clinical, health and biomedical research as such research is in need of large amounts of data. Citizens are increasingly generating data that might prove valuable for researchers and public institutions.

Ethical Issues: It is presently unclear how to ensure ethical conduct when defining data altruism in the context of the commercialization of data. This issue is particularly intervened with the legal challenge of ensuring consistency between legislation of the GDPR and the DGA.

Example: Data altruism may occur in the content creation phase of digital service chains and is particularly connected to health and biomedical data. Private individuals consent to the processing of their health data for research or medical purposes. An ethical issue arises know if the controller of the data decides to re-purpose the data for new processing activities by giving other, commercial

entities access to the data. These new controllers use the data to create services that are sold to other organizations or individuals for a monetary profit. While the re-purposing of the data does compulsorily needs a legal basis, such as consent from the data subject, the question remains whether commercial entities should profit of data altruism in the first place.

Risk Assessment and Discussion: In the DGA, data altruism is referred to as the reuse of data without compensation for "purposes of general interest, such as scientific research purposes or improving public services" [1]. The DGA does not only regulate data altruism and the free reuse of data but also the sharing of data among businesses, "...against remuneration in any form" [1], emphasizing its relationship with the commercialization of data.

Several initiatives and proposals are aiming at fostering data altruism by providing a legal framework on the matter. Individual countries like Denmark are currently studying the introducing of safe spaces to store citizen generated data that can later be used for research [16, p. 86]. In Germany, the draft legislation for the Patient Data Protection Act encompasses the notion of a "data donation" through which patients may consent to the free use of their data. Data is then to be stored in an electronic patient record that is available for research [9]. On a European level, THEDAS, the Joint Action Towards the European Health Data Space aims at promoting the concept of secondary use of health data to benefit public health and research in Europe.[7]

In a joint opinion on the proposal for the DGA, the EDPB and the EDPS emphasize the importance of consistency between the GDPR and other regulation such as the DGA and address the main criticalities of the proposal [24]. It can be seen that especially some elements of the DGA require further clarification in order to foster data altruism while ensuring consistency with the GDPR and ethical conduct. The first element refers to the European data altruism consent form as introduced in Art. 22 DGA. It is advised that the European Commission adopts a modular consent form through which data subjects are able to give and withdraw consent for the processing of personal data for data altruism purposes. Here, the EDPB and EDPS argue that:

"In particular, it is unclear whether the consent envisaged in the Proposal corresponds to the notion of "consent" under the GDPR, including the conditions for the lawfulness of such consent. In addition, it is unclear the added value of 'data altruism', taking into account the already existing legal framework for consent under the GDPR, which provides for specific conditions for the validity of consent" [24].

Furthermore, the GDPR does not allow a data subject to renounce one's rights, even if the data subject might be willing to do so, for instance for research in the public interest. Informed consent, public and legitimate interest remain the legal bases of choice for such instances, creating a collision between the concept of data altruism in the DGA and the GDPR. Individuals might be willing to "offer"

[7] See Joint Action Towards the European Health Data Space – TEHDAS Available under: https://tehdas.eu.

personal data for research even if they do not know exactly how, and how much of, the data will be used, for what specific purposes and by which entity. The GDPR does not allow for such a general consent, for this level of data altruism. Thus, it is not clear whether the concept of consent in the DGA acts as a lawful basis for the processing of personal data or as an extra safeguard that is to be combined with the existing legal basis for the processing for public interest. Similarly, the notions of processing of data for the general interest, as introduced in the DGA, and public interest, in the GDPR, need to be harmonized. Lastly, the DGA introduces "Data Altruism Organizations registered in the Union". Such legal entities should be enabled to gain access to personal data to support purposes of general interest. However, more information need to be provided on the specifics of such organizations. Would these organizations act as controller or processor? What is the legal status of them and should they be allowed to charge a fee for their service? Should they be allowed to share the data with other entities? These issues and open questions could provide an opportunity to more clearly define the objectives of data altruism and its differentiation from the current processing for public interest. Additionally, this provides an opportunity to harmonize the different approaches towards consent that also relate to the role of the individual in the concept of data altruism.

Bias in Training Data for AI

Context: As also reflected in Fig. 1 and elaborated upon by Hagendorff [33] two of the most pressing ethical issues in machine learning are fairness and non-discrimination in data processing.

Ethical Issue: Goodman and Flaxman [30] define the right to non-discrimination as the absence of unfair treatment of a natural person based on the belonging to a specific group, such as a religion, gender or race. Thus, in their opinion, society exhibits exclusion, discrimination and inequality per definition, so a sufficient preparation of data is a crucial step when designing non-discriminatory AI [8]. In the following, we will have a closer look at the issues caused by insufficient data preparation and data bias.

Example Gender Bias: On of the most frequently mentioned issues with regard to discriminatory and unfair AI is the gender bias. For instance, Madgavkar [52] report about the google translator service where sentences from gender-neutral languages like Farsi or Turkish result in gender stereotypical translations. They provide the example that "This person is president, and this person is cooking" will result in "He's president and she's cooking". This shows very well a bias in the training data resulting in a not gender neutral translation. The bias in such AI reflecting the values of the society and/or its creators [18]. Leavy [47] identified five reasons for gender bias in language and text that are naming, ordering, biased descriptions, metaphors and presence of women in text. For example, she summarizes that the male is always named first when pairs of each gender are named resulting in a social order bias [60]. Moreover, men are more often described based on their behavior while women are described based on their

sexuality and external appearance. This will result in a bias of adjectives when used for AI training [10]. A methodology on how to maintain desired associations while removing gender stereotypes is provided by Bolukbasi et al. [7].

Example Ethical Affiliation Bias: Closely related and as frequently discussed as gender bias are ethical affiliation bias. One of the most prominent examples is Microsoft's AI chat bot Tay. After learning from tweets of other users, Tay was shut down after one day because of "obscene and inflammatory tweets" [65]. Finally, Tay mirrored the racism that was picked up from the users. Neff and Nagy [65] also stress that the case of Tay shows very well how not only programmers but also users can assign agency and personality to AI. This example very well clarifies that not only a robust design but also monitoring over the whole life-cycle is required.

Example Uncertainty Bias: Another bias to be considered is the uncertainty bias. In their example of loan payment prediction, Goodman and Flaxman [30] illustrate that a simple under-representation of a group below a certain value will lead to a systematic discrimination in risk avers AI applications. Moreover, they declare that while for geography and income such bias might be easy to detect, more complex correlations such as between race and IP addresses it might not.

Example Indirect Bias: Although a sensitive attribute is not in the dataset, the above mentioned biases can still be indirectly correlated to other attributes. A prominent example for this is the criminal risk assessment tool COMPAS that predicts the risk that a defendant commits a misdemeanor or felony within 2 years. Although no attributes about race were in the data, the algorithm was found to be racial biased [2,21].

Risk Assessment and Discussion: The observed examples demonstrate that biases in data can have manifold reasons and are therefore not always easy to detect. A careful data preparation and problem analysis is therefore key when developing an AI application. However, in specific circumstances, as with the example of the chat bot Tay, the data bias evolves over time. In such cases, only the constant monitoring of the AI's behavior can spot data bias issues. Finally, as already stated by Hall and Gill [34] the key countermeasures to spot and prevent data bias are interpretability, accountability and transparency which goes hand in hand with the results from the Commission et al. [15]. Although these countermeasures aim to avoid bias in data, Caliskan et al. [11] argue that such debiasing is just a "fairness through blindness" [11] what gives the AI an incomplete understanding of the world. They argue that the AI will suffer from debiasing in meaning and accuracy. In their opinion, long-term interdisciplinary research is required to enable AI to understand behavior different from its implicit biases.

Model Reflecting Reality
Context: To evaluate a model, a variety of methods exist to spot different unintentional behavior. But how to define unintentional behavior and how to test it is still a decision often made by a small group of developing experts.

Ethical Issue: Leavy [47] argue that e.g., the problem of gender bias was identified and is in most cases addressed by women. While developers are overwhelmingly male, this can cause a restricted view on the reality. Moreover, she argues that diversity in the area of AI is important because it improves the assessment of training data, incorporation of fairness and assessment of potential bias.

Example: A straightforward example for a developer diversity issue was reported by Dailymail [46] in 2017. A soap dispenser did not recognise hands of people with dark skin so for them no soap was released. One reason for this issue could be an ethical affiliation bias with only white hands in the training data. The problem seems to be obvious and one would expect it to be detected latest during the testing but it was not. In this case, the problem could have been easily avoided if the development team had been more diverse and would have considered different skin colors from the beginning.

Risk Assessment and Discussion: Although we do not want to play down the ethical affiliation bias in the soap dispenser example, its consequences are only annoying. For example, people loose their jobs such as when Uber driver's cares were locked because the face recognition algorithm had problems to identify black and Asian people [5]. Having similar issues in privacy and security areas might raise serious security risks. But also with a diverse team of developers, the question when to know that the dataset is complete is not easy to answer. Löbner et al. [48] argue that a transparent development, providing interpretability in each step of model design can help do identify unfair treatment in the model itself. Finally, this issue relates to the issue of quality control and the degree of investment for quality, which is competing with requirements like saving resources and time-to-market.

4.2 Aggregation

In the second step of digital service chains, data and information from different sources, such as multiple data subjects or organizations, are aggregated. In this step, the trade-off between data anonymization and data quality was identified as an ethical issue.

Anonymization vs. Data Quality
Context: Personal data requires the data controller to get the persons' consent to process their data in most circumstances. This also holds if the data allows to link it without disproportionate effort to the person. Since it is not possible or often not desired to request each person's consent, data sets are anonymized respectively de-identified. For a proper anonymization it is often not sufficient

to just delete a person's name or identifier (cf. Sweeney [81]). Thus, other data fields need to be changed to prevent a re-identification of the respective person. Moreover, numbers might need to be truncated, rounded or noise is added, other data fields might be masked, scrambled or blurred.

Ethical Issue: When changing the data to anonymize it, it might prevent that the data is used for the desired purpose or might lead to false results. Therefore, a trade-off between privacy of the persons in the data set and the precision of the calculations on the data set emerges [29]. One major problem in this trade-off is that for cases where it is easier to identify people because the anonymity set is (too) small, changes to protect the persons' identity will have a large impact on the data quality. On the other hand, when changes to guarantee the persons' identity will have only minor impact to the data quality, then often the privacy of the persons is already in good shape, e.g. because the number data in the data set is already huge and it would be hard to identify specific persons.

Example: Collecting data for security purposes might cause privacy problems if the persons are identifiable. This is in particular the case for intrusion detection systems (cf. [66]) or mobile trajectories of persons which might be used for research or urban planning in smart cities (cf. [88]).

Risk Assessment and Discussion: The trade-off between the persons' privacy and the goal of the data evaluation needs to be done by the person setting up the system. Depending on the system's goal, beneficence (of the user) may be in opposition to non-maleficence (if a user suffers any kind of harm from the miscalculations due to the anonymization of the data) or explicability (if systems can not be protected sufficiently). On the other hand, if the users are pushed to give their consent – perhaps with the argument that if they don't provide their data they would put someone at risk – their autonomy is endangered. As a further observation, we can conclude that this is in particular an issue for small data sets: Small data sets increase the likelihood that someone can be identified while changes within the data set to anonymize participants will have a more significant effect on the data. When the data set is large, it can be considered to be more difficult to extract data on a specific subject and on the other hand, changes will in general have a smaller affect on the quality of the data set.

4.3 Distribution

The third step of a digital service chain relates to the distribution of a service on a suitable system such as a dedicated server for a software solution. Data that is placed on such a solution might not be available for all entities, leading to power asymmetries in the distribution phase.

Power Asymmetries
Context: Data and the information and insights that can be gathered from it are not equally distributed. While individuals typically have only access to personal data that relate to themselves, organizations gather data to create or improve their products and services. Depending on the business model and the size of the organization, the amount of data that an organization possesses differs greatly. For instance, with the rise of "Big Tech", multinational organizations such as Google, Meta, Amazon or Alibaba did not only gain tremendous financial power, but also access to a wealth of data from their customers. Indeed, excessive gathering data is seen as a major business model in "surveillance capitalism" [92] in which a power asymmetry is created between different entities. Network effects only increase the amount of data and the market power of these organizations as "knowledge is power" Bacon [3]. These factors lead to the development of natural monopolies in which one organization maintains control over the wealth of information. This market power then allows organizations to distribute information and services to their own choosing, with little oversight by regulators.

Ethical Issue: Power asymmetry can manifest itself in different forms, from the asymmetric amount of data to an asymmetric distribution and access of data. More precisely, organizations may have more data at their disposal than others and are free to distribute the data to their liking. This results in different ethical issues, from competitive advantages between organizations to questions of autonomy and sovereignty for individuals and organizations alike.

Example: An example of power asymmetry are social media networks whose business model relies on the gathering of data to attracts advertisers to their platforms. The more data on its users a social network possesses, the higher the value for its advertisers. The social network is free to distribute "its" information to the advertisers of choice, while individuals do not know based on what decisions and algorithms advertising is shown to them and to others. The GDPR and other data protection regulation aim to overcome this loss of autonomy by obliging organizations to make the processes behind such distribution of data transparent. Nonetheless, the sharing of data remains problematic as organizations might be pressured from governments or agencies to share the data, or distribute the data their choosing. Similarly, this issue enables industrial espionage if organizations obtain data of their competitors through agencies or other means of "involuntary" sharing of data.

Risk Assessment and Discussion: It can be seen that the sharing of data naturally poses the risk of a loss of autonomy or digital sovereignty. While this risk might be small in cases where entities retain a balance of power, it increases with power and information asymmetry. Especially individuals and smaller organizations cannot be certain that large, multinational organizations process personal data lawfully. Given this risk, organizations and individuals might be inclined to not share their data anymore, stop using certain services or stop working

with particular organizations or states with which they feel a power asymmetry exists. Another consequence might be the emergence of the "chilling-effect", whereby individuals start to behave in conformity with behavior they feel are expected from them, as they feel they are being under constant surveillance [12]. This demonstrates that multiple ethics principles in cybersecurity, namely non-maleficence, explicability, justice and autonomy are endangered. While regulation such as the GDPR rightfully intends to put an end to the unlawful processing of personal data that is the consequence of information asymmetry, this asymmetry itself continuous to remain as organizations continue to hold and gather ever more data. Multiple measures that could and should be combined exist, that provide starting points to mitigate this issue. Regulators and governments should aim to foster competition by strengthening the role of smaller organizations, decreasing lock-in effects and breaking up monopolies, to rectify power asymmetry between organizations in general. European Competitors and a European data ecosystem should be fostered to promote the fair and ethically compliant use of personal data, communicating such usage as a competitive advantage to end-users. Continuous power asymmetries should be transparently communicated to increase trust. A first step in this direction might be the introduction of legislation comparable to the "Freedom of Information Act" in Germany which enables citizens to request information in possession of German authorities [42]. Nonetheless, such measures will ultimately rely on individuals trust in the lawful application of such regulation as well as in the authorities and organizations themselves.

4.4 Data Transport

The original definition of data transport by Voudouris [86] refers to the transport of data through satellite or terrestrial broadcasting such as cables. The ethical issues identified in this step demonstrate that individuals as well as whole regions or countries might be cut off from services or each other through means that were originally introduced to safely protect data during the transport phase.

Restriction of Data Transport
Context: The internet was designed to allow people to peacefully collaborate with each other. However, as the internet matured and gained widespread adoption, criminals, or nation states who attack users to enrich themselves financially or to spy on the users entered the ecosystem. As a consequence firewalls and filters were developed and set up with the aim to block attacks and protect individuals and organizations alike.

Ethical Issue: Firewalls and filters can not only be used to secure a network, but also to lock up users. This can either be done nation wide to suppress opinions or information, or to lock users up in a certain business model, e.g. by not counting certain traffic. Thus, a technology which was designed to protect networks and manage and shape traffic, can be used against the users of the network.

Example: The Great Firewall of China [89] is an example where users free speech and accessibility of information is limited (Justice) by restricting access to services, to the disadvantage of the users. Zero-Rating [62] is an example where the company aims to improve their financial benefits (Beneficience) by nudging users' to use or not use certain services.

User Empowerment
Context: In many contexts the users shall be empowered to enforce their rights, e.g. to protect their privacy or take informed decisions. This has also been the objective of the introduction of the GDPR in Europe. This empowerment may simply go together with changing some settings or even using specific software or services such as anonymization services.

Ethical Issue: Companies may shift tasks to the responsibility of the user. For instance, instead of offering privacy friendly services, they refer to tools, plugins, etc. the user can install. Sometimes these tools come with disadvantages or perceived disadvantages for the user.

Example: Users of the anonymization service Tor[8] hesitate to use the service since they are afraid that this could make them look suspicious, and they will therefore be observed by secret services or the police [41]. These concerns effectively prevent users from using services that let them manage their data privacy preferences.

Risk Assessment and Discussion: Ethical principles concerned are the users' right of self defence and privacy (Justice), the users' informed consent, privacy settings (Autonomy) versus the users' trust in the company and the users' well being (Beneficence) since taking responsibility and getting information can be a burden to the users.

4.5 Digital Experience

In the last step of a digital service chain, the service, that has been created in the prior steps, is experienced by the users. As these services largely rely on personal data of data subjects, the identified ethical issues relate to the value of the data. This includes how to ethically price the data and how to value services that were obtained through the combination of data. Lastly, the ethical implications of paying with personal data for services are discussed.

The Value of Data - Inferences
Context: Privacy, and the protection of personal data, constitute a fundamental human right, recognized in the UN Declaration of Human Rights [64, Art. 12], accentuating the enormous qualitative value typically assigned to personal data. However, no legislation so far offers distinct guidance on how best to determine the monetary value of data. Data subjects are often unaware of the value of

[8] https://www.torproject.org/.

personal data in general as there exist no established pricing mechanism for data. While data subjects might possess a feeling of ownership of personal data that relates to them specifically, the true value of data is not derived from a single data point alone. Oftentimes, data is gaining in value through the combination of personal and non-personal data and the inferences that can be drawn from the data [87]. The value of the collected data is not known at the time of the collection of it, but rather after it has been processed, that is after it was combined and analysed. Technologies such as machine learning, artificial intelligence and big data analytics create new opportunities to draw inferences from personal data, collected from numerous data sources. The value of data therefore varies greatly, not only in the type of data that is gathered but also in the amount of data and the combination of data from different sources.

Ethical Issue and Example: Wachter and Mittelstadt [87] argue that, depending on the definition used, such inferences can be regarded as personal data and should be protected more strongly than it is the case at the moment. For instance, an organization might use an algorithm that creates inferences, out of gathered data, about a specific person: *"Person X is not a reliable borrower as there is a high probability that X has an undiagnosed medical condition."* Such sensitive information surprisingly receive only very limited protection under the GDPR, constituting to both a legal and ethical issue. Inferences can be seen as "new" data, created through the combination of (personal) data of different types and sources. Inferences can also be targeted at de-identified data [49,73] when combining the existing data set with another set to re-identify users. The ethical issue is now how these inferences should be treated under consideration of all circumstances, that is the different entities, creator, data subjects, involved, the type of data as well as its purpose and processing.

Risk Assessment: Art. 15 GDPR, the right of access, grants data subjects the right for confirmation whether personal data regarding the data subject was used by a controller. Data subjects also have the right to obtain a copy of the specific data used for a type of processing. However, a data subject might be denied a copy of inferences drawn about the data subject if they constitute a trade secret or an intellectual property in the Trade Secrets Directive [71] as is likely the case with customer data, preferences and predictions. Thus, the right of access is limited with regards to inferences even if they are seen as personal data. A similar problem can be observed with the right to data portability that only applies to data "provided by" the data subject, which is not the case with inferences. Similarly, Art. 16 GDPR, the right to rectification and Art. 17 GDPR, right to erasure are not tailored towards inferences and therefore not directly applicable for this type of data[9]. This issue poses the ethical questions whether the type of personal data that provides an organization with the most value should solely be under control of the controller. Although inferences are created

[9] See the Joined Cases C-141/12 and C-372/12 and Case C-434/16 by the European Court of Justice.

by the controller, the base of the processing are personal data from a data subject that is often not aware of this increase in economic value in the data. A first step towards an ethical solution to this problem might there-fore be a "right to reasonable interference" [87]. Such a right could enable data subjects to challenge unreasonable inferences and would require controllers to ex-ante disclose why certain sensitive types of data are acceptable for inferences, why the inferences are necessary and disclose the statistical reliability of the techniques and data upon which inferences are created. However, the fact that the true value of data remains unknown.

The Value of Data - How to Price Data
Context: When discussing the value of personal data, one needs to define personal data first. Art. 4(1) GDPR defines personal data as "any information which are related to an identified or identifiable natural person." According to Art. 8(1) of the Charter of Fundamental Rights of the European Union and Art. 16(1) of the Treaty on the Functioning of the European Union, both of which are explicitly mentioned in Recital 1 of the GDPR, in the EU personal data protection constitutes a fundamental right. This approach to informational privacy demonstrates that personal value possesses a qualitative value in society. This qualitative term, the differing functions and objectives for which personal data can be used, can be extended by a quantitative, monetary, term to enable a pricing mechanism for data.

Ethical Issue: The ethical issue with regards to the pricing of data is the following: Is it ethically acceptable, and possible, to put a price on personal data? As the protection of personal data constitutes a fundamental human right, putting a price on such data seems legally and ethically challenging, although the value of the data economy, and the services that can be bought with data, can indeed be priced.

Example: Suppose a data subject would like to sell his/her personal data, containing all the information contained on a personal computer, such as browser history, purchased gooods and service as well as pictures and other information. Would it be possible, and ethically acceptable to put a price on this data?

Risk Assessment and Discussion: While valuations for the EU data economy and data market exist [58], extant legislation offers no guidance on how to determine the monetary value of a specific set of personal data. From an economic perspective personal data can furthermore be considered as a discrete object that can be produced on site, by an individual, an organization or a third party. It can be transferred between entities that can in turn transform and process the data and/or transfer it again to other entities. Data has been titled "the new oil" or a currency, demonstrating the economic value for organizations that are actively taking an effort to obtain, create and process personal data. Personal data is for instance used in marketing and business intelligence in order to market to, and obtain, new customers for a product or service. Data is also currently being

used as de-facto means of payment for access to specific services on the internet, as discussed in this document and the legal evaluation on counter-performance practices in the critical analysis.

Given this economic reality, the current situation therefore requires an ethical consideration on how personal data could and should be valued as there is no established pricing mechanism for personal data.

In his Theory of Communicative Action, Habermas [32] provides a framework within which different areas of law come into place that also apply to personal data. Individuals are seen to behave in a sphere of private autonomy. Here, individuals can choose to do what they like, including buying and selling personal data under the agreed upon conditions, i.e., price and amount of data. In this context, property rights come into place. Property rights concede a basic recognition of ownership, providing a stabilizing condition in a private autonomy. Naturally, different types and forms of property rights exist, for instance depending on the type of economic good, be it a commodity or an intellectual property. The simple absence of property rights for the commercialization of data does not mean that commercialization of data is not possible. Data could still be commercialized in private autonomy, only without property rights put into place to regulate the transfer. Before creating a property right, regulators should be clear on the objective that is to be achieved with the right. What kind of right should be implemented? Should it be a right for intellectual property or rather an object? Lawmakers and regulators might also want to intervene by limiting the capacity of individuals to commercialize data in their private autonomy. Here, fundamental rights come into play, providing individuals with equal opportunities and restrictions. The GDPR clearly granted individuals with fundamental rights related to personal data and the use of it through other entities. However, it is less clear whether and to what extend the GDPR restricts commercialization and propertization of personal data [83].

Valuation Methods. It is not that fundamental rights and property rights need to contradict each other. Instead, property rights, granting and quoting data a definable, monetary, value, could add to the bargaining power of individuals, thereby extending their fundamental rights. There are however other options and tools besides rights that could help in defining the value of personal data. Malgieri and Custers [54] state that *"[a]ttaching a monetary value to personal data requires some clarity on (1) how to express monetary value, (2) which object is actually being priced, and (3) and how to attach value to the object, i.e. the actual pricing system"*. Personal data should be valued in a currency, per a specified time frame and per person. Factors to be considered are the completeness, relative rarity of data as well as the level of identifiability [54]. The pricing could be based on a market valuation or individual valuation method. A market-based valuation would price personal data according to its costs or benefits for market participants, as observed in illegal data markets[10] or data breaches. An indi-

[10] For an exemplary pricing of data records such as passwords and accounts, see keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html.

vidual valuation method could be based on individuals' willingness to pay for data protection and privacy [22]. Both approaches remain incomplete as market valuation methods rely on indicators that are insufficiently precise while individual valuation methods are no incentive compatible. Defining the value of personal data therefore remains an ethical, legal and practical challenge without an apparent optimal solution. To overcome this epistemic uncertainty, more research into fair and ethical pricing mechanisms is needed to educate individuals on the value of personal data. As technology and the data economy are under constant change, the exact value of data at the point of collection is likely to continue to be unknown for most parties involved in the transfer of the data. Thus, the most probable and promising route would aim at developing adequate proxies and indicators that allow for an approximation of the data's value. Renewed legislation could provide examples and frameworks for measuring the value of data in order to compensate data subjects.

The Value of Data - Counter-Performance Practices
Context: Currently, it is unclear whether or not a form of trade that does not involve money transfers but rather the monetarization of the data, i.e., the process of converting personal data into currency, is lawful [83]. As the value of the EU data economy is continuing to grow [23] and many internet service providers are opting to monetise personal data instead of charging a fee for their service or platform [78], this matter also requires ethical consideration.

Ethical Issue and Example: Presently, individuals oftentimes pay with personal data for the usage and experience of digital products and services. An example are popular social media or communication services such as Facebook, WhatsApp or TikTok. While these services are advertised as "free" to individuals, they are paying indirectly by consenting to the processing of their personal data by the service providers. Most often, users do not have the chance to chose between paying with money or their data and personal information. Indeed, it is possible that individuals are not even aware about this possible choice or would simply opt for the payment using personal data as they do not have the means to pay with money, while still relying on the service or product. The ethical issue lies therefore in the question whether personal data should be accepted as a form of payment and under what considerations.

Risk Assessment and Discussion: Kitchener [43] identified several moral principles that can serve as ethical guidelines for this issue. The principles are defined as *beneficence, non-nmaleficence, autonomy, justice* and *fidelity.* As the principle of fidelity does not fit the context of counter-performance practices, the principle of *explicability* is used instead, which has already been used in related work on ethics in AI [26]. It can be seen that data as counter-performance for a service contributes to the welfare of the individual, satisfying the beneficence criterion. Similarly, *non-maleficenc*e be seen as fulfilled, assuming that the service provider does not offer the service to intentionally harm the individual or others. In relation to fundamental right for privacy, a service provider needs to take measure to

prevent accidental or deliberate harm to the data subject when processing personal data. Regulation such as the GDPR acts therefore as a control mechanism for the non-maleficence principle.

The principle of *autonomy* relates to independence, allowing an individual freedom of choice in its actions. In this case, individuals are, in principle, free to choose a service that asks for data as counter-performance for a service. Individuals could decline such an offer, choose no service at all, or search for other service providers that offer the same or a similar service for a monetary fee. To do so, individuals must firstly understand how their decisions impact them and others in a society. Secondly, this decision must be able to be sound and rational, that is, children for instance can-not be expected to make a sound and rational decision on this matter. The Covid-19 crisis demonstrated that access to services that gather personal data as payment is not always a free choice but a necessity. During worldwide lockdowns, especially school-children and students were forced to use services to connect with each other as well as with education institutions in order, as the alternative would have been to not receive any kind of education. For children and students from less fortunate households and countries, a paying-with-money option would not have been a better alternative, given that many individuals were not even able to afford laptops, let alone a functioning working and learning environment. Additionally, individuals are often not aware of the value of their data, as discussed in other sections of this work, or unaware of the potential implications and processing activities that are conducted with personal data. As data can be stored indefinitely, individuals might forget about consent that they gave in the past, preventing them to exercise their right of erasure or to withdraw their consent. Thus, the use of data as counter-performance for a service can therefore not be considered a completely autonomous decision in many circumstances. This however does also apply to instances in which individuals consent to the processing of data for a service. According to the GDPR, consent has to be freely given to act as a legal basis for the processing of personal data. If an individual is not able to use a service or product without consenting to the processing of their personal data, this consent is not freely given. Oftentimes, for instance in the case of website cookies or ubiquitous internet services, individuals are not able to effectively withdraw their consent. There are a number of reasons for this. Especially in the case of cookie notifications, organizations use techniques such as nudging and dark patterns to push individuals into accepting them. While the opt-in choice is easy to choose, finding an opt-out choice is often a tedious and frustrating task. Organizations might also decline website visits or only offer limited functionality if individuals not fully consent to the whole cookie policy. The recent EDPB Statement 03/2021 on the ePrivacy Regulation reiterates the importance of enforcing more strict consent requirements for cookies and similar technologies in the upcoming ePrivacy regulation [6]. However, individuals might have no other option than to consent to the processing of data as they effectively need, feel or are obliged to use a product or a service. This could be because individuals are socially pressured in the case of monopolistic or oligopolistic services or because

individuals are not able to use costly alternatives that collect no or less personal data, demonstrating that individuals are often unable to take autonomous decisions on the processing of personal data in general.

Kitchener [43] defines justice as "treating equals equally and unequals unequally but in proportion to their relevant differences". Treating individuals differently therefore requires a rationale that explains the appropriateness of this treatment to promote fairness and impartiality [27]. In principle it could be argued that individuals could receive different degrees of services for their data, depending on how the service providers values the data. Similarly, the justice principle could also encompass the option of giving individuals the option to pay with data or with money for a specific service. However, this could not be regarded as fair practice given the power imbalance be-tween individuals and service providers in instances outlined above. The ethical is-sues related to the use of data as counter-performance for a service are however not automatically solved if the provider of a service gives the individual the option to pay with money for this particular service. Less wealthy individuals are likely to always prefer data as payment, as money could be used for other goods and services while the same type of data could be used to "pay" for multiple services. Similarly, as the value of data is oftentimes not observable at the time of data collection, but through the combination with other data points, a price discrimination between individuals cannot satisfy the justice principle in this case.

Finally, *explicability* acts as an enabler for the aforementioned principles by promoting intelligibility, accountability and transparency. Individuals should be enabled to understand what data is being processed, how exactly it is being processed, by whom and for how long. Only then can individuals gain an understanding on the current and future value of their data. Service providers need to be held accountable for their processing activities. Again, current regulation such as the GDPR aim to increase explicability by fostering transparency and accountability when personal data is being processed. Under the condition that regulation allows for data as payment for a service and regulates it, the explicability principle can be affirmed.

Overall, the use of data as payment for a service poses both, ethical and legal issues. From an ethical point of view, the simple prohibition of this matter does not solve the underlying power imbalance between individuals and service providers. Instead, it may hinder individuals in gaining an understanding over the value of personal data. Clear contractual agreements and regulation could allow for data as payment while complying with legal and ethical requirements.

5 Discussion

Based on the analysis of the ethical issues identified and elaborated upon in the prior section, Table 2 provides an assessment of the ethical principles of cybersecurity potentially violated in each step of a digital service chain. Moreover, for each ethical issue the negatively affected party as well as the party that could potentially resolve the issue is identified. These parties are namely the user, or

individual, or the organization that is providing a specific service to a user. We deliberately decided not to include the state, that could introduce additional legislation to overcome ethical issues, in the table. Instead, the aim of this work is to assess whether and how organizations and individuals may overcome these ethical issues without further regulation.

Table 2. Ethical issues and potentially violated ethical cybersecurity principles in digital service chains

Stage in Service Chain	Ethical Issue	Non-Maleficence	Beneficence	Autonomy	Justice	Explicability	Affected Party	Potential Resolver
Content Creation	Defining Fairness	✓	✓		✓	✓	User	Organization
Content Creation	Data Altruism		✓	✓	✓	✓	Both	Organization
Content Creation	Bias in AI Training Data	✓	✓		✓	✓	User	Organization
Content Creation	Model Reflecting Reality	✓	✓		✓	✓	Both	Organization
Aggregation	Anonymisation vs. Quality	✓	✓	✓		✓	Both	Organization
Data Transport	Power Asymmetries	✓		✓	✓		User	Organization
Data Transport	Restriction of Data Transport		✓		✓		User	Organization
Data Transport	User Empowerment		✓	✓	✓		User	Both
Digital Experience	Inferences	✓				✓	User	Organization
Digital Experience	How to price Data		✓		✓	✓	User	Both
Digital Experience	Counterperformance Practices		✓	✓	✓		User	Organization

The results suggest that different ethical issues in different steps of digital service chains affect different ethical cybersecurity principles. Consequently, there cannot exist a one-size-fits-all solution to solve these ethical issues. Moreover, in all cases, the individual is the entity negatively affected through the specific ethical issue. Organizations are largely found to be potentially in the position to resolve or mitigate ethical issues, although there exist issues were both entities may be negatively affected or able to resolve an issue. We find that each cybersecurity ethics principle is violated through at least one ethical issue identified in this work. Similarly, for each step in the digital service chain, at least one ethical issue could be identified. As discussed in the beginning of this work, the objective has not been to provide a comprehensive list of all ethical issues but to focus on the ones derived through the methodology of this work.

Schoentgen and Wilkinson [77] noted that while digital technologies should be used for the benefit of individual people and the society, most of them are rather designed for commercial benefits. They sketch the transition of digital services prioritising ethics through a feedback loop. In order to have companies incorporating ethics, it is essential that they are rewarded for their efforts, i.e.

benefits need to exceed costs. To benefit from ethical services, it is necessary that customers notice that organizations take ethical compliance serious and that individuals benefit from this compliance. Increased ethical awareness can be achieved through increased transparency and accountability, but requires ethics to be measurable to allow customers to compare digital services on their ethical conduct.

Consequently, stronger ethical conduct can build users' trust which in turn will increase engagement and consumption of digital technologies which could reward the company. These observation are in line with findings of Hagendorff [33] who concluded that there are currently no consequences if an organization is not considering ethical issues when developing and offering their services.

However, Schoentgen and Wilkinson [77] also note that users of digital services face the ethical dilemmas of self-responsibility and choice making and that the best way to drive awareness of ethics is education and data literacy. In particular for privacy enhancing technologies, this is not new, as for Tor[11] and Jondonym[12], two tools safeguarding against mass surveillance, trust in the technology has been shown to be one of the major drivers [37–39,41]. The trust in the technology was driven by online privacy literacy [40] supporting Schoentgen and Wilkinsons' theory. In accordance with Schoentgen and Wilkinson [77] is also the result of a study [35] investigating incentives and barriers for the implementation of privacy enhancing technologies from a corporate view where ethics and reputation of the company were among the named incentives. Another incentive mentioned is to charge for more privacy friendly services. This is a business model which is currently popular among German publishers who require online users to either pay a fee or agree to accept cookies for targeted advertising. However, besides the question whether users are willing to pay [36], offering privacy-friendly services only with additional charge may amplify other ethical issues. In particular, if users can opt-out from their data being used if they pay for it, this will most likely cause biased data since one will expect that only more wealthy people would afford to pay for their privacy. As sketched in the previous section any bias in the data, which might be used to train machine learning models, may cause algorithms to fail causing other problems.

Nonetheless, even if an organization wants to provide services in an ethical way, the resulting trade-offs are sometimes difficult to overcome. Examples are the storage of personal data, where it is not per se clear if data on a local device is necessarily more secure than if stored in the cloud [69]. Although it might seem logical that the users keeps as much data as possible on their devices, with manufactures not providing updates for still used devices and current malware targeting mobile users, it may be that data stored in a trustworthy environment, such as a cloud, where professionals operate and secure the systems might be more secure. Another example is the provision of open data for the benefit of the society. While it might allow the creation of new services, research or just transparency, it might on the other hand threaten the users' privacy if its possible

[11] https://www.torproject.org/.
[12] https://anonymous-proxy-servers.net/.

to link the data with existing datasets [70]. Thus, even well-intentioned ideas might backfire to the disadvantage of the users. For instance, questioning users directly on their preferences might be an obvious ethical solution. However, this solution requires well-educated users being able to make informed decisions and being willing to take the time and effort necessary to do so, which can not be assumed in any context [44].

6 Conclusion and Future Work

This work demonstrates the importance of the consideration of ethical issues in digital service chains. As such service chains strongly rely on data and information for the creation, aggregation, distribution, transport and experience of an organizations' products and services, ethical issues are highly related to the data and information that is used in these steps. Using workshops and encounters with ethical experts as well as experts in data protection from both, a technological and a legal point of view, multiple ethical issues were identified. When analyzing these ethical issues it became apparent that ethical issues arise particularly in the steps of data creation and aggregation as well as in the last step, digital experience. While the first steps need to carefully consider how data is obtained, created and combined, the last step of a digital service chain needs to consider how the service, and its underlying use of data and information are to be valued. Following the classification of Hagendorff [33], all ethical cybersecurity principles were at least once potentially violated in the ethical issues identified in this work. The analysis of the differing ethical issues demonstrated that their exists no one-size-fits-all solution to solve these ethical issues. Various different ethical frameworks for cybersecurity as well as different approaches to overcome or mitigate the ethical issues exist. Prior research indicated that different approaches can lead to differing and conflicting solutions. In this work, we did not focus on the introduction of additional regulation to overcome ethical issues but aimed to elaborate on them in the context of digital service chains. Here, organizations create content and information by aggregating and processing personal data to offer new, digital services to users. Not surprisingly, we find that in particular users are the ones that may be harmed through the identified issues while organizations are in the position to overcome these issues.

Limitations and Future Work. The objective of this work has not been to develop or list all possible ethical issues with regards to cybersecurity and digital service chains. While experts were asked to state their most pressing issues, there might exist other ethical issues that were not discussed in this work. Moreover, changes and advancements in technology could lead to the rise of other, more pressing, issues, constituting a limitation of this work. Additionally, we did not discuss potential solutions to the ethical issues but rather aimed to create awareness on them in the context of digital service chains and cybersecurity. Several opportunities for future work could be identified. Further research could build up on the results of this work by developing a framework on how best to overcome

the identified ethical issues. Here, it could be assessed whether the violation of different ethical principles, as outlined in the previous section, could require differing approaches to mitigate the identified ethical issues. Such frameworks should incorporate and assess economic benefits for organizations to comply with ethical principles [77]. Lastly, future work might focus on the empowerment of users in the context of digital service chains as the mere awareness and education on ethical issues could lead to a change in behavior and might help in mitigating the identified ethical issues.

Acknowledgements. This work was supported by H2020 Science with and for Society Programme's projects PANELFIT (grant no. 788039) and CyberSec4Europe (grant no. 830929).

References

1. Act, D.G.: Proposal for a regulation of the European Parliament and the Council on European data governance (Data Governance Act). EUR-Lex-52020PC0767 (2020)
2. Angwin, J., Larson, J., Mattu, S., Kirchner, L.: Machine bias: there's software used across the country to predict future criminals. And it's biased against blacks. ProPublica (2016). https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Accessed 1 Feb 2022
3. Bacon, F.: Meditationes sacrae (1597). The Works of Francis Bacon **14**, 149 (1864)
4. Barocas, S., Selbst, A.D.: Big data's disparate impact. Calif. L. Rev. **104**, 671 (2016)
5. Bateman, T.: Uber's 'racist' facial recognition software is firing black and Asian drivers, former driver claims. euronews.next (2021). https://www.euronews.com/next/2021/10/06/uber-s-racist-facial-recognition-software-is-firing-black-and-asian-drivers-former-driver-. Accessed 1 Feb 2022
6. European Data Protection Board: Statement 03/2021 on the ePrivacy Regulation (2021)
7. Bolukbasi, T., Chang, K.W., Zou, J.Y., Saligrama, V., Kalai, A.T.: Man is to computer programmer as woman is to homemaker? Debiasing word embeddings. In: Advances in Neural Information Processing Systems, vol. 29, pp. 4349–4357 (2016)
8. Brunet, M.E., Alkalay-Houlihan, C., Anderson, A., Zemel, R.: Understanding the origins of bias in word embeddings. In: International Conference on Machine Learning, pp. 803–811. PMLR (2019)
9. Bundestag, D.: Entwurf eines gesetzes zum schutz elektronischer patientendaten in der telematikinfrastruktur (patientendaten-schutz-gesetz-pdsg). Deutscher Bundestag, Berlin (2020)
10. Caldas-Coulthard, C.R., Moon, R.: 'Curvy, hunky, kinky': using corpora as tools for critical analysis. Discourse Soc. **21**(2), 99–133 (2010)
11. Caliskan, A., Bryson, J.J., Narayanan, A.: Semantics derived automatically from language corpora contain human-like biases. Science **356**(6334), 183–186 (2017)
12. Cas, J.: D4.1 issues and gap analysis on security and cybersecurity ELI in the context of ICT research and innovation (2020). https://www.panelfit.eu/wp-content/uploads/2020/11/D41-Issues-and-gap-analysis-on-Security-and-Cybersecurity-ELI-in-the-context-of-ICT-research-and-innovation.pdf. Accessed 1 Feb 2022

13. Christen, M., Gordijn, B., Loi, M.: The Ethics of Cybersecurity. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-29053-5
14. European Commission: Communication from the commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions a European strategy for data (2020). https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb202_en.pdf. Accessed 1 Feb 2022
15. European Commission: Directorate-General for Communications Networks, Content and Technology, Ethics guidelines for trustworthy AI. Publications Office (2019)
16. EUHealthSupport Consortium: Assessment of the EU member states' rules on health data in the light of GDPR (2021). www.ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf. Accessed 1 Feb 2022
17. Corbett-Davies, S., Pierson, E., Feller, A., Goel, S.: A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear. Washington (2016). https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas. Accessed 1 Feb 2022
18. Crawford, K.: Artificial intelligence's white guy problem. New York Times (2016)
19. European Union Agency for Cybersecurity: Glossary. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary. Accessed 1 Feb 2022
20. Dorne, R., Voudouris, C., Lesaint, D., Owusu, G.: Service Chain Management: Technology Innovation for the Service Business. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-75504-3
21. Dressel, J., Farid, H.: The accuracy, fairness, and limits of predicting recidivism. Sci. Adv. **4**(1), eaao5580 (2018)
22. Organisation for Economic Co-Operation and Development: Exploring the economics of personal data: a survey of methodologies for measuring monetary value. OECD Publishing (2013)
23. European Commission: Communication from the commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions "building a European data economy" (2017). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:9:FIN. Accessed 1 Feb 2022
24. European Data Protection Board, European Data Protection Supervisor: Joint opinion on the proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) (2021). https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-opinion-proposal-regulation-european_en. Accessed 1 Feb 2022
25. FIDIS, I.: Information technology - security techniques - information security risk management ISO/IEC 27005:2018 (2018)
26. Floridi, L., et al.: AI4people-an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. Mind. Mach. **28**(4), 689–707 (2018). https://doi.org/10.1007/s11023-018-9482-5
27. Forester-Miller, H., Davis, T.E.: A Practitioner's Guide to Ethical Decision Making. American Counseling Association Alexandria (1995)
28. Formosa, P., Wilson, M., Richards, D.: A principlist framework for cybersecurity ethics. Comput. Secur. **109**, 102382 (2021)
29. Ghinita, G., Karras, P., Kalnis, P., Mamoulis, N.: A framework for efficient data anonymization under privacy and accuracy constraints. ACM Trans. Database Syst. (TODS) **34**(2), 1–47 (2009)

30. Goodman, B., Flaxman, S.: European Union regulations on algorithmic decision-making and a "right to explanation". AI Mag. **38**(3), 50–57 (2017)
31. Grace, K., Salvatier, J., Dafoe, A., Zhang, B., Evans, O.: When will AI exceed human performance? Evidence from AI experts. J. Artif. Intell. Res. **62**, 729–754 (2018)
32. Habermas, J.: The Theory of Communicative Action: Volume 1: Reason and the Rationalization of Society. Beacon Press (1985)
33. Hagendorff, T.: The ethics of AI ethics: an evaluation of guidelines. Minds Mach. **30**(1), 99–120 (2020). https://doi.org/10.1007/s11023-020-09517-8
34. Hall, P., Gill, N.: An Introduction to Machine Learning Interpretability. O'Reilly Media Incorporated, Sebastopol (2019)
35. Harborth, D., Braun, M., Grosz, A., Pape, S., Rannenberg, K.: Anreize und hemmnisse für die implementierung von privacy-enhancing technologies im unternehmenskontext. In: Sicherheit 2018: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 9. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Konstanz, 25–27 April 2018, pp. 29–41 (2018). https://doi.org/10.18420/sicherheit2018_02
36. Harborth, D., Cai, X., Pape, S.: Why do people pay for privacy-enhancing technologies? The case of Tor and JonDonym. In: Dhillon, G., Karlsson, F., Hedström, K., Zúquete, A. (eds.) SEC 2019. IAICT, vol. 562, pp. 253–267. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-22312-0_18
37. Harborth, D., Pape, S.: Examining technology use factors of privacy-enhancing technologies: the role of perceived anonymity and trust. In: 24th Americas Conference on Information Systems, AMCIS 2018, New Orleans, LA, USA, 16–18 August 2018. Association for Information Systems (2018). https://aisel.aisnet.org/amcis2018/Security/Presentations/15. Accessed 1 Feb 2022
38. Harborth, D., Pape, S.: JonDonym users' information privacy concerns. In: Janczewski, L.J., Kutyłowski, M. (eds.) SEC 2018. IAICT, vol. 529, pp. 170–184. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-99828-2_13
39. Harborth, D., Pape, S.: How privacy concerns and trust and risk beliefs influence users' intentions to use privacy-enhancing technologies - the case of Tor. In: 52nd Hawaii International Conference on System Sciences (HICSS) 2019, pp. 4851–4860, January 2019. https://scholarspace.manoa.hawaii.edu/handle/10125/59923. Accessed 1 Feb 2022
40. Harborth, D., Pape, S.: How privacy concerns, trust and risk beliefs and privacy literacy influence users' intentions to use privacy-enhancing technologies - the case of Tor. In: ACM SIGMIS Database: The DATABASE for Advances in Information Systems, vol. 51, no. 1, pp. 51–69 (2020). https://dl.acm.org/doi/abs/10.1145/3380799.3380805
41. Harborth, D., Pape, S., Rannenberg, K.: Explaining the technology use behavior of privacy-enhancing technologies: the case of Tor and JonDonym. In: Proceedings on Privacy Enhancing Technologies (PoPETs), vol. 2020, no. 2, pp. 111–128, May 2020. https://content.sciendo.com/view/journals/popets/2020/2/article-p111.xml. Accessed 1 Feb 2022
42. Government Federal Ministry of Justice: Federal Act Governing Access to Information held by the Federal Government (Freedom of Information Act) (2013). https://www.gesetze-im-internet.de/englisch_ifg/. Accessed 1 Feb 2022
43. Kitchener, K.S.: Intuition, critical evaluation and ethical principles: the foundation for ethical decisions in counseling psychology. Couns. Psychol. **12**(3), 43–55 (1984)

44. Kröger, J.L., Gellrich, L., Pape, S., Brause, S.R., Ullrich, S.: Personal information inference from voice recordings: user awareness and privacy concerns. In: Proceedings on Privacy Enhancing Technologies (PoPETs), vol. 2022, no. 1, pp. 6–27, January 2022. https://www.sciendo.com/article/10.2478/popets-2022-0002. Accessed 1 Feb 2022
45. Kusner, M.J., Loftus, J.R., Russell, C., Silva, R.: Counterfactual fairness. arXiv preprint arXiv:1703.06856 (2017)
46. Lazzaro, S.: Soap dispenser only responds to white skin. Dailymail.com (2017). https://www.dailymail.co.uk/sciencetech/article-4800234/Is-soap-dispenser-RACIST.html. Accessed 1 Feb 2022
47. Leavy, S.: Gender bias in artificial intelligence: the need for diversity and gender theory in machine learning. In: Proceedings of the 1st International Workshop on Gender Equality in Software Engineering, pp. 14–16 (2018)
48. Löbner, S., Tesfay, W.B., Nakamura, T., Pape, S.: Explainable machine learning for default privacy setting prediction. IEEE Access **9**, 63700–63717 (2021)
49. Löbner, S., Tronnier, F., Pape, S., Rannenberg, K.: Comparison of de-identification techniques for privacy preserving data analysis in vehicular data sharing. In: Brücher, B., Krauß, C., Fritz, M., Hof, H., Wasenmüller, O. (eds.) CSCS 2021: ACM Computer Science in Cars Symposium, Ingolstadt, Germany, 30 November 2021, pp. 7:1–7:11. ACM, November 2021. https://dl.acm.org/doi/10.1145/3488904.3493380
50. Loi, M., Christen, M.: Ethical frameworks for cybersecurity. In: Christen, M., Gordijn, B., Loi, M. (eds.) The Ethics of Cybersecurity. TILELT, vol. 21, pp. 73–95. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-29053-5_4
51. Macnish, K., van der Ham, J.: Ethics in cybersecurity research and practice. Technol. Soc. **63**, 101382 (2020)
52. Madgavkar, A.: A conversation on artificial intelligence and gender bias (2021). https://www.mckinsey.com/featured-insights/asia-pacific/a-conversation-on-artificial-intelligence-and-gender-bias. Accessed 1 Feb 2022
53. Malgieri, G.: The concept of fairness in the GDPR: a linguistic and contextual interpretation. In: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, pp. 154–166 (2020)
54. Malgieri, G., Custers, B.: Pricing privacy-the right to know the value of your personal data. Comput. Law Secur. Rev. **34**(2), 289–303 (2018)
55. Manjikian, M.: Cybersecurity Ethics: An Introduction. Routledge, London (2017)
56. Mason, R.: Policy for ethical digital services. J. Assoc. Inf. Syst. **22**(3), 11 (2021)
57. Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., Galstyan, A.: A survey on bias and fairness in machine learning. ACM Comput. Surv. (CSUR) **54**(6), 1–35 (2021)
58. Micheletti, G., Pepatou, C.: The European data market monitoring tool: key facts & figures, first policy conclusions, data landscape and quantified stories (2019). https://datalandscape.eu/sites/default/files/report/D2.6_EDM_Second_Interim_Report_28.06.2019.pdf. Accessed 1 Feb 2022
59. Morgan, G., Gordijn, B.: A care-based stakeholder approach to ethics of cybersecurity in business. In: Christen, M., Gordijn, B., Loi, M. (eds.) The Ethics of Cybersecurity. TILELT, vol. 21, pp. 119–138. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-29053-5_6
60. Motschenbacher, H.: Gentlemen before ladies? A corpus-based study of conjunct order in personal binomials. J. Engl. Linguist. **41**(3), 212–242 (2013)

61. Mozer, M.C.: Neural network music composition by prediction: exploring the benefits of psychoacoustic constraints and multi-scale processing. Connect. Sci. **6**(2–3), 247–280 (1994)
62. Muller, A., Asakura, K.: The Telenor case: the (in) compatibility of zero-rating with the net neutrality principle. Eur. Competition Reg. L. Rev. **5**, 59 (2021)
63. Nabbosa, V., Kaar, C.: Societal and ethical issues of digitalization. In: Proceedings of the 2020 International Conference on Big Data in Management, pp. 118–124 (2020)
64. United Nations: Universal declaration of human rights (1948). https://www.un.org/en/about-us/universal-declaration-of-human-rights. Accessed 1 Feb 2022
65. Neff, G., Nagy, P.: Automation, algorithms, and politics: talking to Bots: symbiotic agency and the case of Tay. Int. J. Commun. **10**, 17 (2016)
66. Niksefat, S., Kaghazgaran, P., Sadeghiyan, B.: Privacy issues in intrusion detection systems: a taxonomy, survey and future directions. Comput. Sci. Rev. **25**, 69–78 (2017)
67. Nissenbaum, H.: Where computer security meets national security. Ethics Inf. Technol. **7**(2), 61–73 (2005). https://doi.org/10.1007/s10676-005-4582-3
68. Nissenbaum, H.: Privacy in Context. Stanford University Press, Redwood City (2009)
69. Pape, Sebastian, Rannenberg, Kai: Applying privacy patterns to the Internet of Things' (IoT) architecture. Mob. Netw. Appl. **24**(3), 925–933 (2018). The Journal of Special Issues on Mobility of Systems, Users, Data and Computing. https://doi.org/10.1007/s11036-018-1148-2
70. Pape, S., Serna-Olvera, J., Tesfay, W.: Why open data may threaten your privacy. In: Workshop on Privacy and Inference, Co-Located with KI, September 2015
71. European Parliament: Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (2016)
72. van de Poel, I.: Core values and value conflicts in cybersecurity: beyond privacy versus security. In: The Ethics of Cybersecurity, p. 45 (2020)
73. Rannenberg, K., Pape, S., Tronnier, F., Löbner, S.: Study on the technical evaluation of de-identification procedures for personal data in the automotive sector. Technical report, Goethe University Frankfurt, May 2021. http://publikationen.ub.uni-frankfurt.de/frontdoor/index/index/docId/63413. Accessed 1 Feb 2022
74. Repetto, M., Carrega, A., Rapuzzi, R.: An architecture to manage security operations for digital service chains. Future Gener. Comput. Syst. **115**, 251–266 (2021). https://www.sciencedirect.com/science/article/pii/S0167739X20303290. Accessed 1 Feb 2022
75. Repetto, M., Striccoli, D., Piro, G., Carrega, A., Boggia, G., Bolla, R.: An autonomous cybersecurity framework for next-generation digital service chains. J. Netw. Syst. Manag. **29**(4) (2021). Article number: 37. https://doi.org/10.1007/s10922-021-09607-7
76. Royakkers, L., Timmer, J., Kool, L., van Est, R.: Societal and ethical issues of digitization. Ethics Inf. Technol. **20**(2), 127–142 (2018). https://doi.org/10.1007/s10676-018-9452-x
77. Schoentgen, A., Wilkinson, L.: Ethical issues in digital technologies (2021)
78. Schreiner, M., Hess, T.: Why are consumers willing to pay for privacy? An application of the privacy-freemium model to media companies. Published in Twenty-Third European Conference on Information Systems (ECIS), Münster, Germany (2015)

79. Selbst, A.D., Boyd, D., Friedler, S.A., Venkatasubramanian, S., Vertesi, J.: Fairness and abstraction in sociotechnical systems. In: Proceedings of the Conference on Fairness, Accountability, and Transparency, pp. 59–68 (2019)
80. Stevens, S.: A framework for ethical cyber-defence for companies. In: Christen, M., Gordijn, B., Loi, M. (eds.) The Ethics of Cybersecurity. TILELT, vol. 21, pp. 317–329. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-29053-5_16
81. Sweeney, L.: k-anonymity: a model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl. Based Syst. **10**(05), 557–570 (2002)
82. Timmers, P.: Ethics of AI and cybersecurity when sovereignty is at stake. Minds Mach. **29**(4), 635–645 (2019). https://doi.org/10.1007/s11023-019-09508-4
83. Tronnier, F.: D3.1 issues and gap analysis on data commercialisation in the context of ICT research and innovation (2020). https://www.panelfit.eu/wp-content/uploads/2020/11/D31-Issues-and-gaps-analysis-on-Data-Commercialisation-in-the-Context-of-ICT-Research-and-Innovation.pdf. Accessed 1 Feb 2022
84. Vacca, J.R.: Computer and Information Security Handbook. Newnes (2012)
85. Vallor, S., Green, B., Raicu, I.: Ethics in technology practice. The Markkula Center for Applied Ethics at Santa Clara University (2018)
86. Voudouris, C.: Defining and understanding service chain management. In: Voudouris, C., Lesaint, D., Owusu, G. (eds.) Service Chain Management, pp. 1–17. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-75504-3_1
87. Wachter, S., Mittelstadt, B.: A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. Colum. Bus. L. Rev. 494 (2019)
88. Wang, H., Gao, C., Li, Y., Wang, G., Jin, D., Sun, J.: De-anonymization of mobility trajectories: dissecting the gaps between theory and practice. In: The 25th Annual Network & Distributed System Security Symposium (NDSS 2018) (2018)
89. Weinberg, Z., Barradas, D., Christin, N.: Chinese wall or Swiss cheese? Keyword filtering in the great firewall of China. In: Proceedings of the Web Conference 2021, pp. 472–483 (2021)
90. Wirth, R., Hipp, J.: Crisp-DM: towards a standard process model for data mining. In: Proceedings of the 4th International Conference on the Practical Applications of Knowledge Discovery and Data Mining, vol. 1, pp. 29–39. Springer, London (2000)
91. Zafar, M.B., Valera, I., Rogriguez, M.G., Gummadi, K.P.: Fairness constraints: mechanisms for fair classification. In: Artificial Intelligence and Statistics, pp. 962–970. PMLR (2017)
92. Zuboff, S.: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Profile Books (2019)