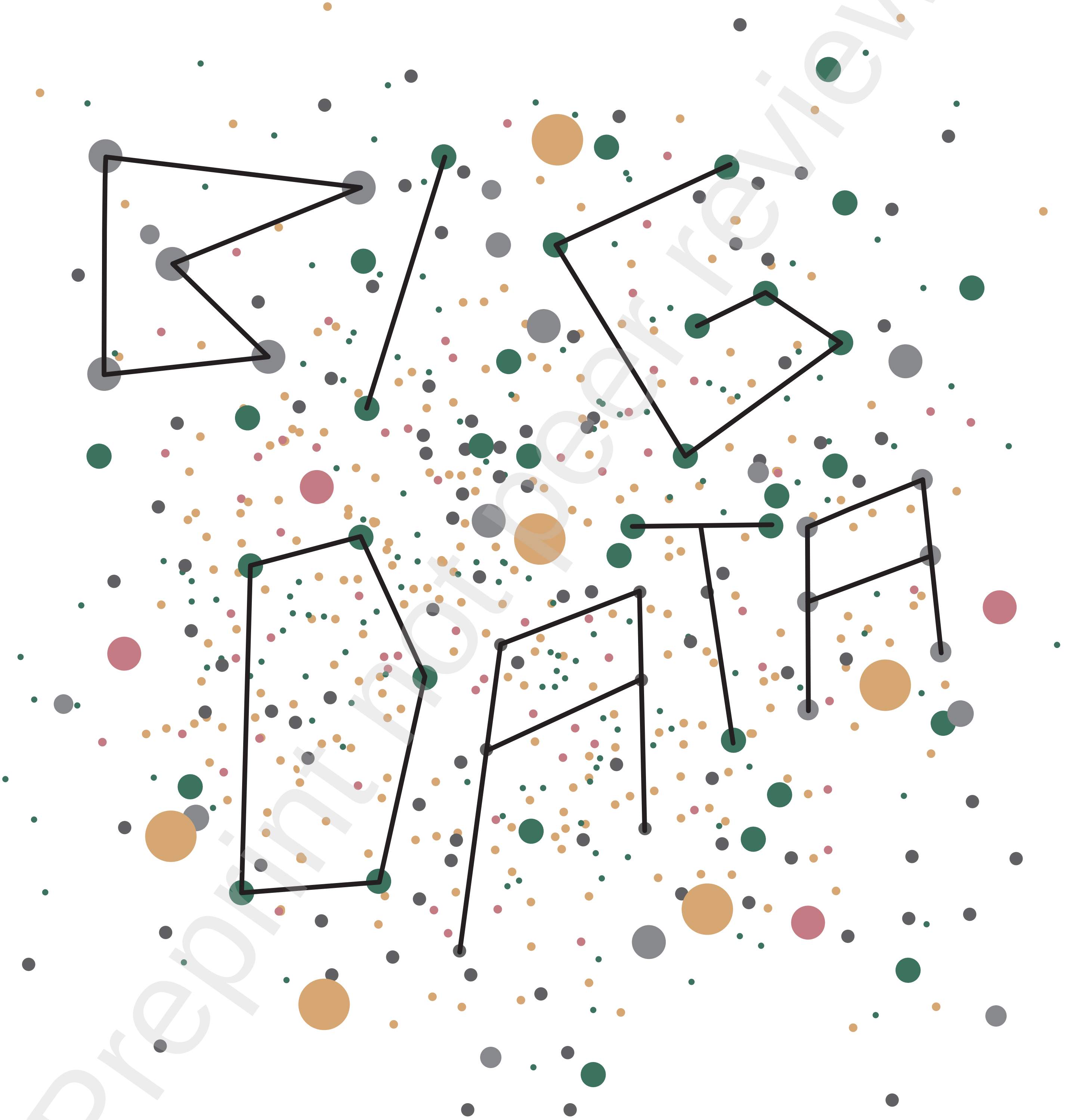
Eleonora Viganò (Editor)

Ethical, Legal and Social Issues of Big Data – a Comprehensive Overview

White Paper



University of Zurich^UZH

75 NRP Big Data
National Research Programme

Ethical, Legal and Social Issues of Big Data – a Comprehensive Overview

White Paper

Editor of the White Paper:
Eleonora Viganò (University of Zurich)

Authors of the main articles (in alphabetical order):
Markus Christen (University of Zurich),
Bernice Elger (University of Basel),
Marcello Ienca (EPFL),
Michele Loi (University of Zurich),
Christophe Schneble (University of Basel),
Eleonora Viganò (University of Zurich)

Authors of the commentary articles (in alphabetical order):
Mira Burri (University of Lucerne),
Christian Hauser (University of Applied Science of the Grisons),
David Shaw (University of Basel)

University of Zurich^UZH

75 NRP Big Data
National Research Programme

The National Research Programme “Big Data” (NRP 75)

Computing and communication devices accompany, influence, and guide our everyday life. They are embedded in large networks and produce increasing amounts of data. Novel solutions are needed to contend with and create value from these enormous volumes of data. This results in highly relevant research questions in the area of computing and information technology. Thus, NRP 75 supported innovative foundational research with the goal of processing and managing big data efficiently and effectively.

Furthermore, big data will have a profound effect on our society. The way we live, work and interact within society will be transformed. Appropriate regulatory measures are required, and citizens must understand the implications of big data. To this end, NRP 75 supported research projects in law and social sciences. Finally, NRP 75 promoted projects that bring together computing and domain experts to enable new, specific big data applications in business and society with a substantial potential for value creation. In this way, the NRP 75 aimed to lay the foundation for responsible research and innovation in a data-driven society.

Big Data ELSI Task Force

The societal acceptability of big data solutions crucially depends on the proper handling of the ethical, legal, and social issues (ELSI) those technologies raise. Consequently, several projects within NRP 75 explicitly deal with ELSI topics. In order to tackle such challenges, an ELSI Task Force including all projects of Module 2 “Societal and regulatory challenges” of NRP 75 has been formed. The members of this ELSI Task Force are (in alphabetical order, including former members): Christoph Baumberger, Mira Burri, Markus Christen, Ulrich Leicht-Deobald, Trude Hirsch, Marcello Ienca, Michele Loi, Sophie Mützel, Christophe Schneble, David Shaw, Eleonora Viganò and Kirsten Johanna Wesiak-Schmidt. The cross cutting activity of the ELSI Task Force for NRP 75 has set up an institutional structure and decision-making procedures for allocating ELSI expertise and resources within NRP 75 for the following aims:

(1) Providing ethical, legal, and social expertise for all NRP 75 projects;

(2) Supporting NRP 75 management board when preparing dissemination activities;

(3) Stimulating knowledge exchange among the ELSI experts within NRP 75 with the aim to enhance understanding of the core ELSI topics of big data.

Contact for requests:
eleonora.vigano@ibme.uzh.ch
christen@ethik.uzh.ch

Graphic concept & layout:
Rosa Guggenheim, guggenheim.li

National Research Programme
“Big Data” (NRP 75) of the Swiss
National Science Foundation (SNSF)

The authors of the ELSI White Paper are responsible for the statements and recommendations expressed in the ELSI White Paper. The content of the ELSI White Paper does not necessarily correspond to the opinions of the members of NRP 75 Steering Committee, the Swiss National Science Foundation, or the research teams.

Table of Contents

MAIN ARTICLES

COMMENTARY ARTICLES

Introduction

Eleonora Viganò

The ELSI White Paper is the final achievement of the ELSI Task Force for the National Research Programme "Big Data" (NRP 75). It is an informational document that provides an overview of the key ethical, legal, and social challenges of big data and provides guidance for the collection, use, and sharing of big data. The document aims to bring together the expertise of the ELSI Task Force members rather than exhaustively covering all topics in big data relating to ethical, legal, and social issues (ELSI).

The white paper comprises two parts: main articles and commentaries on it. The main articles give an overview of the major concerns associated with the use of big data, based on the assessment of the participating researchers. The commentary articles either examine in depth one or more of the issues that are presented in the main articles or highlight other issues that are considered relevant by their authors but are not covered in the main articles.

The main articles are divided into three sections corresponding to the three ELSI levels of analysis. In the section on ethics, Marcello Ienca explores the threat of big data to ethics commissions, privacy rights, personal autonomy, and equality in the healthcare sector and biomedical research. Bernice Elger focuses on the need to address informed consent differently and complement it with additional mechanisms in the big data context. In the legal section, Christophe Schneble explores whether current Swiss data protection laws adequately regulate and protect individuals' data. Eleonora Viganò analyses the threat of big data to state sovereignty and explore the two contrasting acceptations of the term "digital sovereignty" in the context of big data. In the section on social issues, Markus Christen addresses the big data divide, namely, the uneven distribution of benefits and harms from big data and the connected issue of the transparency asymmetry between data givers and data owners. Michele Loi delves into the debate on fair algorithms, presenting the risks of discriminating against certain groups when adopting big data-based predictive algorithms, such as those for predicting inmates' recidivism.

The second part of the ELSI White Paper contains three commentaries. In the first, Mira Burri focuses on the viability of new approaches to global trade governance that seek to address big data issues and makes recommendations for a better informed and more proactive Swiss approach. In the second commentary, David Shaw explores the lack of protection for vulnerable groups in big data research and the temporospatial and moral distance between researchers and participants that increases the risk of exploitation. In the third commentary, Christian Hauser tackles big data from the perspective of business ethics and provides guidance to companies employing big data.

Einführung

Eleonora Viganò

Das ELSI White Paper ist ein Ergebnis der ELSI Task Force des Nationalen Forschungsprogramms «Big Data» (NFP 75). Es handelt sich um eine Informationsbroschüre, die einen Überblick über die wichtigsten ethischen, rechtlichen und sozialen Herausforderungen (ELSI steht für «ethical, legal & social issues») von Big Data gibt und Empfehlungen für die Sammlung, Nutzung und Weitergabe von Big Data macht. Das Dokument vereint das Fachwissen der Mitglieder der ELSI Task Force, bietet aber keine erschöpfende Diskussion aller möglichen ethischen, rechtlichen und soziale Fragen von Big Data.

Das White Paper besteht aus zwei Teilen: den Hauptartikeln sowie Kommentaren dazu. Die Hauptartikel geben einen Überblick über die wichtigsten Bedenken im Zusammenhang mit der Nutzung von Big Data, basierend auf der Einschätzung der beteiligten Forschenden. In Kommentaren werden entweder ein oder mehrere der in den Hauptartikeln behandelten Themen vertieft oder andere Themen hervorgehoben, die von den Autorinnen und Autoren als relevant erachtet, aber im Hauptartikel nicht behandelt werden.

Die Hauptartikel sind in drei Abschnitte unterteilt, die den drei ELSI-Analyseebenen entsprechen. Im Ethik-Teil untersucht Marcello Ienca die Herausforderungen von Big Data für Ethikkommissionen, die Aspekte wie Datenschutzrechte, persönliche Autonomie und Gleichheit im Gesundheitssektor und in der biomedizinischen Forschung prüfen müssen. Bernice Elger befasst sich mit der Notwendigkeit, die informierte Zustimmung im Kontext von Big Data anders zu behandeln und sie durch zusätzliche Mechanismen zu ergänzen. Im rechtlichen Teil geht Christophe Schneble der Frage nach, ob die aktuellen Schweizer Datenschutzgesetze die Daten des Einzelnen angemessen schützen. Der Beitrag von Eleonora Viganò analysiert die mögliche Bedrohung der staatlichen Souveränität durch Big Data und untersucht dazu zwei gegensätzliche Auffassungen des Begriffs «digitale Souveränität» im Zusammenhang mit Big Data. Im Teil über soziale Fragen befasst sich Markus Christen mit der «Big Data Divide», d. h. der ungleichen Verteilung von Nutzen und Schaden durch Big Data und dem damit verbundenen Problem der Transparenzasymmetrie zwischen denjenigen, welche die Daten geben, und denjenigen, welche sie sammeln. Michele Loi befasst sich mit der Debatte über faire Algorithmen und zeigt die Risiken der Diskriminierung bestimmter Gruppen bei der Anwendung von Big-Data-basierten Vorhersagealgorithmen auf, z. B. bei der Vorhersage der Rückfälligkeit von Häftlingen.

Der zweite Teil des ELSI White Paper enthält drei Kommentare. Im ersten befasst sich Mira Burri mit der Realisierbarkeit neuer Ansätze für eine globale Handelsgovernance, die sich mit Big-Data-Fragen befassen, und sie macht Vorschläge für einen besser informierten und proaktiveren Schweizer Ansatz. Im zweiten Kommentar untersucht David Shaw den mangelnden Schutz für gefährdete Gruppen in der Big-Data-Forschung und die zeitlich-räumliche und moralische Distanz zwischen Forschenden und Teilnehmenden, was das Risiko einer ungerechtfertigten Nutzung der Daten erhöht. Im dritten Kommentar betrachtet Christian Hauser Big Data aus der Perspektive der Wirtschaftsethik und gibt Unternehmen, die Big Data einsetzen, einen Leitfaden an die Hand.

Die Beiträge liegen auf Englisch vor, eine Zusammenfassung sowie die Empfehlungen auf Deutsch und Französisch.

Introduction

Eleonora Viganò

Le livre blanc ELSI est le résultat final de la Task Force ELSI du Programme national de recherche « Big Data » (PNR 75). Il s'agit d'un document d'information qui donne un aperçu des principaux défis éthiques, juridiques et sociaux (ELSI signifie « ethical, legal & social issues ») posés par le big data, et formule des recommandations pour la collecte, l'utilisation et le partage des big data. Le document réunit l'expertise des membres de la Task Force ELSI, mais ne prétend pas faire un examen exhaustif de toutes les questions éthiques, juridiques et sociales potentiellement liées au big data.

Le livre blanc se compose de deux parties : des articles principales et des commentaires à propos de celui-ci. Les articles principaux donnent un aperçu des principales préoccupations liées à l'utilisation des big data, sur la base des évaluations menées par les chercheurs impliqués. Les commentaires permettent soit d'approfondir un ou plusieurs sujets traités dans les articles principaux, soit de mettre en avant d'autres aspects que les auteurs jugent pertinents, mais qui ne sont pas abordés dans les articles principaux.

Les articles principaux se subdivise en trois sections, qui correspondent aux trois niveaux d'analyse ELSI. Dans la partie consacrée à l'éthique, Marcello Ienca examine les défis posés par le big data aux comités d'éthique, qui doivent examiner des aspects tels que le droit à la confidentialité des données, l'autonomie personnelle et l'équité dans le secteur de la santé et de la recherche biomédicale. Bernice Elger se penche sur la nécessité de traiter différemment le consentement éclairé dans le contexte des big data et de le compléter par des mécanismes supplémentaires. Dans la partie juridique, Christophe Schneble s'intéresse à la question de savoir si les lois suisses actuelles sur la protection des données protègent les données personnelles de façon appropriée. L'article d'Eleonora Viganó analyse la menace potentielle que les big data font peser sur la souveraineté des États en examinant deux conceptions opposées de la notion de « souveraineté numérique » dans le contexte du big data. Dans la partie consacrée aux questions sociales, Markus Christen s'intéresse à la « big data divide », c'est-à-dire à la répartition inégale des avantages et des inconvénients liés aux big data et au problème de l'asymétrie de transparence qui en découle entre ceux qui fournissent les données et ceux qui en sont propriétaires. Michele Loi évoque le débat sur l'équité des algorithmes et met en évidence les risques de discrimination de certains groupes lors de la mise en œuvre d'algorithmes prédictifs basés sur les big data, par exemple pour prédire le risque de récidive des détenus.

La deuxième partie du livre blanc ELSI comporte trois commentaires. Dans le premier, Mira Burri se penche sur la possibilité de mettre en œuvre des approches inédites de gouvernance commerciale mondiale, tenant compte des questions de big data, et formule des propositions pour une approche suisse mieux informée et plus proactive. Dans le deuxième commentaire, David Shaw examine le manque de protection des groupes vulnérables dans la recherche sur les big data, ainsi que la distance spatio-temporelle et morale séparant les chercheurs et les participants, susceptible d'accroître le risque d'une utilisation injustifiée des données. Dans le troisième commentaire, Christian Hauser aborde les big data sous l'angle de l'éthique économique et propose un fil conducteur aux entreprises qui ont recours au big data.

Les contributions sont disponibles en anglais, un résumé ainsi que les recommandations en allemand et en français.

MAIN ARTICLES

Ethical issues of big data
Legal issues of big data
Social issues of big data

Ethical issues of big data

The ethics of big data use in the healthcare sector and biomedical research

Marcello Ienca

Marcello Ienca is a Principal Investigator at the College of Humanities at EPFL, where he leads the Intelligent Systems Ethics group, and an ordinary member of the Competence for Rehabilitation Engineering & Science at ETH Zurich. His scholarship focuses on the ethical, legal, social and policy implications of emerging technologies. Marcello Ienca is an appointed member of the Organisation for Economic Co-operation and Development's (OECD) Steering Committee on Neurotechnology, an expert advisor to the Council of Europe's Bioethics Committee and a Board Member of the Italian Neuroethics Society.

Big data is employed in an increasing number of human activities including, but not restricted to, banking, advertising, insurance, commerce, transportation, governance, national security, and science (Stephens et al. 2015). In recent years, big data has become pivotal to healthcare as well (Murdoch and Detsky 2013). Data sources related to human health have grown in volume and variety and became increasingly available for large-scale aggregation and high-speed analysis through computational methods. Data sources related to human health include both conventional health data and novel data sources. Conventional health data include electronic health records (EHRs), physiological measurements, population registries, medical images such as magnetic resonance imaging scans, mental health assessments, etc. Novel data sources include mobile health apps, digital phenotyping, social media, records of online behaviour, data from personal wearable devices, digital passports, etc. Such conventional and non-conventional datasets, used alone or aggregated, can be analysed computationally to reveal patterns, trends, and correlations that are relevant to human health. These include inferences related to disease prevention, diagnostics, therapy, assisted care, or other components of human medicine.

Leveraging big data for human health holds the promise of exerting a positive impact on the delivery of healthcare services. For example, big data is being widely used in epidemiology to predict and detect outbreaks, model epidemics, and develop public health interventions (Ehrenstein et al. 2017). Personal wearable devices and smartphones are being used as continuous sources of real-world data for purposes such as health monitoring (Smuck et al. 2021; Ienca et al. 2017).

Despite its potential for improving medicine and healthcare service delivery, the use of health-related big data raises ethical challenges. In light of its methodological novelty, reliance on large data repositories and computational complexity, big data may challenge existing oversight mechanisms such as independent review by an ethics review committee (ERC) [1]. There are two reasons for this. First, big data research involving publicly available and/or anonymised data may fall outside of the traditional purview of ERCs. Hence, a formal risk-benefit assessment may not be conducted by an oversight body before research begins. Second, even when big data studies do not bypass ethics review, ERCs may lack the expertise to scrutinise complex big data models computationally, especially those that rely on opaque machine learning algorithms (Ienca et al. 2018). Furthermore, big data trends in medicine raise privacy challenges (Price and Cohen 2019). This is because data can be collected from subjects under weaker consent regimes in a big data ecosystem than in a conventional medical research setting. For example, by accepting the rarely read terms of use of social media platforms, users may grant companies the right to process and reprocess their data. Consequently, they may share private information unintentionally or, at least, without a reasonable expectation of privacy. This risk is exacerbated when such data processing occurs in the absence of appropriate infrastructures for data storage and security. Studies have shown that de-identified and even anonymised data can be reverse engineered to re-identify individuals (Yoshiura 2019; Farzanehfar et al. 2021), leading experts to conclude that "there is no such thing as anonymous data" (Berinato 2015). This raises the question of whether big data projects should require oversight by an ERC even when the data collected are public and anonymised or de-identified (de Montjoye et al. 2015). The subjects' lack of awareness about data processing and data lifecycles may also compromise their autonomy. Big data models relying on biased training datasets may undermine fairness and lead to algorithmic discrimination (Hajian et al. 2016). Finally, big data's reliance on digital devices and data analytics software presents a challenge for equality and justice. It may exacerbate the divide between digitally savvy holders of technology and the rest of the human population (Taylor 2018).

In the light of these challenges, a debate has arisen in the scientific community about whether existing regulatory and ethical governance tools, as well as current ERC practices and expertise, are adequate to protect human participants and enable ethical research (Ferretti et al. 2022). Some authors argued that ethical principles and structures that traditionally govern research must be adapted considering the new context of big data research (Parasidis et al. 2019; Vayena and Blasimme 2018). Recent empirical studies revealed four main areas of ethical significance and a corresponding number of challenges of ERCs and analogous oversight

[1] In Switzerland, research involving human subjects, biomedical data, and biological samples requires the approval of the Research Ethics Committee. Most of the research projects conducted in biomedical and health fields are reviewed by Cantonal committees (Coordination Office for Human Research 2019).

bodies (Ferretti et al. 2022). First, the researchers revealed a lack of specific conceptual and normative standards for the ethics review of big data studies. Although ERC members may hold a general idea of what constitutes big data, they report to lack a precise common definition and clear guidance on how to assess those studies in practice. Second, ERCs report facing epistemic challenges and disclose a feeling of insufficient experience and expertise on this topic. This problem is exacerbated by the narrow mandate of the Human Research Act, which requires only a small portion of big data studies to be evaluated by an ERC (von Elm and Briel 2019). ERC members acknowledged that unless the law is amended to expand the purview mission of the ethical oversight mechanism, Cantonal ERCs have no choice but to encourage researchers to submit their study proposals on a voluntarily basis. Finally, normative ethical challenges have emerged in relation to the scope of ethical reflection on big data and the conceptual tools traditionally used to assess biomedical research, with several ERC members considering them inadequate to assess unforeseeable and novel risks generated by big data studies. To address these oversight-related challenges, proposals for reform have been made. These include both conservative reforms such as building capacity and promoting data literacy among ERC members and more radical reforms, such as complementing ERCs with big-data-specific oversight bodies.

Zusammenfassung:
Die Nutzung von Big Data durchdringt immer mehr menschliche Aktivitäten, auch im Gesundheitswesen. Dies geht einher mit dem Versprechen eines positiven Einflusses auf die Erbringung von Dienstleistungen. Da die Nutzung von Big Data aber von grossen Datenbeständen abhängig ist, sowie in methodischer und rechnerischer Hinsicht komplex ist, führt dies zu neuen Herausforderungen für Aufsichtsorgane (z.B. Ethikkommissionen). Dieser Beitrag untersucht, unter welchen Bedingungen Big-Data-Projekte im Gesundheitswesen einer Aufsicht unterliegen sollten, selbst wenn die erhobenen Daten öffentlich bzw. anonymisiert sind.

Empfehlungen:
Die Anforderungen an die Genehmigung von Big-Data-Studien durch Ethikkommissionen sollten besser geklärt werden. Dies mit dem Ziel der Schaffung einer Kultur der Verantwortlichkeit unter Forschenden, die an gesundheitsbezogenen Big-Data-Aktivitäten beteiligt sind. Dies bedingt eine Erhöhung des Kompetenzgrads von Ethikkommissionen, damit diese Big-Data-Studien besser beurteilen können (z. B. Erweiterung Ihrer Fachkenntnisse in Datenwissenschaft). Gegebenenfalls sollte die Einrichtung von ergänzenden Aufsichtsgremien wie Datenethikausschüssen erwogen werden.

Résumé :
La tendance du big data se propage à un nombre croissant de secteurs d'activité, y compris les soins de santé. L'exploitation du big data pour la santé humaine promet d'avoir un impact positif. Toutefois, compte tenu de sa nouveauté méthodologique, de sa dépendance à l'égard de vastes référentiels de données et de sa complexité informatique, le big data peut remettre en question les mécanismes de surveillance existants, par exemple par un comité consultatif d'éthique. Cela soulève la question de savoir si les projets de big data doivent nécessiter la surveillance d'un comité d'éthique, même lorsque les données collectées sont publiques et anonymisées ou dépersonnalisées.

Recommandations :
Les exigences relatives à l'approbation des études big data par les comités d'éthique devraient être mieux clarifiées. Ceci dans le but de créer une culture de responsabilité parmi les chercheurs impliqués dans des activités big data liées à la santé. Cela implique une augmentation du niveau de compétence des comités d'éthique, afin qu'ils puissent mieux évaluer les études big data (par exemple en améliorant leur expertise en science des données). Le cas échéant, il conviendrait d'envisager la création d'organes de surveillance complémentaires, tels que des comités d'éthique des données.

The challenges big data poses to informed consent and how to address them

Bernice Elger

Prof. Bernice Elger is the Head of the Institute for Biomedical Ethics (IBMB) at the University of Basel, a vibrant and interdisciplinary centre focused on research and teaching about ethical issues in medicine and the biosciences. She studied medicine and theology in Germany, the US, France, and Switzerland. She obtained her medical diploma as well as a university degree in protestant theology in Germany and her FMH (Swiss Medical Association) specialist title in internal medicine in Switzerland. For the past 20 years she has been teaching ethics and health law at the University of Geneva where she was nominated Associate Professor in 2007.

In this main article, I will deal with the ethical issues of informed consent and its legal framework. The requirement of informed consent is based on the fundamental ethical principle of respect for the autonomy of human beings. Already in the 19th century, studies that included human subjects without their knowledge or consent caused public outrage and led to legislation requiring informed consent from research participants (Maaßen 2015). For a long time, the use of data has been considered exempt from consent requirements under certain conditions. There are two primary reasons for this. First, contrary to clinical trials that include direct interventions on human beings, data are detached from human subjects. Therefore, there did not seem to be a strong need to protect subjects whose data was used from bodily harm. Second, the use of medical data from entire patient populations is important to detect adverse reactions to medications or other side effects of medical treatments. Thus, important side effects might be overlooked if some patients refused to consent to the use of their data, especially as patients with negative side effects tend to be angry at the healthcare system and refuse consent. Since identifiable data may cause harm, the easiest protection against harm seems to be anonymisation, which prevents data from being linked to the person who provided them. These considerations have influenced the Swiss Federal Act on Human Subject Research (HFG) as well as the Declaration of Helsinki (Swiss Confederation 2011; World Medical Association 2008). Both treat only the use of identifiable data as human subject research that falls under the protective regulations. In addition, both permit, under some conditions, weaker standards of consent, such as presumed consent with a right to opt out or general consent (general consent means that research participants do not receive any specific information about any future research projects to be carried out using their data, see HFG Art. 32, 33) or grant the option to a research ethics committee (REC) to waive consent requirements under certain conditions (Art. 34 HFG).

The era of big data has exacerbated the ethical and legal debate about appropriate consent for data use, in the medical arena and outside it. Concerns originate from the growing awareness that “all our data will be health data one day” (Schneble, Elger, and Shaw 2020a), and that true anonymisation is difficult or, in the case of genetic data, even impossible (Elger and Caplan 2006; Genevieve et al. 2018). The Swiss and international research ethics regulations reveal the theoretical and practical problems with informed consent in the era of big data. On the one hand, respect for autonomy requires the provision of a maximum of information and choice to those whose data are being used and their protection against harm. On the other hand, there are interests that override the right to informed consent; for example, data may be accessed without consent to prevent epidemics or crimes (Schneble, Elger, and Shaw 2020b). Furthermore, the complexities of big data make fully informed consent procedures impractical or at least so time-consuming that Internet users or research participants will tick boxes or provide agreement based on trust rather than true understanding. A common example is the often uninformed “consent” given by users to the terms and conditions of apps and social media companies (Schneble et al. 2021). Users rarely take the time to try to read and understand what they are “ticking themselves into” when they join Internet platforms or use services. While some experts recommend additional regulation for big data (Terry 2014), others are against what they call *big data exceptionalism*, that is, they are convinced that existing regulations concerning data processing and use apply equally to big data (Rothstein 2015).

One of the six lawful bases for processing personal data that are listed in Article 6 of the General Data Protection Regulation (GDPR) of the European Union is to obtain valid user consent. In the case of children or incapacitated adults, this would be parental consent or the consent of legal proxies. But how can this be put into practice? How can the challenges of big data to informed consent be adequately addressed in real life? The EU working party that provided guidance before GDPR entered into force wrote that “Swiping a bar on a screen, waving in front of a smart camera, turning a smartphone around clockwise, or in a figure-eight motion may be options to indicate agreement, as long as clear information is provided, and it is clear that the motion in question signifies agreement to a specific request (e.g., if you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm). The controller must be able to demonstrate that consent was obtained this way, and data subjects must be able to withdraw consent as easily as it was given” (Article 29, Working Party 2018). While this may help to address the ambiguity of ticking boxes on the Internet, it does not solve the very essence of consent to big data use: the fact that the human brain is unable to cope with the huge amount of information and possible consequences of big data use. Thus, it might be necessary, more transparent, and more honest to abandon, at least in part, the concept of informed consent to big data processing and use and complement it with mechanisms that ensure protection from harm or guarantee appropriate compensation in the case of harm.

In the field of research ethics, the approval of the research project by a research ethics committee (REC) is such a mechanism. As the competence of REC members concerning big data might be limited, it could be prudent to enlist experts on big data to consider more specialised protection mechanisms not only for research but also for much broader use. These experts and procedures should ensure that data protection is sufficient (by anonymisation, for example); that people receive short, understandable information about the most significant ways their data will be used; and that data abuse will be either unlikely or detected early enough to prevent significant harm, independently of the choices people make about the use of their data.

Zusammenfassung:
In der heutigen digitalisierten Welt ist es schwierig, das Erfordernis einer echten informierten Zustimmung zur Datennutzung zu erfüllen. Dieser Beitrag plädiert dafür, dass es transparenter und ehrlicher ist, das Konzept der Einwilligung angesichts der heutigen Möglichkeiten der Nutzung von Big Data zumindest teilweise aufzugeben. Stattdessen sollte das Prinzip der informierten Zustimmung durch Mechanismen ergänzt werden, die einen Schutz vor Schaden gewährleisten oder eine angemessene Entschädigung im Falle eines Schadens garantieren.

Empfehlungen:
Fachpersonen und Verfahren sollen sicherstellen, dass der Datenschutz durch Anonymisierung ausreichend ist; dass die Menschen kurze, verständliche Informationen über die wichtigsten Verwendungsmöglichkeiten ihrer Daten erhalten; und dass Datenmissbrauch entweder unwahrscheinlich ist oder früh genug erkannt wird, um erheblichen Schaden zu verhindern, unabhängig davon, welche Entscheidungen die Menschen über die Verwendung ihrer Daten treffen.

Résumé :
Dans le monde numérisé d’aujourd’hui, il est difficile de satisfaire à l’exigence d’un véritable consentement éclairé pour l’utilisation des données. Il pourrait s’avérer nécessaire, plus transparent et plus honnête d’abandonner, au moins en partie, le concept de consentement éclairé au traitement et à l’utilisation du big data, et de l’assortir de mécanismes assurant une protection contre les préjudices ou garantissant une indemnisation appropriée en cas de préjudice.

Recommandations :
Les experts et les procédures doivent garantir que la protection des données par l’anonymisation est suffisante, que les personnes reçoivent des informations brèves et compréhensibles sur les principales façons dont leurs données seront utilisées, et que l’abus de données est soit improbable, soit détecté suffisamment tôt pour éviter un préjudice important, indépendamment des choix que les personnes font concernant l’utilisation de leurs données.

Legal issues of big data

Data protection laws and their implications for big data – Are they up to date?

Christophe Schneble

Christophe Schneble holds a PhD in Bioethics and is part of the ELSI Task Force for NRP 75. His interests are in interdisciplinary research especially at the boundary of ethics, law, and computer science. Prior to his PhD, Christophe was Manager of a Department at ETH Zurich, former member of ETH's Strategy Commission, and held several roles as Software Developer. Currently he is managing the focus area of Personalised Health at the European Campus lead by the University of Basel.

Ensuring the protection of data subjects[1] has become central to both the research and commercial use of big data. Many laws have upheld the principles of data minimisation[2] when personal data are being processed. Although the definition of big data and the ways big data can be used differ from field to field and context to context (De Mauro et al. 2016; Favaretto et al. 2020), the essence of any kind of big data methodology is the linking and use of a large amount of data. Whenever the processing of information concerns personal data, privacy rights could be at risk. Currently, laws impose safeguards to mitigate risks such as requesting either risk—for example, mandating the subject's consent for data use—or requiring lawful grounds for processing personal data. Data that is anonymised or non-personal is exempted from such safeguards and can be processed without further limitations.[3] Exempting anonymised data is problematic, as anonymised data might be easily re-identified by linking sources or employing advanced computational methods. Thus, there is a clear need for other approaches to address this issue (Samarati and Sweeney 1998; Kairouz and Viswanath 2017; Torra and Navarro-Arribas 2016). Differentiating between personal and non-personal data is also problematic. The power of

[1] The term "data subjects" refers to individuals whose data is processed. The term "data processor" refers to the entity doing the processing.

[2] The General Data Protection Regulation (GDPR) has influenced many other laws. In Article 5, it lays out the principles relating to processing personal data, including that such data should be adequate, relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation"). Although the Federal Act on Data Protection (FADP) does not define the principle of data minimisation, it states in Article 4, Numeral 3, that data may only be processed for the purpose indicated at the time of collection, evident from the circumstances, or provided for by law.

[3] Martani et al. (2020) provide a decision tree for this issue. Anonymisation eliminates the reference to a data subject/person so that the subject or person can no longer be identified.

big data lies in the linkage of different data sources for prediction or analysis. Linking non-personal data that is not subject to data protection with personal information might reveal problematic patterns (Schneble, Elger, and Shaw 2020a) and lead to discrimination and disrespect for individual privacy.

Swiss legislation makes a distinction between the processing of data by private entities (private individuals and companies) and their public counterparts (entities such as governments and cantons). Whilst private entities need either some interest or direct consent from individuals to process data, the processing of data by the government needs a legal base in addition. Private entities are subject to the federal law as well as federal institutions[4], while their cantonal counterparts are subject to cantonal legislation, which rests on the same principles as the federal laws but differs on minor issues. Besides this umbrella law, to which institutions and private entities refer, there are sectorial regulations, like the Law on Health Insurance in the insurance sector, the Epidemic Law in the case of pandemics, the Law on Electronic Health Records for clinical data, and the Human Research Act for biomedical research.[5] This diversity as well as the cantonal differences have made it hard for individuals and researchers to determine which laws they must adhere to (Martani et al. 2020).

Especially in the public discourse, the concept of data ownership is often mooted as a possible solution because it is commonly associated with increased control over (personal) data. However, many legal scholars have opposed the concept—mainly because ownership in property law entails exclusive rights and rights of dominion and defense (Picht 2017; Weber and Thouvenin 2018; Widmer et al. 2021). As data are not of a physical nature, those rights do not fulfill the characteristics. It has also been argued that market failure has typically been the spur for increased regulation, but, as Thouvenin and others point out, this would only apply if data would not be created or used to the extent desired by society (Widmer et al. 2021).

However, some safeguards in respect to the use of data are in force in many domains. For example, the use of health-related data in biomedical research is governed by the Human-Research Act (HRA), which places additional safeguards on the use of data in this domain (D'Amico and Rütsche 2015). Because data are immaterial goods, they are covered to some extent by the Federal Act on Copyright and Related

[4] In the academic environment this might lead to a paradoxical situation. For example, a federal institution on one side of the street is governed by federal law, whereas its cantonal counterpart on the other side of the street is subject to jurisdiction of the canton.

[5] For a comprehensive overview of laws relating to data handling in biomedical research, see Martani et al. (2020).

Rights. However, it is often hard to delineate when data are intellectual creations to which the extended safeguards would apply.[6]

Nevertheless, there is a need for action, especially with regard to the monetisation of data. At a time when data are becoming increasingly important assets and can be used to generate capital in many areas, data subjects should be allowed to benefit from the use of their data (Amstutz 2018). This sentiment was also voiced by data-protection officers during research conducted within NRP 75 (Widmer et al. 2021).

As demonstrated in the previous paragraphs, the legal landscape is characterised by heterogeneity, and different types of data (for example, health data) are subject to different safeguards. However, the scope of the Federal Act on Data Protection (FADP) is more comprehensive than it might seem at first glance as it is philosophically based on personal rights. This implies that the principles are vaguely defined and lack precise instructions for action (Epiney 2015). This is where ethics and ethical guidelines come into play; an analysis of recent scandals (Schneble et al. 2020c, 2018) showed that there is a conflict of objectives between what is feasible (in terms of technology) and ethical behaviour. This risk, however, could be mitigated by mandating ethical review boards in the commercial field. This concept has been successfully adopted in biomedical research for several decades.

Another angle for improvement lies in the area of consent. As mentioned before, getting approval to process data has largely involved presenting data subjects with terms and conditions. However, the latter has proven rather ineffective (Cate and Mayer-Schonberger 2013). Terms and conditions are long and written in complex language, so this approach can be problematic when targeting groups of vulnerable persons—especially children (Schneble et al. 2021) There have been various attempts to improve this situation. For instance, the process of getting consent could be made simpler by providing simplified terms and conditions or presenting them graphically (Brunschwig 2001). Another approach is to provide users oversight of which data they share in a portal-based solution, as proposed by opponents of the dynamic consent solution (Steinsbekk et al. 2013; Kaye et al. 2015), or delegating those rights to a third party that acts as a steward (Hafen 2015).

[6] For a more detailed view on this, see Weber et al. (2018) and Widmer et al. (2021).

Zusammenfassung:
Der Schutz von Datensubjekten ist sowohl für die Forschung als auch für die kommerzielle Nutzung von Big Data von zentraler Bedeutung. Die aktuellen Datenschutzbestimmungen spielen eine wichtige Rolle bei der Gewährleistung von Schutzmassnahmen, der Risikominderung und der Festlegung von Rechten für die Betroffenen. Die heutige Rechtslandschaft ist jedoch oft durch Heterogenität gekennzeichnet, was den Überblick erschwert. Darüber hinaus ist es wichtig, eine Brücke zwischen dem rechtlichen Kontext und der Umsetzung zu schlagen, indem Leitlinien für die Umsetzung dieser Grundsätze bereitgestellt werden.

Empfehlungen:
Da Datenschutzgesetze der Dynamik der Entwicklung im Bereich Big Data nicht folgen können, ist die Bereitstellung von Leitlinien ein komplementärer Weg. Ein vielversprechender Bereich, in dem Leitlinien wirken könnten, ist die dynamischen Einwilligung in die Datennutzung. Dadurch kann die Autonomie der einzelnen Person wie auch der Schutz ihrer Rechte gewahrt werden.

Résumé :
La protection des personnes concernées est devenue centrale, tant pour la recherche que pour l’utilisation commerciale du big data. Les réglementations actuelles en matière de protection des données jouent un rôle important en fournissant des garanties, en atténuant les risques et en imposant le respect des droits des personnes concernées. Cependant, le paysage juridique actuel se caractérise souvent par une grande hétérogénéité, ce qui permet difficilement d’en avoir une vision d’ensemble. En outre, il est essentiel de faire le lien entre le contexte juridique et les mises en œuvre en fournissant des lignes directrices et de mettre en application les principes.

Recommandations :
Étant donné que les lois sur la protection des données ne peuvent pas suivre l’évolution très dynamique du big data, le recours à des lignes directrices s’avère complémentaire. Le contexte de l’obtention du consentement est un domaine où l’utilisation de mécanismes modernes tels que le consentement dynamique pourrait par exemple être bénéfique pour les individus, leur engagement et la protection de leurs droits en préservant leur autonomie.

Big data and digital sovereignty
Eleonora Viganò

Eleonora Viganó is Postdoctoral Researcher at the Institute of Biomedical Ethics and History of Medicine and the Executive Manager of the ELSI Task Force for NRP 75. Currently she is working on philosophical theories of discrimination in the project “Socially acceptable AI and fairness tradeøffs in predictive analytics” funded by the National Research Programme “Digital Transformation” (NRP 77). Her research areas are self-regarding-morality, the implications on moral philosophy of neuroscientific discoveries on decision-making, and the ethical issues of digital technologies aiming to improve people’s well-being.

Big data flows from one country to another and spreads in a constellation of digital networks without state barriers: it is gathered in one country and can be used in others. Because of this dispersion, as well as the global interdependence of states, big data challenges the concept of *state sovereignty*, which always involves a circumscribed physical territory.

Sovereignty is a concept that we inherited from early modern Europe. Its primary meaning is the *supreme authority within a territory* that is attributed to a state. The authority of a holder of sovereignty is not held through coercion. Instead, it is legitimate because derived from an acknowledged source of legitimisation such as natural or divine law, a constitution, or international law (Philpott 2020). The authority of a holder of sovereignty is supreme in that it is greater than that of other powers in the territory and independent vis-à-vis other states (Philpott 2020; Pohle and Thiel 2020). Territoriality is thus a fundamental element of sovereignty, which is authoritative only within a precisely defined geographical space (Philpott 2020). This characteristic of sovereignty explains why big data is a hindrance to the sovereignty of states. It belongs to a space—*cyberspace*—that is not physical and thus cannot be limited to a territory, even though its collection, storage, sharing, and transmission is based on physical components such as hardware. The intangibility of big data challenges traditional international law on jurisdiction, which is founded on state sovereignty and presupposes that people and things are located in a knowable and finite location (Eichensehr 2016, pp. 145–146).

Although big data challenges the traditional concept of sovereignty, it has been progressively associated with a notion of sovereignty applied to the digital realm: *digital sovereignty*. Here, with “digital,” I broadly mean technologies, infrastructures, data, and content based on electronic computing techniques (Peters 2016). As shown by Couture and Toupin, digital sovereignty has been conceptualised in different ways by different types of actors (Couture and Toupin 2019, p. 2306). In contemporary political discourse, digital sovereignty incorporates two main concepts, each involving big data. The first concept is based on the idea that a state is autonomous and thus should make independent decisions about technology innovation and digital infrastructure, guarantee the security of such infrastructure, and be independent of foreign technology and infrastructure (Pohle and Thiel 2020, pp. 8, 10). This idea of digital sovereignty supports regulation of the Internet at the national level, as well as data localisation (limiting data storage, movement, and processing to specific areas) (Chander and Le 2014; Hill 2014). For instance, in Europe, Schengen Routing (i.e., routing Internet traffic among hosts that are in the Schengen area) was put forth as a countermeasure against monitoring activities of some intelligence agencies. In this way, Internet traffic does not leave the borders of the Schengen Agreement signatories and cannot be wiretapped as easily by intelligence agencies outside the Schengen area (Dönni et al. 2015). The other side of the coin of the concept of digital sovereignty as the possession of independent and secure national infrastructures is that a state or system of states can intrude into the private life of citizens by accessing their personal data through intelligence actors and law-enforcement agencies and justifying the intrusion as a matter of security (Cavelty and Egloff 2019; Möllers 2021). For instance, the Schengen Internet traffic is still vulnerable to wiretapping by intelligence agencies located in the Schengen area.

The second and more recent concept of digital sovereignty focuses on users' autonomy and self-determination in the digital realm. Self-determination in the digital realm is defined as the ability to make decisions about the use of one's personal data, digital platforms, and devices in an autonomous, competent, and informed way (Pohle and Thiel 2020, p. 11). Several measures have been proposed to enhance users' sovereignty over their data; for instance, programmes that provide users with the skills to act in the digital space (i.e., digital literacy) and encourage them to reflect critically on digital technologies. Other proposals for enhancing users' digital sovereignty include demanding that tech companies encrypt users' data and become more transparent about their use of users' data.

It is noteworthy that the two concepts of digital sovereignty potentially conflict with each other; this tension is evident in the case of big data. On the one hand, each state aims to exercise sovereignty over the digital realm that is inscribable in its territory and thus aims to protect its citizens' big data from, for instance, foreign surveillance. On the other hand, citizens' digital sovereignty over their own big data, as well as the privacy and security of such data, is threatened by the possibility that the state can access it.

In conclusion, big data has been associated with a specific meaning of sovereignty, which is digital sovereignty. Big data is a good over which both states and individuals aim to exercise their sovereignty in the digital realm. Both individuals and states aim to act autonomously in the management of such data, and this can generate conflicts between the state and individuals. As big data is intangible and spreads in networks that cross state borders, it cannot be easily regulated in ways that are based on the sovereignty of the state over a finite and knowable physical space. Big data's intangible nature transcends state regulations. Therefore, the collection, storage, sharing, and transmission of big data should be addressed through coordination and cooperation among states (Eichensehr 2014, p. 320).

Zusammenfassung:
Einerseits stellen Big Data das Konzept der staatlichen Souveränität in Frage, da diese Daten immateriell sind und sich über Staatsgrenzen hinweg ausbreiten. Andererseits wird Big Data mit einem neuen Begriff von Souveränität in Verbindung gebracht: der digitalen Souveränität. In diesem Abschnitt werde ich zunächst die beiden Bedeutungen von digitaler Souveränität im Zusammenhang mit Big Data vorstellen, nämlich die Autonomie eines Staates bei der Regulierung und dem Schutz der Daten seiner Bürgerinnen und Bürger und die Selbstbestimmung der Nutzerinnen und Nutzer bei der Verwendung ihrer persönlichen Daten. Dann werde ich zeigen, dass die beiden Bedeutungen im Fall von Big Data miteinander in Konflikt stehen, weil letzteres ein Gut ist, auf das sowohl Individuen als auch Staaten ihre Autonomie ausüben wollen.

Empfehlungen:
Da Big Data immateriell sind, können sie nicht auf eine Weise reguliert werden, die auf der Souveränität des Staates über einen endlichen physischen Raum beruht. Folglich sollten sich die Staaten untereinander abstimmen und zusammenarbeiten, um die Erhebung, Speicherung, Weitergabe und Übertragung von Big Data zu regeln. Dabei muss das Ziel des Staates, die Sicherheit seiner digitalen Infrastruktur zu schützen, gegen die Autonomie seiner Bürgerinnen und Bürger abgewogen werden, um ungerechtfertigte Eingriffe des Staates in das Privatleben zu vermeiden.

Résumé :
D’une part, le big data remet en question le concept de souveraineté des États, car il est intangible et s’étend au-delà des frontières des États. D’autre part, le big data est associé à une nouvelle notion de souveraineté: la souveraineté numérique. Dans cette section, je présenterai d’abord les deux significations de la souveraineté numérique dans le contexte du big data, à savoir l’autonomie d’un État en matière de régulation et de protection des données de ses citoyens, et l’auto-détermination des utilisateurs dans l’usage de leurs données personnelles. Ensuite, je montrerai que ces deux significations entrent en conflit dans le cas du big data car ce dernier est un bien sur lequel les individus ainsi que les États visent à exercer leur autonomie.

Recommandations :
Car le big data étant immatériel, il ne peut être réglementé selon des modalités fondées sur la souveraineté de l’État sur un espace physique fini. Par conséquent, les États doivent se coordonner et coopérer entre eux pour réglementer la collecte, le stockage, le partage et la transmission du big data. Dans ce contexte, l’objectif de l’État de protéger la sécurité de son infrastructure numérique doit être mis en balance avec l’autonomie de ses citoyens, afin d’éviter toute intrusion injustifiée de l’État dans la vie privée de ses citoyens.

Social issues of big data

The big data divide between companies and customers

Markus Christen

Markus Christen is Managing Director of the Digital Society Initiative (DSI) of the University of Zurich (UZH) and heads the digital ethics lab at the Institute of Biomedical Ethics and History of Medicine at UZH. His research areas are ethics of information and communication systems, neuroethics and empirical ethics. Current research topics include the use of video games (Serious Moral Games) to measure and promote moral competence, ethical questions of big data, cybersecurity and artificial intelligence, as well as research into human-machine interaction in moral issues, such as the use of drones.

One of the fundamental ethical issues associated with big data is the "big data divide"—a term used to describe the asymmetric relationship between "those who collect, store, and mine large quantities of data, and those who are the target of data collection" (Andrejevic 2014). In this section, I sketch the ethical nature of this problem by highlighting the values that make the big data divide, and transparency asymmetry in particular, problematic. We argue that, although those values provide orientation in an ethically justified direction, overcoming the big data divide is the *wrong goal* due to the structure of this problem. Instead, the focus should be on safeguarding those potentially disadvantaged by this divide from its negative consequences.

Structurally, the big data divide (with a focus on transparency asymmetry) involves (at least) two actors: data givers and data owners. They must be distinct to some degree such that the notions of "divide" and "asymmetry" make sense. Data givers disclose information of various types and are aware to varying degrees that they are doing so. Data owners collect this data and make use of it in various ways. In the early years of data protection (the 1970s or earlier), this asymmetry was described as mainly present between states and their citizens (Hornung and Schnabel 2009). Currently, the asymmetry is usually conceived of as existing between a very specific group of companies (those controlling large platforms such as search engines and social networks) and the customers of those companies (Coley 2017). Obviously, the situation can be much more complex. For example, states may demand by law access to big data collected by tech companies (e.g., Apple is required to store data from Chinese customers in China, and the Chinese state may access this data). However, let us for the sake of the argument restrict this discussion of the big data divide between tech companies and their customers to the Western context. In that respect, it is important to note that the big data divide concerns not only access to data but also the capacity to make sense of it—by machine learning, for example—a point that will become relevant below.

Furthermore, the digital divide is closely linked to a transparency problem—namely, the claim that the data givers (the customers) lack transparency in terms of knowledge about the existence and consequences of this divide. Thus, the notion of transparency has both a content (what data are collected?) and a process (what could be done with this data?) dimension. In that respect, transparency is a tricky concept. First, it is observer dependent (the cognitive capabilities of the person determine whether transparency has been achieved). Second, it is embedded in a temporal structure: having achieved transparency as to the content and process of data at time t_1 does not mean that transparency is still present at time t_2 because, for example, new methods to analyse data may have been developed at t_2 that allow for insights that could not have been foreseen at t_1.

From an ethical point of view, this data divide problem can be described as a combination of violating the value of equality (with respect to access to information about the content and process dimensions of big data) and violating the autonomy of those who are the objects of data collection. Arguments for equality in access to and use of big data are often consequentialist (e.g., the claim that equal access to big data may increase welfare because markets can become more efficient (Zuiderwijk et al. 2012). This consequentialist framing of equality denies that "big data equality" is an ethical goal per se (a point that will become clearer below). The reference to autonomy is usually justified by deontological reasoning—for example, by making the argument that having control over personal data is an expression of privacy, which is a fundamental human right (Rouvroy and Poullet 2009). Again, this sketch simplifies the situation; real-world situations may have additional ethical aspects that should be considered. However, let us for the sake of the argument consider only two values, namely, (1) equality as a means to increase welfare and (2) autonomy. The value of transparency has here mainly a functional role. First, it is necessary to check to what extent equality has been achieved. Second, it is a condition for acting autonomously. Unless the data giver is aware of the content and process dimensions of the data to be disclosed, disclosing them cannot be considered an autonomous act of the data giver. In the following paragraphs, we discuss the question of whether these two guiding values provide sufficient support for a goal to *eliminate* the big data divide. The answer is negative.

The goal to eliminate the big data divide can have two different meanings. First, it could refer to an *actual* elimination: all data givers are also data owners—that is, everybody has access to his or her data (knows what data are there and can understand them) and can process this data in a meaningful way. This goal is conceptually unclear, factually not achievable, and ethically wrong. It is conceptually unclear because the ontological status of many of the involved data is unclear. For example, linking data in a social network (who knows who) do not belong to a single individual, and their meaning is context dependent. The fact that person C knows that person A knows person B has a different meaning than the fact that person D knows that person A knows person B because the interaction histories of C (with A and B) and D (with the same persons) are different. Therefore, the notion of "my data" is unclear for many data types that are particularly relevant in the digital age. Furthermore, C has no access into the mind of D; this means that there will always be a data divide. Given that C and D are also likely to differ in their interests in and capabilities of achieving transparency, transparency asymmetries in particular will remain in any case. Removing those asymmetries would require forcing C and D to have equal interests and gain equal data processing capabilities: an obvious violation of autonomy and thus unethical. This argument also remains valid when C and D are legal persons (i.e., companies). Thus, factual elimination of the big data divide is the wrong goal.

A second interpretation of the goal is to *potentially* eliminate the big data divide. Namely, measures are put in place such that those who *want* equal access to big data and have (or are willing to obtain) the capabilities to reach content and process transparency can achieve this goal.[1] This is often what people have in mind when they argue against the big data divide. In addition, the legislator (e.g., the GDPR) works hard to ensure that people are empowered to gain informational self-determination as a means to diminish the big data divide.

At first sight, this interpretation of the goal is in line with the guiding values. First, autonomy is preserved, as no one is forced to become an "expert in their own data" and measures are supported that consider human competence variability (at least to a certain degree). Second, the reference to equality is restricted to its welfare aspect. For example, the open data movement assumes that freely usable data leads to more transparency and collaboration. This, however, puts a burden on the argument: measures to decrease the digital divide (such as the right to data portability) and reduce transparency asymmetry (such as regulations mandating the provision of details on data processing) must be shown to have these positive effects.

This is the place where the structural aspects of the big data divide come into place. The content and process dimensions of big data are not fixed entities but rather result from scientific enquiry: finding out what big data can reveal (content), and which methods are needed to capture that information, is an expensive endeavour. Those who already have a skilled workforce or other resources (financial, cognitive, etc.) will disproportionally benefit from any measures that decrease the big data

[1] In the following, we will abstain from discussing the conceptual problems with the notion of "my data" mentioned above.

divide. Big tech companies will be better able to crush start-ups, and individuals with greater cognitive abilities will have more opportunities to outperform those with lesser cognitive abilities.

This certainly does not mean that measures guided by the values of equality/welfare and autonomy are problematic per se. But the effect of those measures has to be considered, taking into account the social fact that the resources to handle big data and generate knowledge from it are not equally distributed—and there are good reasons not to enforce equalisation in that respect (clarifying this point, however, goes beyond the scope of this contribution).

Consequently, the ethical debate on the big data divide, including transparency asymmetry, should not focus on measures to decrease the divide and asymmetry. Instead, it should identify realistic harms that could result from the big data divide and transparency asymmetry and develop (legal) safeguards for those who are disadvantaged by the divide. This shift in focus will need an additional guiding value—nonmaleficence or harm reduction. Current data protection legislation that relies primarily on autonomy (and privacy) is poorly structured in that respect. It is insufficient to handle the negative consequences of the big data divide, which is to a certain extent inevitable in a society that values freedom and diversity.

Zusammenfassung:
Der Ausdruck «Big Data Divide» beschreibt die asymmetrische Beziehung zwischen denjenigen, die grosse Datenmengen sammeln, speichern und auswerten (in der Regel Unternehmen), und denjenigen, die das Ziel der Datenerhebung sind (z. B. Kundinnen und Kunden). In diesem Beitrag wird behauptet, dass die Überwindung der «Big Data Divide» nicht im Mittelpunkt des ethischen Interesses stehen sollte. Vielmehr sollte das Ziel darin bestehen, diejenigen zu schützen, die durch diese Kluft potenziell benachteiligt werden.

Empfehlungen:
Die «Big Data Divide» ist eine unvermeidliche Folge einer Gesellschaft, die Freiheit und Vielfalt schätzt; die Beseitigung dieser Kluft ist ein falsches politisches Ziel. Stattdessen sollte der Gesetzgeber realistische Schaden-Szenarien identifizieren, die aus der «Big Data Divide» resultieren könnten, und rechtliche Schutzmassnahmen für diejenigen entwickeln, die durch die Kluft benachteiligt werden. Dabei können Werte wie Nichtschaden und Fairness wichtiger sein als Autonomie und Privatsphäre.

Résumé :
Le « big data divide » décrit la relation asymétrique entre ceux qui collectent, stockent et exploitent de grandes quantités de données (généralement des entreprises) et ceux qui sont la cible de cette collecte de données (p. ex. les clients). Cette contribution affirme que le dépassement du big data divide ne devrait pas être au centre des préoccupations éthiques. L'objectif devrait plutôt être de protéger les personnes potentiellement désavantagées par cette fracture.

Recommandations :
Le big data divide est une conséquence inévitable dans une société qui valorise la liberté et la diversité; éliminer cette fracture est un objectif politique erroné. Au lieu de cela, le législateur devrait identifier les préjudices réalistes susceptibles de résulter du big data divide et élaborer des garanties juridiques pour ceux qui sont désavantagés par cette fracture. Dans ce contexte, des valeurs comme la non-malfaisance et l'équité peuvent s'avérer plus pertinentes que l'autonomie et la vie privée.

Risks of discriminating against certain groups when using big data

Michele Loi

Michele Loi is a political philosopher by training interested in the ethical and political implications of algorithms and data. He is now researching algorithmic fairness with a Marie Sklowdoska-Curie Individual Fellowship at Milano Politecnico; moreover he continues to co-lead scientifically the project funded by the Swiss National Science Foundation “Socially acceptable AI and fairness tradeøffs in predictive analytics” (www.fair-ai.ch) as principal investigator with Prof. Christoph Heitz.

The debate on the social, political, and ethical implications of artificial intelligence, in particular machine learning, engages with normative concepts such as the fairness of predictive methods. However, the debate on what makes a prediction or a score associated with a prediction fair is far older. It can be traced back at least to the era of the Civil Rights Movement in the USA when the fairness of standardised university admission test scores was debated. That debate ceased without a clear reason before an answer was agreed upon (Hutchinson and Mitchell 2019). It was perhaps predictable that this debate could be reignited by the popularisation of statistical methods to make all kinds of decisions about people that have accompanied the development of machine learning and big data. So far, scientists have not agreed on what criterion or set of criteria an algorithm must pass to be characterised as free of bias or fair. This is an active area of research, in which linking the dots between the approaches of different disciplines is difficult but highly important. The dots that must be linked are several: between purported statistical tests of indirect discrimination based on theories of discrimination developed in law versus those developed in philosophy; between definitions of bias in data science and comparable definitions in the philosophy of science; and between definitions of fairness in machine learning and those in moral and political philosophy.

A value-free definition of “unbiased” or “fair” can be given, in the sense that the mere statement of a mathematical condition does not imply any value judgement (except possibly the judgment that it is worth spending the time to state it). Values, however, enter the debate, given that different definitions of fairness have been proposed in the field of statistics. Deciding which is appropriate, whether universally or for a specific use, is not an easy matter (Chouldechova 2017; Kleinberg et al. 2017; Barocas, Hardt, and Narayanan, incomplete work in progress). More than a single statistical condition appears to bare intuitions as stating an ideal that a fair, non-discriminatory, or bias-free prediction, test, or model, should achieve. Some of these definitions can be realised jointly but only in highly ideal circumstances—for example, by a model that predicts the future with perfect certainty—or when the base rates of the target to be predicted are distributed in identical proportions in different subpopulations (e.g., subpopulations of people who are similar in sex, gender, race, or ethnicity). The value-ladenness of the entire debate about bias is recognised by all (competent) parties in the debate as uncontroversial.[1]

The idea that bias and statistical indicators are value laden is not an arcane new concept proposed to replace more established ideas that are argued to be defective but rather rests on classical and widely used metrics. These are referred to as group-fairness criteria. Such criteria are used to measure treatment inequalities associated with individuals being members of particular groups. Although we have witnessed an explosion of new definitions in the last five years, the value-laden nature of the choice of a fairness standard or desideratum is clear even if only the simplest group metrics are considered. Even within this limited set of proposals, there are measures that are not only different but mathematically incompatible. Because of the incompatibility, statisticians and machine learning theorists are in the uncomfortable position of not being able to specify the conditions that make a statistical test fair from a purely scientific point of view. Before they do so, they have to justify morally why they choose a given definition of (un)fairness.

To be more concrete, consider the standard of equal calibration, or “test fairness” as it has been called (Chouldechova 2017). This requires that the result of a statistical test (e.g., an evaluation score) has the same meaning for members of different groups for which fairness is evaluated. The simplest example of this is when a score is intended as an indication of whether the individual has or will have some feature that is currently unknown—for example, whether an individual will graduate or avoid recidivism (criminal activity) during parole. For simplicity, we shall only consider binary predictions, where the goal is to ascertain whether an individual has (or will have) a given unknown property. Typically, the answer to this question produced by a statistical method is a score that has a value between 0 and 1. It is assumed that the score has some kind of informative relationship with the truth of the statement that the individual has the property or not. For example, the score may express the probability that the individual has a given property (belongs to the positive class). In that case, one would expect that among all people with the same score (e.g., 0.2), the score is approximately equal to the share of people who have (or will have) a certain property (e.g., 20%). It would appear unfair if, for example, among people with a score of 0.2, 10% of people from group A have the property, whereas 25% of people from group B have it. It therefore seems intuitive that a score that implies different probabilities for different people, depending on the group to which they

[1] For a useful reconstruction of the arguments, see Scantamburlo (2021).

belong, has some kind of bias and, when used, may lead to some kind of unfairness. And yet, the political discussion around the software COMPAS ended up branding a widely used software application as discriminatory (Angwin and Larson 2016a), even though the underlying statistical model satisfied precisely this criterion (Brennan, Dieterich, and Ehret 2009), and the requirement COMPAS was accused of violating was mathematically incompatible with it (Kleinberg et al. 2017; Chouldechova 2017).[2]

COMPAS is a tool that uses a statistical model to produce scores representing the chances an inmate will re-offend when released from prison. The scores in themselves do not indicate that a certain decision should be made. For instance, assigning a probability of recidivism of 0.8 to an inmate does not imply that the inmate should be given or denied parole. The company producing the tool, however, provides normative guidance suggesting risk thresholds for grouping candidates into low-risk, medium-risk, and high-risk categories. A study conducted by ProPublica showed that the average score among people who do not recidivate differed by race. Among people who did not recidivate, black defendants were more likely to be placed in the medium- or high-risk categories than white defendants, suggesting that recidivism in this group was overestimated relative to whites. Among defendants who did recidivate, white defendants were more likely to be placed in the low-risk category than black defendants, suggesting that recidivism is underestimated among white defendants relative to black ones. Both biases favoured white defendants relative to black defendants, so the ProPublica journalists and data scientists alleged that the statistical model led judges to make discriminatory bail decisions and possibly make discriminatory parole decisions (Angwin and Larson 2016a).

The bias in question, which amounts to a violation of the parity of false negative and false positive rates between groups, is mathematically inevitable whenever different base rates of recidivism occur in different populations if the same threshold values of risk are used to decide whether to give or deny parole or bail. Journalists popularised this result by saying that “bias is mathematically inevitable” (Angwin and Larson 2016b).

How has the theoretical discussion advanced since 2016? So far, the scientific community has not achieved a consensus on which measure is generally preferable, or which moral or scientific criteria should be used to determine whether the one or the other should be employed. At the same time, a new theoretical construct, called

[2] The rediscovery (Hutchinson and Mitchell 2019) of this long-forgotten fact was made in two publications with very high citation rates (Kleinberg et al. 2017; Chouldechova 2017) that formulated the problem in ways most accessible to data scientists.

“counterfactual fairness,” has been proposed by the machine learning community (Kusner et al. 2017). Despite having “fairness” in its name, counterfactual fairness is most easily understood as an attempt to model mathematically the existence of indirect discrimination. Notice that the recent shift to speaking more about fairness and less about discrimination is due precisely to the fact that what is discussed in data science is not discrimination in its most paradigmatic and easily detectable form, where the discriminator is fully conscious of the group of the discriminated person or at least has some degree of belief about it that plays a demonstrable role in reaching the discriminatory decision. Such cases of direct discrimination are very rare in machine learning because they are easily avoided by depriving the algorithm of all information about the protected group. Counterfactual fairness deals with this problem by using a dedicated statistical analysis to detect unequal predictions and decisions that can be causally attributed to group membership, even when the information about group membership is not available explicitly to the algorithm.

Despite the considerable number of academic papers on this approach by data scientists, philosophers of science, and moral philosophers (Glymour and Herington 2019; Herington 2020), counterfactual fairness is probably not considered the gold standard of fairness in machine learning. Although surveys are lacking, it appears that it might be less used in practice than the traditional group fairness criteria, which seem to have remained the standard. Part of the reason is that using counterfactual fairness as a standard requires data scientists to make commitments about social reality that they do not feel prepared to make. Moreover, counterfactual fairness raises a host of philosophical problems because it unavoidably presupposes some kind of theorisation of the nature of the causal interactions between social constructs (e.g., race and gender) and other features that are ordinarily used to make predictions. This is not an easy matter, to say the least. Several scholars have pointed out that it is unclear whether the causal properties attributed to such constructs in this methodology are compatible with a significant number of theories about the socially constructed reality of gender and race (as opposed to, for example, naturalistic categories such as sex, which, however, also has paths of social causation that make it difficult to distinguish from gender) (Kasirzadeh and Smart 2021; Hu and Kohler-Hausmann 2020). In addition to these problems, it is unclear whether counterfactual fairness is designed to provide a new theory of what is morally wrong with discrimination or a more general framework to be adapted to one’s preferred moral theory or the theory that proves most convincing from the normative point of view.
If the former, it appears that the account is either incomplete or, if interpreted as complete as it has been presented to date, faces some obvious objections such as direct conflicts with certain philosophical theorisations of what discrimination is.
If the latter, it appears that philosophical guidance for integrating moral theories of discrimination with the counterfactual criteria of fairness is still to be provided. An

alternative approach consists in reasoning morally about the implicit presuppositions, in terms of prescriptive desiderata within traditional definitions of group fairness, such as statistical parity, test fairness, and balanced positive and negative rates (Heidari et al. 2019; Hertweck, Heitz, and Loi 2021; Räz 2021; Loi, Herlitz, and Heidari 2021). Few scholars have taken this approach as it requires the tight integration of mathematical modeling and modeling of theories in moral or political philosophy. It has so far produced a limited number of publications but might provide some guidance in the future. Yet another approach consists in starting with a definition of fairness from philosophy or economics and investigating what it implies for machine learning (e.g., Gummadi and Heidari 2019; Liu et al. 2021). Interestingly, this approach and the previous one may eventually converge (Heidari et al. 2019).

Zusammenfassung:
Dieser Beitrag befasst sich mit dem Problem des Daten-Bias und der daraus möglicherweise folgenden Diskriminierung beim maschinellen Lernen. Kernpunkt des Beitrags ist, dass die Definition dessen, was als Diskriminierung gilt, nicht nur eine technische Angelegenheit ist, sondern eine normative Entscheidung. Wir überprüfen einige Definitionen von Diskriminierung, die derzeit entwickelt werden, und bewerten sie von einem normativen Standpunkt aus.

Empfehlungen:
Politische Entscheidungsträger sollten Fairness als Voraussetzung für die Gestaltung von algorithmischen Systemen in sensiblen Bereichen definieren. Diskriminierung wird nicht dadurch vermieden, indem man auf die Verarbeitung von bestimmten geschützten Merkmalen verzichtet. Stattdessen soll die Fairness von Algorithmen systematisch überprüft werden. Allfällige Antidiskriminierungs-Massnahmen müssen aber flexibel genug sein, um unterschiedliche statistische Standards für unterschiedliche Anwendungsfälle zu legitimieren.

Résumé :
Cette section examine le problème des a priori, de la discrimination et de l'iniquité dans l'apprentissage automatique. Le point principal de cette section est que la définition de ce qui est considéré comme un a priori ne relève pas seulement d'une question technique mais d'un choix normatif. Nous passons en revue certaines approches actuellement développées pour évaluer le choix d'une définition des a priori (ou de la discrimination, ou de l'iniquité) du point de vue normatif.

Recommandations :
Les décideurs politiques devraient faire de l'équité une exigence pour la conception de systèmes algorithmiques impliquant des enjeux importants. La discrimination ne s'évite pas en évitant le traitement des informations relatives aux groupes. Ces données doivent pouvoir être collectées afin de vérifier l'équité des algorithmes. Les politiques anti-discrimination doivent être suffisamment souples pour permettre l'emploi de différentes normes statistiques dans différents cas d'utilisation.

References

Amstutz, M. 2018. **Dateneigentum.** *Archiv für die civilistische Praxis* 218: 2–4.

Andrejevic, M. 2014. **The Big Data Divide.** *International Journal of Communication* 8: 1673–1689.

Angwin, J. and J. Larson. 2016a. **Machine Bias.** *ProPublica*. May 23, 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

———. 2016b. **Bias in Criminal Risk Scores Is Mathematically Inevitable, Researchers Say.** *ProPublica*. → https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say.

Article 29 Working Party. 2018. **Guidelines on Consent under Regulation** 2016/679. → https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (accessed 01.07.2020).

Barocas, S., M. Hardt, and A. Narayanan. Incomplete work in progress. *Fairness and Machine Learning*. → https://fairmlbook.org.

Berinato, S. 2015. **There's No Such Thing as Anonymous Data.** *Harvard Business Review*.

Brennan, T., W. Dieterich, and B. Ehret. 2009. **Evaluating the Predictive Validity of the Compas Risk and Needs Assessment System.** *Criminal Justice and Behavior* 36 (1): 21–40.

Brunschwig, C.R. 2001. **Visualisierung von Rechtsnormen: legal design.** *Zürcher Studien zur Rechtsgeschichte*: 45. Zürich: Schulthess.

Cate, F.H. and V. Mayer-Schonberger. 2013. **Notice and consent in a world of Big Data.** *International Data Privacy Law* 3 (2): 67–73. Available from: → https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipt005

Cavelty, M.D. and F. J. Egloff. 2019. **The Politics of Cybersecurity: Balancing Different Roles of the State.** *St Antony's International Review* 15 (1): 37–57.

Chander, A. and U.P. Le. 2014. **Data Nationalism.** *Emory Law Journal,* 64.

Chouldechova, A. 2017. **Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments.** *Big Data* 5 (2): 153–63. → https://doi.org/10.1089/big.2016.0047.

Coley, A. 2017. **International Data Transfers: The Effect of Divergent Cultural Views in Privacy Causes Déjà vu.** *Hastings Law Journal* 68 (5): 1111–1134.

Coordination Office for Human Research. 2019. *The Human Research Act and the Ethics Committees for Research*. → https://www.bag.admin.ch/bag/en/home/medizin-und-forschung/forschung-am-menschen/koordinationsstelle-forschung-mensch.html (accessed 20.03.2021).

Couture, S. and S. Toupin. 2019. **What does the notion of sovereignty mean when referring to the digital?.** *New Media & Society* 21 (10): 2305–2322. doi: 10.1177/1461444819865984.

D'Amico N., and B. Rütsche. 2015. *Humanforschungsgesetz (HFG). Bundesgesetz vom 30. September 2011 über die Forschung am Menschen*. Stämpfli. Available from: → https://www.staempfliverlag.com/detail/ISBN-9783727225611

De Mauro, A., M. Greco, M. Grimaldi M. 2016. **A formal definition of Big Data based on its essential features.** *Library Review* 65.

de Montjoye, Y.-A., L. Radaelli, V.K. Singh, and A.S. Pentland. 2015. **Unique in the shopping mall: On the reidentifiability of credit card metadata.** *Science* 347 (6221): 536.

Dönni, D. et al. 2015. **Schengen routing: A compliance analysis.** *Lecture Notes in Computer Science:* 100–112. doi: 10.1007/978-3-319-20034-7_11.

Ehrenstein, V., H. Nielsen, A.B. Pedersen, S.P. Johnsen, and L. Pedersen. 2017. **Clinical epidemiology in the era of big data: new opportunities, familiar challenges.** *Clinical epidemiology:* 9, 245.

Eichensehr, K.E. 2014. **The Cyber-Law of Nations.** *Georgetown Law Journal,* 103.

Eichensehr, K.E. 2016. **Data Extraterritoriality.** *Texas Law Review,* 95.

Elger, B.S., and A.L. Caplan. 2006. **Consent and anonymization in research involving biobanks: differing terms and norms present serious barriers to an international framework.** *EMBO Reports*, 7: 661-6.

Epiney, A. 2015. **Big Data und Datenschutzrecht – Gibt es einen gesetzgeberischen Handlungsbedarf?** *Jusletter IT,* 21. Mai 2015.

Farzanehfar, A., F. Houssiau, and Y.A. de Montjoye. 2021. **The risk of re-identification remains high even in country-scale location datasets.** *Patterns* 2 (3): 100204.

Favaretto, M., E. de Clercq, C.O. Schneble, and B.S. Elger. 2020. **What is your definition of Big Data? Researchers' understanding of the phenomenon of the decade.** *PLoS ONE* 15(2): e0228987.

Ferretti, A., M. Ienca, M.R. Velarde, S. Hurst, and E. Vayena. 2022. **The Challenges of Big Data for Research Ethics Committees: A Qualitative Swiss Study.** *Journal of Empirical Research on Human Research Ethics*, 17 (1-2): 129–143.

Genevieve, L.D., T. Wangmo, D. Dietrich, O. Woolley-Meza, A. Flahault, and B.S. Elger. 2018. **Research Ethics in the European Influenzanet Consortium: Scoping Review.** *JMIR Public Health & Surveillance,* 4: e67.

Gummadi, K.P. and H. Heidari. 2019. **Economic Theories of Distributive Justice for Fair Machine Learning.** *Companion Proceedings of the 2019 World Wide Web Conference*: 1301–1302. → https://doi.org/10.1145/3308560.3320101.

Glymour, B., and J. Herington. 2019. **Measuring the Biases That Matter. The Ethical and Casual Foundations for Measures of Fairness in Algorithms.** *Proceedings of the Conference on Fairness, Accountability, and Transparency:* 269–278.

Hajian, S., F. Bonchi, and C. Castillo. 2016. **Algorithmic bias: From discrimination discovery to fairness-aware data mining.** *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining:* 2125–2126.

Hafen, E. 2015. **MIDATA cooperatives - citizen-controlled use of health data is a pre-requiste for big data analysis, economic success and a democratization of the personal data economy.** *Tropical Medicine & International Healt*h 20: 129.

Heidari, H., M. Loi, K.P. Gummadi, and A. Krause. 2019. **A Moral Framework for Understanding Fair ML Through Economic Models of Equality of Opportunity.** *Proceedings of the Conference on Fairness, Accountability, and Transparency*: 181–90. → https://doi.org/10.1145/3287560.3287584.

Herington, J. 2020. **Measuring Fairness in an Unfair World.** *Proceedings of 2020 AAAI-ACM Conference on Artificial Intelligence, Ethics, and Society*. → https://doi.org/10.1145/3375627.3375854.

Hertweck, C., C. Heitz, and M. Loi. 2021. **On the Moral Justification of Statistical Parity."** *FAccT 2021, Virtual Event, Canada*. → https://doi.org/10.1145/3442188.3445936.

Hill, J.F. 2014. **The growth of data localization post Snowden: analysis and recommendations for US policymakers and industry leaders.** *Lawfare Research Paper Series* 2 (3): 1–41.

Hornung, G., C. Schnabel. 2009. **Data protection in Germany I: The population census decision and the right to informational self-determination.** *Computer Law & Security Review* 25 (1): 84–88.

Hu, L., and I. Kohler-Hausmann. 2020. **What's Sex Got to Do with Machine Learning?** *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. → https://doi.org/10.1145/3351095.3375674.

Hutchinson, B., and M. Mitchell. 2019. **50 Years of Test (Un)Fairness: Lessons for Machine Learning.** *Proceedings of the Conference on Fairness, Accountability, and Transparency*: 49–58. → https://doi.org/10.1145/3287560.3287600.

Ienca, M., F.J., B.S. Elger, M. Caon, A. Scoccia Pappagallo, R.W. Kressig, and T. Wangmo. 2017. **Intelligent assistive technology for Alzheimer's disease and other dementias: a systematic review.** *Journal of Alzheimer's Disease* 56 (4): 1301-1340.

Ienca, M., A. Ferretti, S. Hurst, M. Puhan, C. Lovis, and E. Vayena. 2018. **Considerations for ethics review of big data health research: A scoping review.** *PloS one* 13 (10): e0204937.

Kairouz, P., S. Oh, and P. Viswanath. 2017. **The Composition Theorem for Differential Privacy.** *IEEE Transactions on Information Theory* 63 (6).

Kasirzadeh, A., and A. Smart. 2021. **The Use and Misuse of Counterfactuals in Ethical Machine Learning.** *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*: 228–36. → https://doi.org/10.1145/3442188.3445886.

Kaye, J., E.A. Whitley, D. Lund, M. Morrison, H. Teare, K. Melham. 2015. **Dynamic consent: a patient interface for twenty-first century research networks.** *European Journal of Human Genetics* 23 (2): 141–6. Available from: → http://www.ncbi.nlm.nih.gov/pubmed/24801761.

Kleinberg, J., H. Lakkaraju, J. Leskovec, J. Ludwig, and S. Mullainathan. 2017. **Human Decisions and Machine Predictions.** Working Paper 23180. *National Bureau of Economic Research*. → https://doi.org/10.3386/w23180.

Kusner, M.J., J.R. Loftus, C. Russell, and R. Silva. 2017. **Counterfactual Fairness.** *ArXiv:1703.06856*. → http://arxiv.org/abs/1703.06856.

Liu, D., Z. Shafi, W. Fleisher, T. Eliassi-Rad, and S. Alfeld. 2021. **RAWLSNET: Altering Bayesian Networks to Encode Rawlsian Fair Equality of Opportunity.** *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society:* 745–55. → https://doi.org/10.1145/3461702.3462618.

Loi, M., A. Herlitz, and H. Heidari. 2021. **Fair Equality of Chances for Prediction-Based Decisions.** *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* 756. → https://doi.org/10.1145/3461702.3462613.

Maaßen, C. 2015. **C. Die rechtlichen Grundlagen der klinischen Prüfung. 1. Preußischer Erlass vom 29.12.1900.** in C. Maaßen (ed.) *Die Versicherung klinischer Arzneimittel- und Medizinprodukteprüfungen (Europäische Hochschulschriften Recht)*, Peter Lang: Frankfurt am Main.

Martani, A., P. Egli, M. Widmer, B.S. Elger. 2020. **Data protection and biomedical research in Switzerland: setting the record straight.** *Swiss Medical Weekly*: 150: w20332.

Möllers, N. 2021. **Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State.** *Science, Technology, & Human Values* 46 (1): 112–38. doi: 10.1177/0162243920904436.

Murdoch, T.B., and A.S. Detsky. 2013. **The inevitable application of big data to health care.** *Jama* 309 (13): 1351–2. pmid:23549579.

Parasidis, E., E. Pike, D. McGraw. 2019. **A Belmont report for health data.** *The New England Journal of Medicine*, 380 (16): 1493–1495.

Peters, B. 2016. **Digital**, in Peters, B. (ed.) *Digital Keywords: A Vocabulary of Information Society and Culture*. Princeton University Press: Princeton.

Philpott, D. 2020. **Sovereignty**, in Zalta, E. N. (ed.) *The Stanford Encyclopedia of Philosophy.*

Picht, P.G. 2017. **Dateneigentum und Datenzugang – Schutz von Geschäftsgeheimnissen als Alternative?** *Jusletter IT,* Flash *(*11. 12. 2017.

Price, W.N. and I.G. Cohen. 2019. **Privacy in the age of medical big data.** *Nature medicine* 25 (1): 37–43.

Pohle, J. and T. Thiel. 2020. **Digital sovereignty.** *Internet Policy Review*: 1–19. doi: 10.14763/2020.4.1532.

Räz, T. 2021. **Group Fairness: Independence Revisited.** *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*: 129-37. → https://doi.org/10.1145/3442188.3445876.

Rothstein, M.A. 2015. **Ethical Issues in Big Data Health Research: Currents in Contemporary Bioethics**. *Journal of Law, Medicine & Ethics* 43: 425-9.

Rouvroy A., Y. Poullet. 2009. **The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy.** In Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds.) *Reinventing Data Protection?*. Springer: Dordrecht. → https://doi.org/10.1007/978-1-4020-9498-9_2.

Samarati, P., L. Sweeney L. 1998. **Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression.** Available from: → http://citeseerx.ist.psu.edu/viewdoc/summary?-doi=10.1.1.37.5829

Scantamburlo, T. 2021. **Non-Empirical Problems in Fair Machine Learning.** *Ethics and Information Technology*, August. → https://doi.org/10.1007/s10676-021-09608-9.

Schneble, C.O., B.S. Elger, D.M. Shaw. 2018. **The Cambridge Analytica affair and Internet-mediated research.** *EMBO Reports* 19 (8): e46579. Available from: → http://www.ncbi.nlm.nih.gov/pubmed/29967224

Schneble, C.O., B.S. Elger, and D.M. Shaw. 2020a. **All Our Data Will Be Health Data One Day: The Need for Universal Data Protection and Comprehensive Consent.** *Journal of Medical Internet Research* 22: e16879.

Schneble, C.O., B.S. Elger, and D.M. Shaw. 2020b. **Data protection during the coronavirus crisis.** *EMBO Reports* 21: e51362.

Schneble, C.O., B.S. Elger, and D.M. Shaw. 2020c. **Google's Project Nightingale highlights the necessity of data science ethics review.** *EMBO Molecular Medicine 12 (3): e12053.*

Schneble, C.O., M. Favaretto, B.S. Elger, and D.M. Shaw. 2021. **Social Media Terms and Conditions and Informed Consent From Children: Ethical Analysis.** *JMIR Pediatrics and Parenting* 4: e22281.

Smuck, M., C.A. Odonkor, J.K. Wilt, N. Schmidt, and M.A. Swiernik. 2021. **The emerging clinical role of wearables: factors for successful implementation in healthcare.** NPJ *Digital Medicine* 4 (1): 1–8.

Steinsbekk, K.S., B. Kare Myskja, B. Solberg. 2013. **Broad consent versus dynamic consent in biobank research: Is passive participation an ethical problem?** *European Journal of Human Genetics* 21 (9).

Stephens, Z.D. et al. 2015. **Big data: astronomical or genomical?** *PLoS biology* 13 (7): e1002195.

Swiss Confederation. 2011. **HFG (Humanforschungsgesetz). Law on human subject research [Loi relative à la recherche sur l'être humain]**, adopted by the parliament on 30.9.2011. Available from: → https://www.fedlex.admin.ch/eli/oc/2013/617/de

Taylor, L. 2017. **What is data justice? The case for connecting digital rights and freedoms globally.** *Big Data & Society*, 4 (2).

Terry, N.P. 2014. **Big data proxies and health privacy exceptionalism**. *Health Matrix Clevel*, 24: 65-108.

Torra, V. and G. Navarro-Arribas. 2016. **Big Data Privacy and Anonymization.** In Lehmann A., Whitehouse D., Fischer-Hübner S., Fritsch L., Raab C. (eds.) *Privacy and Identity Management Facing up to Next Steps*. 11th IFIP WG 92, 95, 96/117, 114, 116/SIG 922 International Summer School, Karlstad, Sweden, Cham: Springer International Publishing: 15–26. Available from: → https://doi.org/10.1007/978-3-319-55783-0_2.

Vayena, E. and A. Blasimme. 2018. **Health research with big data: Time for systemic oversight.** *The Journal of Law, Medicine & Ethics*, 46 (1): 119–129.

von Elm, E. and M. Briel. 2019. *Survey on researchers' opinion about and experience with the Swiss Federal Act on Research involving human beings*. Available from: → https://www.bag.admin.ch/dam/bag/de/dokumente/biomed/forschung-am-menschen/forschung-biomedizin/Hauptbericht-Befragung.pdf.download.pdf/190715_EDFI_Main%20Report (accessed 27.10.21).

Widmer, M., C.O. Schneble, P. Egli, B.S. Elger. 2021. **«Eigentum» an Patientendaten – Wer meint damit eigentlich was?** *Pflegerecht* 2: 97–105.

Weber, R. and T. Thouvenin. 2018. **Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?** *Zeitschrift für Schweizerisches Recht*.

World Medical Association. 2008. **WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects, amended by the 59th WMA General Assembly, Seoul, Korea.** Available from: → https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/

Yoshiura, H. 2019. **Re-identifying people from anonymous histories of their activities.** *2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST)*: 1–5.

Zuiderwijk, A., M. Janssen, S. van den Braak, Y. Charalabidis. 2012. **Linking open data: challenges and solutions**. *Proceedings of the 13th Annual International Conference on Digital Government Research:* 304–305. → https://doi.org/10.1145/2307729.2307797

COMMENTARY ARTICLES

New approaches to data and big data in trade agreements

Lack of protections for vulnerable groups in big data research

Big data from the perspective of business ethics

New approaches to data and big data in trade agreements
Mira Burri

Mira Burri is Professor of International Economic and Internet Law at the Faculty of Law of the University of Lucerne. She teaches international intellectual property, media, internet and trade law. Mira's current research interests are in the areas of digital trade, culture, copyright, data protection and data governance. Mira is the principal investigator of the project 'Trade Law 4.0' (ERC Consolidator Grant 2021–2026). She consults the European Parliament, UNESCO, the WEF and others on issues of digital innovation and cultural diversity.

Introduction: From E-Commerce to the Data-Driven Economy

The critical importance of data for all economic sectors seems nowadays uncontested. Beyond the somewhat flawed mantra of data being the "new oil" (The Economist 2017), many studies point to the enormous potential of data to enable more efficient business operations, more innovative solutions, and better policy choices in all areas of society (Manyika et al. 2011; Mayer-Schönberger and Cukier 2013; Henke et al. 2016). It is noteworthy that this transformative capacity refers not only to "digital native" areas, such as search engines and social networks, but also to "brick-and-mortar" businesses, such as those in manufacturing and logistics (Manyika et al. 2011). The COVID-19 pandemic has only augmented the value of digital transactions and the significance of data-driven platforms (e.g., WTO 2020). Emerging technologies, like Artificial Intelligence (AI), are also highly dependent on data inputs (The Royal Society 2017). With regard to trade, it can be argued that we have moved on from the age of electronic commerce (e-commerce), where goods and services were traded online to economies, and indeed societies, driven by and dependent on data. This shift has frequently been discussed in association with the Fourth Industrial Revolution (Floridi 2014; Schwab 2017). At the same time, and as has been well documented, the increased dependence on data has brought about a new set of concerns. The impact of data collection, use, and re-use on privacy has been widely acknowledged by scholars and policymakers alike, while also being felt by regular users of digital products and services. The risks to privacy have only augmented in the era of big data (e.g., Mayer-Schönberger and Cukier 2013; Burri 2019), which presents distinct challenges to the protection of personal data and, by extension, to the safeguarding of personal and family life (e.g., Tene and Polonetsky 2013; The White House 2014; Gasser 2016; Pan 2016; Council of Europe 2017).

Governments have not been idle and have responded to these concerns in a variety of ways. In terms of external safeguards, states have sought new ways to assert control over data—in particular, by prescribing measures to "localise" data, its storage, or its suppliers, so as to keep it within the state's sovereign territory (e.g., Chander 2016; Ferracane 2021). However, erecting barriers to data flows affects trade and may endanger the realisation of an innovative data economy (USITC 2013, 2014), even in a domestic context (e.g., Ferracane 2021). Many of the innovations that we are used to in everyday life—streaming, cloud computing, the app economy, or, if we think in more future-oriented terms, the Internet of things (IoT) and AI—would not function under restrictions of cross-border data flows (e.g., Chander 2021).

In terms of internal safeguards, the preoccupation with the perceived perils of big data has triggered the reform of data protection laws around the world, as perhaps best exemplified by the European Union (EU)'s adoption of the 2016 General Data Protection Regulation (GDPR). Such reform initiatives are not, however, coherent. Indeed, they are culturally and socially embedded, reflecting societies' constitutional values, relationships between citizens and the state, and the role of the market, among other factors (e.g., Burri 2021a). The striking divergence in both the perceptions and the regulation of privacy protection across nations—and, in particular, between the fundamental rights approach of the EU and the more market-based, laissez-faire approach of the United States—has meant that conventional forms of international cooperation, and agreement on shared standards of data protection, appear highly unlikely (e.g., Schwartz and Solove 2014; Burri 2021a).

Developments in Global Trade Law

Against this backdrop of a complex and contentious regulatory environment, data and cross-border data flows have become important topics in global trade law discussions. With the stalemate at the multilateral forum of the World Trade Organization (WTO) (e.g., Burri 2015, 2017)—and despite the current revival of the e-commerce negotiations (WTO 2019; Burri 2021b)—new rule-making has unfolded predominantly in preferential trade venues of a bilateral or regional nature (Burri 2015, 2017; WTO 2018). A project of NRP 75 ("The Governance of big data in Trade Agreements") has traced these developments in free trade agreements (FTAs) and analysed their evolution along with the positioning of stakeholders. It has done this by comprehensively mapping all data-related norms, so as to facilitate the understanding of the big picture of digital trade regulation and its implications. This comment showcases some of the project's results, stressing the critical importance of trade law and linking with the discussions of the main article of the ELSI White Paper on data sovereignty (Viganò's main article) and data protection in a fluid technological environment (Schneble's main article).

The regulatory landscape has indeed profoundly changed in recent years and our careful analysis of more than 350 FTAs attests to the heightened preoccupation of policymakers with digital trade, which has translated into an increased density and bindingness of the commitments that the parties have agreed to.[1] In the context of these new developments in international economic law, relevant questions that may be asked are whether any nascent trends can be discerned and, perhaps even more importantly, what the real implications of the intensified rule-making on data are. The next sections briefly address these pertinent questions, while also providing a basis for recommendations of a more proactive approach by Switzerland.

Evolution and Trends in Data Flow Rule-Making

First, it is important to note that the new regulatory framework, which has been substantially shaped by FTAs, goes well beyond WTO rules and the mere attempt to reduce trade barriers in the areas of goods and services trade (Burri 2017; Burri 2021c). The framework deals with distinct aspects of digital trade and cross-border data flows, striving for legal certainty for the businesses involved and a level of interoperability between the different domestic regimes. Particularly noteworthy in the latter context is the increased number of rules on free data flows and the prohibition of data localisation measures (Burri 2021c). The 2018 Comprehensive and Progressive Agreement for Transpacific Partnership (CPTPP), agreed to by eleven countries in the Pacific Rim,[2] and the renegotiated NAFTA, now referred to as the "United States-Mexico-Canada Agreement" (USMCA), are particularly important in this sense. They have created the most comprehensive template for digital trade governance so far by including a number of new features, such as provisions on domestic electronic transactions, personal information protection, Internet interconnection charge sharing, location of computing facilities, unsolicited commercial electronic messages, net neutrality, and source code.

Second, it is notable that the United States has played a key role in this process and has sought to endorse liberal rules in the implementation of its "Digital Agenda." The emergent regulatory template on digital issues is not, however, limited to US agreements; it has diffused and can be found in other FTAs. Singapore, Australia, Japan, and Colombia have been among the major drivers of this diffusion (Elsig and Klotz 2021). We have also recently seen the adoption of particularly detailed dedicated

[1] The information stems from our own dataset, TAPED: Trade Agreement Provisions on Electronic Commerce and Data. The TAPED dataset is available for general use and has been developed under the creative commons (attribution, non-commercial, share-alike) license at the University of Lucerne website (https://www.unilu.ch/taped) (Burri and Polanco 2020).

[2] Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam.

digital economy agreements, such as the ones between Chile, New Zealand, and Singapore (Digital Economy Partnership Agreement, DEPA), and between the United States and Japan (Digital Trade Agreement, DTA). Embedded features of all these agreements is that they provide for free data flows, compatibility with lower standards of domestic data protection and priority is given to trade over privacy protection (Burri 2021b).

Third, the EU has been, in general, cautious when committing in the area of digital trade (e.g., Burri 2017), particularly when inserting rules on data in its free trade deals. It is only recently that the EU has made a step towards such rules, whereby parties have agreed to consider in future negotiations commitments related to the cross-border flow of information. Such a clause is found in the 2018 EU-Japan Economic Partnership Agreement (EPA) and in the updated trade part of the EU-Mexico Global Agreement. In both of these agreements, the parties commit to "reassess," within three years of the agreement coming into force, the need to include provisions on the free flow of data in the treaty. This signalled a repositioning of the EU on the issue of data flows, which is now fully endorsed in its currently negotiated deals with Australia, New Zealand, and Tunisia, which include in their draft digital trade chapters norms on the free flow of data and data localisation bans. This repositioning has been confirmed by the now finalised post-Brexit Trade and Cooperation Agreement (TCA) between the EU and the United Kingdom. However, the newer commitments are also linked to the high data protection standards of the GDPR, which enshrine data protection as a fundamental human right and include a number of safeguards for the EU's current and future measures in this area. It is apparent, therefore, that personal data protection has become an important topic on trade negotiation tables, as well as a major battlefield between the key stakeholders (e.g., Farrell and Newman 2019; Burri 2021a).

Fourth, beyond the competing models of the US and the EU, there are a great number of states that still need to define a clear approach towards digital trade and, in particular, data flows. China, another key actor and one typically associated with highly restrictive policies that seek to protect its national sovereignty to the fullest, has recently taken some interesting steps in this regard—specifically, the China's commitments on conditional data flows under the 2020 Regional Comprehensive Economic Partnership (RCEP) and its newly expressed wish to join the CPTPP. The United Kingdom is another actor to watch out for. Although it has strong links with the EU, including in the area of data protection, the UK has, post-Brexit, taken a more liberal stance on the international stage, pursuing membership of the CPTPP as well as an agreement with the United States. Switzerland belongs to the group of late-comers in the domain of digital trade policy and has for an astonishingly long time not defined a discrete strategy. The newly developed model chapter on e-commerce follows the EU's approach but remains somewhat uninspired and less innovative in comparison to the US-led agreements and, especially, to the digital economy partnerships, such as the one between Chile, New Zealand, and Singapore, which touch upon newer issues like digital identities and AI (Burri 2021a).

Concluding Remarks

The era of big data has ushered in new challenges for global trade law. Policymakers face the extremely difficult task of matching the existing, largely analogue-based, institutions and rules of international economic law with the dynamic, scruffy innovation of digital platforms (e.g., Benkler 2011; Yu 2014) and data that flows regardless of state borders. At the same time, and which only makes the task more demanding, it is evident that the future regulatory framework will have immense effects on innovation and the fate of the data-driven economy (e.g., Chander 2014, 2021), as well as on fundamental rights beyond the economic domain, such as the protection of citizens' privacy. Despite the importance and the urgency of finding appropriate governance solutions, global trade law has so far not undergone a radical overhaul, and legal adaptation has been slow and patchy. Where digital trade rules have been adopted, FTAs have become the preferred venue. These agreements partly compensate for the lack of progress under the umbrella of the WTO. More importantly, however, they create rules that address new trade barriers, such as data localisation measures, as well as new and pressing concerns, such as the acute need to interface trade and personal data protection mechanisms. Above all, FTAs provide a regulatory environment that reflects the practical reality of digital trade and ensures a level of legal certainty for all actors involved.

Understanding the existing rules on digital trade and their evolution over time is absolutely essential for future attempts by individual states and the international community to grapple with the digital challenge. It may also be important for other actors, such as companies, think-tanks, non-governmental organisations, and even individual citizens, who may wish to become more actively engaged in the rule-making processes of trade agreements, which tend to be carried out behind closed doors and with little-to-no stakeholder involvement (e.g., Cho and Kelly 2013). The experience gathered in FTAs is also invaluable for the ongoing, reinvigorated efforts in the WTO to reach an agreement on e-commerce—as well as in the new, bolder deals that go beyond existing commitments and look at a range of emerging issues, such as digital identity, AI, electronic invoicing, and open governance data.

As a final thought, it should be stressed that the data economy has placed greater demands on regulatory cooperation. As the complexity of the data-driven society increases, enhanced regulatory cooperation seems indispensable for moving forward, since data issues cannot be covered by the traditional "lower tariffs, more commitments” stance in trade negotiations, but entail the need for reconciling different interests and providing oversight. In this context, while the paths for engaging in and advancing regulatory cooperation would ideally be followed in the multilateral forum of the WTO (e.g., Mitchell and Mishra 2021), preferential trade venues can serve as valuable governance laboratories. Though it has so far made only a hesitant start in this direction, Switzerland could play an important role in the future as a legal entrepreneur, both in the multilateral and preferential trade venues.

Zusammenfassung:
Digitaler Handel und Data Governance sind auf der Agenda der politischen Entscheidungsträger nach oben gerückt. Dies, weil der Wert von Daten für moderne Volkswirtschaften stark gestiegen ist, was in allen Bereichen des gesellschaftlichen Lebens zu regulatorischen Herausforderungen geführt hat, etwa im Hinblick auf den Schutz der Privatsphäre. In den letzten zwei Jahrzehnten sind Handelsabkommen zu einer wichtigen Plattform für die Regelsetzung geworden, was über blosse Liberalisierungsbemühungen hinausgeht und das regulatorische Umfeld in Bezug auf Daten effektiv gestaltet. Der Kommentar bietet einen kurzen Überblick und eine Kontextualisierung dieser Entwicklungen.

Résumé
Le commerce numérique et la gouvernance des données ont gagné en importance sur l’ordre des jours des décideurs politiques – d’une part parce que la valeur des données a augmenté de façon exponentielle dans les économies modernes, et d’autre part parce que cela a déclenché des défis réglementaires dans tous les aspects de la vie en société, par exemple en ce qui concerne la protection de la vie privée. Au cours des deux dernières décennies, les accords commerciaux sont devenus une plate-forme importante pour l’élaboration de règles, qui vont au-delà des simples efforts de libéralisation et façonnent efficacement l’environnement réglementaire en matière de données. Ce commentaire offre un bref aperçu et une mise en contexte de ces développements.

References

Benkler, Y. 2011. **Growth-Oriented Law for the Networked Information Economy: Emphasizing Freedom to Operate over Power to Appropriate.** In Kauffman Taskforce on Law, Innovation and Growth (ed.), *Rules for Growth: Promoting Innovation and Growth through Legal Reform*. Kansas City: Kauffman Foundation: 313–342.

Burri, M. 2015. **The International Economic Law Framework for Digital Trade.** *Zeitschrift für Schweizerisches Recht* 135: 10–72.

Burri, M. 2017. **The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation.** *UC Davis Law Review* 51 (2017), 65–132.

Burri, M. 2019. **Understanding the Implications of Big Data and Big Data Analytics for Competition Law: An Attempt for a Primer.** In K. Mathis and A. Tor (eds.), *New Developments in Competition Behavioural Law and Economics*. Berlin: Springer: 241–263.

Burri, M. 2021a. **Interfacing Privacy and Trade.** *Case Western Journal of International Law* 53: 35–88.

Burri, M. 2021b, **Towards a New Treaty on Digital Trade.** *Journal of World Trade* 55: 71–100.

Burri, M. 2021c. **Data Flows and Global Trade Law.** In M. Burri (ed.), *Big Data and Global Trade Law Cambridge*: Cambridge University Press: 11–41.

Burri, M. and R. Polanco. 2020. **Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset.** *Journal of International Economic Law* 23: 187–220.

Chander, A. 2014. **How Law Made Silicon Valley**. *Emory Law Journal* 63: 639–694.

Chander, A. 2016. **National Data Governance in a Global Economy**. *UC Davis Legal Studies Research Paper* 495.

Chander, A. 2021. **Artificial Intelligence and Trade.** In M. Burri (ed.), Big Data and Global Trade Law. Cambridge: *Cambridge University Press*: 115–127.

Cho, S., and C.R. Kelly. 2013. **Are World Trading Rules Passé?** *Vanderbilt Journal of International Law* 53: 623–666.

Council of Europe. 2017. *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, Strasbourg, T-PD (2017) 01.

Elsig, M., and S. Klotz. 2021. **Data Flow-Related Provisions in Preferential Trade Agreements: Trends and Patterns of Diffusion.** In M. Burri (eds.), *Big Data and Global Trade Law*. Cambridge: Cambridge University Press: 42–62.

Farrell, H., and A.L. Newman. 2019. Of Privacy and Power: *The Transatlantic Struggle over Freedom and Security*. Princeton: Princeton University Press.

Ferracane, M.F. 2021. **The Costs of Data Protectionism.** In M. Burri (ed.), *Big Data and Global Trade Law*. Cambridge: Cambridge University Press: 63–82.

Floridi, L. 2014. *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality*. Oxford: Oxford University Press.

Gasser, U. 2016. **Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy.** *Harvard Law Review* 130 (2): 61–70.

Henke, N., J. Bughin, M. Chui, J. Manyika, T. Saleh, B. Wiseman, and G. Sethupathy. 2016. *The Age of Analytics: Competing in a Data-Driven World*. Washington, DC: McKinsey Global Institute.

Manyika, J., M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, and A. Hung Byers. 2011. *Big Data: The Next Frontier for Innovation, Competition, and Productivity*. Washington, DC: McKinsey Global Institute.

Mayer-Schönberger, V., and K. Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. New York: Eamon Dolan/Houghton Mifflin Harcourt.

Mitchell, A.D., and N. Mishra. 2021. **WTO Law and Cross-Border Data Flows: An Unfinished Agenda.** In M. Burri (ed.), *Big Data and Global Trade Law*. Cambridge: Cambridge University Press: 82–112.

Pan, S.B. 2016. **Get to Know Me: Protecting Privacy and Autonomy under Big Data's Penetrating Gaze.** *Harvard Journal of Law and Technology* 30: 239–261.

Schwab, K. 2017. *The Fourth Industrial Revolution*. New York: Portfolio.

Schwartz, P.M., and D.J. Solove. 2014. **Reconciling Personal Information in the United States and European Union.** *California Law Review* 102: 877–916.

Tene, O., and J. Polonetsky. 2013. **Big Data for All: Privacy and User Control in the Age of Analytics.** *Northwestern Journal of Technology and Intellectual Property 11*: 239–273.

The Economist. 6 May 2017. **The World's Most Valuable Resource Is No Longer Oil, But Data.**

The Royal Society. 2017. *Machine Learning: The Power and Promise of Computers That Learn by Example*. London: The Royal Institute.

United States International Trade Commission (USITC). 2013. *Digital Trade in the US and Global Economies, Part 1*, Investigation No 332–531. Washington, DC: USITC.

USITC. 2014. *Digital Trade in the US and Global Economies, Part 2*, Investigation No 332–540. Washington, DC: USITC.

The White House. May 2014. *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President.

WTO. 2018. World Trade Report 2018: *The Future of World Trade: How Digital Technologies Are Transforming Global Commerce*. Geneva: World Trade Organization.

WTO. 25 January 2019. *Joint Statement on Electronic Commerce,* WT/L/1056.

WTO. 4 May 2020. *E-Commerce, Trade and the Covid-19 Pandemic*, Information Note by the WTO Secretariat.

Yu, P. K. 2014. **Trade Agreement Cats and Digital Technology Mouse.** In B. Mercurio and N. Kuei-Jung (eds.), *Science and Technology in International Economic Law: Balancing Competing Interests*. Abington: Routledge: 185–211.

Lack of protections for vulnerable groups in big data research

David Shaw

David Shaw is Senior Researcher in Biomedical Ethics at the University of Basel and Associate Professor of Health Law and Ethics at Maastricht University. His background is in philosophy and bioethics, and he is an expert on organ donation, research ethics and research integrity.

Introduction

It is a well-known cliche that just because scientists can do something does not mean they should do it. Unfortunately, science often advances at such a speed that ethical considerations are an afterthought or at least lag behind. And just as ethics often struggles to keep up with scientific innovation, so research ethics systems struggle to adapt to new ways of doing research. In this commentary, I revisit the issues of informed consent, the transparency asymmetry between companies and individuals, and discrimination against certain groups, discussed respectively in Elger's, Christen's, and Loi's main articles of this white paper to explore the lack of protections for vulnerable groups in big data research.

In the decades since the Second World War, humans participating in scientific research have become subject to a series of protections designed to protect them from harm and ensure that their autonomy is respected. Institutional review boards (IRBs) and research ethics committees (RECs) are the governance structures that evaluate research proposals to ensure that participants are provided with sufficient protection. Until fairly recently, however, the principles and mechanisms of research ethics were geared solely towards biomedical research, in which experiments of one sort or another are conducted on human beings. The classic example is the clinical trial, in which a new drug is tested on healthy volunteers or people who are sick. When reviewing research projects, IRBs and RECs pay particular attention to the potential exploitation of *vulnerable groups*—a catch-all term that can include children, elderly people, pregnant women, ethnic minorities, people with mental health issues, or anyone who lacks the capacity to consent to participation in research.

As the development of new ways of doing research has expanded human involvement beyond clinical trials, corresponding ethical governance methods have, belatedly, emerged. Many universities now have committees that evaluate psychology research, sociology research, and even survey research, where the risk of harm might seem low but still exists. Committees also seek to check that participants' time is not being wasted on pointless research. But another type of research challenges ethical oversight mechanisms to an even greater extent: big data research and, specifically, internet-mediated research (IMR). IMR can be conducted ethically but also raises several issues that do not occur in more traditional clinical or sociological research.

The challenges of big data research

The classic example of big data IMR is social media research. Facebook, Instagram, WhatsApp, and Twitter are only four examples of online spaces in which billions of people share information about their lives every day. Such websites are very popular because they enable people to stay in touch very easily and share their stories with their friends without having to be in the same place as them. Thus, many of us can now stay in touch with friends on multiple continents, some of whom we may never have met in person.

Yet the ease with which information can be shared with people all over our planet also hints at the types of problems that can affect social media and research employing this medium. If it is easy to share your data, then it is easy for other people to access your data. And if you want to share your data to the maximal extent, you will set your privacy settings—which give you some control over who can view your posts—to public.

Now, that might not seem to be a problem. After all, people know what they sign up to when they start using Facebook or other social media, and they can control who sees their posts. However, the previous sentence has two errors in it. First, many people simply tick the box at the bottom of the terms and conditions for social media software and apps without reading the text itself, so they do not know what they are signing up for. Of course, that could be seen as their problem, but one of the concerning issues with the social media giants is that one must accept all of their terms to access their services; one cannot opt out of the bits one dislikes. So, if you want to use Facebook, you have no choice but to accept the terms—a possible reason why people don't bother to read the agreement properly. Second, while it is true that on Facebook one's privacy settings can be chosen so that no one, or only friends, or only friends of friends, or absolutely anyone can see your posts, the terms and conditions also state that Facebook may use your data for *its own* research. So, anyone signing up to Facebook gives their consent to being a research participant, even if they haven't realised that.

The fact that consent to research can be given at the point of initial access to social media is highly problematic. Normally participants are informed about a specific research project and the associated potential harms before deciding whether to consent to their involvement. An agreement to participate in research obtained from someone who doesn't know what is involved in the research amounts to exceptionally broad consent—all the more so if the person consenting did not realise what they were agreeing to. In such cases, any consent gained may be legally valid but nonetheless is ethically worthless.

At the other end of the ethical spectrum, the use of social media data by researchers raises a different issue: the participants are remote from the researchers in time and space and thus are less known or knowable than typical research participants. Their social media accounts may contain a great deal of data, but the data are not necessarily reliable; people can say whatever they want about themselves online. And even if the data are reliable, it is still impossible for researchers to apply the usual safeguards, such as verifying that a person is competent to give consent or is not a member of a vulnerable group.

Vulnerable groups and big data research

The ethical issues discussed above apply all the more to vulnerable groups such as children, but there are additional potential problems. Children and people with mental health issues are perhaps less likely to care about the contents of the terms and conditions when signing up for a service they want to access. This is particularly true of children who sign up for accounts despite being below the minimum age for doing so. Even if such children do read the conditions of use, they are likely to disregard them because they want to use the service. It might be assumed that social media companies valued at billions of dollars have age verification features in place, but this is normally not the case. Anyone with an e-mail address can set up accounts on Facebook and many other services (Schneble et al. 2021). Some social media platforms do have age verification components, but the evidence suggests that many parents are happy to help their children circumvent such protections—in effect, endorsing their underage use of social media. Indeed, parents are often Facebook friends of their children, despite the latter not being old enough to use Facebook in line with the terms and conditions of the platform.

The implications for researchers of children who are too young to be permitted to use social media should now be obvious: if many Facebook users are underage children, that means that any research using Facebook data is likely to involve children who are too young to use the service and very probably too young to consent to their participation in research, depending on the jurisdiction. (Given that Facebook is a global company, the legal context will vary.) In the UK, 30% of 5 to 7-year-olds and 44% of 8 to 11-year-olds had a social media account in 2020, indicating the scope of the problem (Ofcom, 2020).

The fact that children and people with mental health problems use social media would not be a research ethics problem if researchers were always sensitive to ethical issues. But there have been two massive scandals involving Facebook's use of social media data for research. Many people have heard of the (mis)use of Facebook data by Cambridge Analytica (Schneble et al. 2018). But long before that scandal broke, an even worse incident occurred that highlights the dangers of big data Internet research to vulnerable groups.

In the Emotional Contagion study, which was conducted in 2014, almost 700,000 Facebook users were subjected to an experiment without their consent. The study investigated the effects of changing the proportion of positive and negative stories appearing on their News Feeds (the main channel for seeing what one's Facebook friends have been doing). Some friends' positive stories were removed from the feeds of half of the Facebook users included in the study; some negative stories were removed from the feeds of the other half of the users included. This censoring might seem relatively unimportant, but it means that hundreds of thousands of people experienced either more positive or less positive News Feeds for a week. And the behaviour of those in the different groups changed: users who saw more positive stories were more likely to post positive stories themselves. The opposite was true of those who saw more negative stories. This suggests that the emotions of participants were affected by their participation—participation that they did not consent to and did not even know about.

What are the implications of the Emotional Contagion experiment for vulnerable groups? Besides the presence of children on Facebook, including those too young to legitimately access the service, many Facebook users can be assumed to suffer from depression or other mental health issues. This means that the researchers conducting the Emotional Contagion experiment not only included non-consenting adults but also non-consenting children and people suffering from depression and manipulated their emotions. The effects of this are unknown, but given that the study did seem to make some people feel better and others feel worse, it is highly likely that young children had their mood altered negatively by this study; the same goes for depressed people. Some of those included may have been both children and depressed.

This might seem like arbitrary speculation, but we can make these concerns more concrete by working out how many people in each of these vulnerable groups were probably included in the study, as I did in an article analysing the experiment (Shaw 2016). Extrapolating Facebook user statistics as well as research suggesting that at least 5% of people are suffering from depression at any given time, I calculated that "15% or more than 100,000 participants were children" and "at least 30,000 people with depression were included in the study" (Shaw 2016). If we apply the same numbers to the Cambridge Analytica scandal, in which the data of 87 million people were used inappropriately, 13 million children and over 4 million people with depression may have had their data used without consent.

How did the contagion study ever get approved? In fact, it was never approved by a REC or IRB. Social media research is often unregulated by RECs or IRBs because it is conducted by researchers at institutions where no committee exists that reviews such research or because they work not at universities but at social media companies or private companies such as Cambridge Analytica; this applies not only to social media research but to a great deal of IMR (Schneble et al. 2018). This fact further compounds the dangers posed to vulnerable groups by big data research. Not only can researchers involve participants, including vulnerable participants, without informing them of a specific project or obtaining their consent but also ethical oversight is missing in action at the very point where an ethics committee or IRB is most needed. In fact, an IRB did have the opportunity to review this study as one of the researchers was affiliated with Cornell University. But the university's IRB decided that "he was not engaged directly in human research" because he "had access only to results—and not to any individual, identifiable data at any time" and Facebook had conducted the study independently (Cornell University 2014). This conclusion is questionable at best, given that he was the lead researcher on a project that manipulated people's emotions. Furthermore, it is wrong to assume that this research only concerned American citizens, as Cornell seems to have done. Emotional Contagion was an international study as any Facebook users with English as their chosen language were eligible for inclusion. Therefore, any REC reviewing the study should at least have considered whether ethics review in countries such as Canada, the UK and Australia might be necessary (even then, English speakers in any country could have been included).

It emerged after the scandal surrounding the Emotional Contagion study that Facebook's terms and conditions did not mention the possibility of user data being employed for research. In the years since, Facebook has made the role of research clearer in its terms and conditions, stating that "We engage in research to develop, test, and improve our products." This is still a very broad statement, even assuming that users bother to read it. While we can hope that researchers would not make the same mistakes again, history suggests that such scandals tend to recur.

Conclusion

The fact that big data research is often conducted using the Internet and social media can make it seem like a safer way of doing research. There are no physical interventions, and thus no risk of direct physical harm. But in fact, the removal of the necessity for physical proximity between researchers and research participants vastly increases the potential for unethical research to be conducted, particularly when combined with a relative lack of ethical oversight. These risk factors are multiplied even further when we consider the lack of protections for vulnerable groups in online spaces. Any researchers using the Internet or big data must remain extremely vigilant to the possibility that the people whose data they are using for the research might belong to vulnerable groups, particularly when the nature of the study means that participants' identities are unknown or unclear. Just because research using social media can be done easily doesn't mean that it should be done. Similarly, users of social media and the Internet would do well to remember that just because they can participate in research and share their data on social media doesn't mean that they should.

Zusammenfassung:
Dieser Kommentar befasst sich mit der Frage des (mangelnden) Schutzes für vulnerable Gruppen in der Big-Data-Forschung. Obwohl das Risiko körperlicher Schäden bei dieser Art von Forschung geringer ist, wirft die Distanz zwischen Forschenden und Teilnehmenden neue Fragen auf, wie der Fall einer Studie mit Facebook-Nutzenden zeigt, von denen einige Kinder waren oder an Depressionen litten.

Empfehlungen:
Forschende, die Big Data nutzen, sollten sich der Möglichkeit bewusst sein, dass die Teilnehmenden zu einer vulnerablen Gruppe gehören könnten. Nutzende sozialer Medien wiederum sollten die Allgemeinen Geschäftsbedingungen genau lesen und sich bewusst sein, dass ihre Daten für Forschungszwecke verwendet werden können.

Résumé

Ce commentaire aborde la question de la protection (insuffisante) des groupes vulnérables dans les recherches en big data. Bien que le risque de préjudice physique soit réduit avec ce type de recherches, la distance entre les chercheurs et les participants soulève de nouvelles questions, comme l'illustre le cas d'une étude menée sur les utilisateurs de Facebook, dont certains étaient des enfants ou des personnes souffrant de dépression.

Recommandations:

Les chercheurs qui utilisent Internet pour mener des études doivent être attentifs à la possibilité que les participants appartiennent à un groupe vulnérable. De leur côté, les utilisateurs de médias sociaux doivent lire attentivement les conditions générales et être conscients que leurs données peuvent être utilisées à des fins de recherche.

References

Cornell University Media Relations Office. 2014. *Media statement on Cornell University's role in Facebook "emotional contagion" research*.

Ofcom. 28 April 2021. *Children and parents: Media use and attitudes report 2020/21*. → https://www.ofcom.org.uk/__data/assets/pdf_file/0025/217825/children-and-parents-media-use-and-attitudes-report-2020-21.pdf.

Schneble, C.O., B.S. Elger, and D.M. Shaw. 2018. **The Cambridge Analytica affair and Internet-mediated research**. *EMBO* Reports 19 (8):e46579. doi:10.15252/embr.201846579.

Schneble, C.O., M. Favaretto, Elger B.S., and D. Shaw. 2021. **Social media terms and conditions and informed consent from children: Ethical analysis.** *JMIR Pediatrics and Parenting* 4 (2):e22281.

Shaw, D.M. 2016 **Facebook's flawed emotion experiment: Antisocial research on social network users.** *Research Ethics*, 12 (1): 29-34. doi:10.1177/1747016115579535.

Big data from the perspective of business ethics

Christian Hauser

Christian Hauser is a Professor of Business Economics and International Management at the University of Applied Sciences of the Grisons and a visiting scholar at the Digital Society Initiative of the University of Zurich. He is co-chair of the Ethics and Compliance Switzerland (ECS) Working Group on Whistleblowing, a member of the topical platform Ethics of the Swiss Academy of Engineering Sciences (SATW), and head of the first PRME Business Integrity Action Center in Europe. PRME is the academic branch of the United Nations Global Compact (UNGC). His research interests include international entrepreneurship, SME & private sector development, corporate responsibility, business integrity, and data ethics.

Big data has been likened to a currency of the future (Eggers et al. 2013). Digitalisation has allowed not only for the mass creation, storage, and analysis of large amounts of heterogeneous data but also the commoditisation of this data. The use of digital technologies generates data on processes and areas of life that were not observable in the pre-digital age—for example, one can compare rummaging in a brick-and-mortar bookstore with searching for books on Amazon, where each online movement and click leaves a digital data trail. In general, every interaction with digital technologies creates a digital trace, and those traces can be combined to paint an intimate picture of everyday lives, habits, and interests. This is because digitalisation not only makes it easier to collect and store data but also because it has become increasingly inexpensive and convenient to analyse huge data sets, especially with the help of powerful (self-)learning algorithms. Thus, data on production and consumption processes have become commercially exploitable in a way that was almost unthinkable just a few years ago (Christen et al. 2019a).

Such drastic changes arouse both hopes and fears. Some emphasise the huge economic potential of big data, calling it the "oil of the 21st century," that is, an enormous resource for innovation, progress, and wealth creation. Others consider big data to be a fundamental threat to freedom and privacy—a demonic instrument of an Orwellian surveillance regime (Helbing 2015). Neither position is nuanced enough, but they reflect the tensions surrounding the ethical, legal, and social issues (ELSI) of big data. Several aspects of this ongoing discussion have already been covered in detail in this white paper. These include the ethical challenges of using big data applications in certain sectors, namely healthcare (see Ienca's and Elger's main articles); values threatened by big data, such as privacy, autonomy, and transparency (see Christen's main article); and fairness and non-discrimination in big data use (see Loi's main article). In this commentary, I will expand on these issues. For this purpose, the topic of big data will be addressed from the perspective of business ethics. Recommendations for action, based on some concrete use cases, will be formulated for private sector companies that use or want to use big data technology.

With data increasingly available, private companies are seeking ways to harness it for commercial purposes. Use cases for the commercial exploitation of big data applications include, but are not limited to, (1) avoiding payment defaults, (2) improving risk management, (3) tailoring offer conditions, (4) enhancing the efficiency of advertising campaigns, and (5) creating innovations and opening up new revenue streams (Hauser et al. 2017).

First, to forecast the likelihood that a customer will pay on time and not default, companies have traditionally relied on the credit ratings of their customers. Big data-based scoring models are being used more and more frequently for this purpose. Algorithms analyse a plethora of (often unrelated) data points such as behaviour and interactions on social media platforms, browsing behaviour on search engines and websites, and the technical specifications of devices that are used to access the Internet (e.g., desktop computer, laptop, tablet, or smartphone) to determine a score. In online shopping, this score can be used to determine whether a particular customer can pay by invoice or must prepay. In banking transactions, the score can influence the terms on which a loan is granted.

Second, the business models of some companies (e.g., those in the insurance industry) are reliant on successful risk management (Christen et al. 2019b). Big data allows for a more accurate, case-by-case assessment of risks such as the probability and degree of damage. For example, telematic solutions used by the car insurance industry collect information on how a policyholder drives to calculate the likelihood of a collision. Policyholders of health insurance companies grant their insurers access to fitness data collected by wearables and smartphones. These data can be used by insurance companies to predict their clients' health risks more accurately and offer tailored insurance products.

Third, dynamic pricing is a standard practice in several industries, used, for example, by airlines, e-merchants, and gas stations. Such industry players dynamically change prices based on data points such as demand, availability, time of day, and the behaviour of competitors. Big data allows companies to go beyond these traditional approaches and to predict the "ideal price" of a good or service for each customer by using both personal and technical data on each individual. For example, an online tour operator displayed higher prices to Apple users, because they tended to be less price-sensitive when booking (Mattioli 2012).

Fourth, advertising is effective when it reaches customers who are interested in a given product, but traditional advertising campaigns tend to use the "shotgun approach" (e.g., billboard advertising). Campaign accuracy can be improved with the help of big data analysis. In e-commerce, it is common practice to show adverts to (potential) customers based on their search or purchase history as well as their geographic location and other variables. With the advent of digital billboards, individualised ads that were previously confined to personal devices can in principle also be displayed on billboards to target people in the vicinity. Additionally, the advertising chosen can be tailored to the emotional state of the customer by an artificial intelligence-based application that analyses visual and auditory information.

Finally, companies can use big data to generate innovation. For instance, data analysis can identify emerging trends and prompt the development of new products (e.g., in manufacturing or streaming services). Similarly, data from voice recognition software can be utilised to improve voice-control technology or related services such as translation. Big data also enables advances in infrastructure and mobility planning that can help to minimise traffic congestion, for example. Moreover, thanks to big data, new business models are emerging, and companies can tap into new sources of revenue. For instance, companies can make their data available to other businesses and thus complement their product portfolio.

These use cases show the wide range of big data applications in the private sector and illustrate how big data is transforming the way that companies from different industries do business. These applications may produce added value for companies and their customers but also entail significant ethical risks. The ethical discourse has identified eight values that are affected by big data applications: (1) privacy protection, (2) equality and non-discrimination, (3) informational self-determination, (4) control of one's (digital) identity, (5) transparency, (6) solidarity, (7) contextual integrity, and (8) property and copyright (Hauser et al. 2017). Each of the use cases described above touches on these eight values to some extent. Companies are advised to manage these risks carefully as customers and other stakeholders are likely to be critical of the violation of these values. Additionally, companies must demonstrate responsible data handling in their big data applications to obtain or retain their license to operate. Therefore, they should consider the following points when dealing with big data.

Take the "ethics case" into account

When evaluating (novel) big data applications, companies should not only focus on the technical feasibility and business case of the application but also its ethical implications; they should embed ethical considerations into the design process from the beginning. By systematically including the ethics case in the development process, companies can understand where potential violations of ethical values and conflicts may arise and resolve them proactively. Looking at the use cases described above, the following ethical deliberations might be considered.

To ensure privacy, data should only be collected for a specific purpose, in accordance with the principle of purpose limitation. Furthermore, according to the principles of data avoidance and data economy, only data relevant for achieving this purpose and not exceeding it should be collected. Big data applications often collide with these principles, as it is precisely through the combination of data sets from different sources that new insights can be gained. This exposes the risk that personal data are being used beyond the scope of their intended purpose, thereby violating the privacy of consumers, which can lead to a loss of legitimacy for a company.

The merger of datasets from multiple sources raises further questions around the control of the individual's digital identity and right to self-determination of personal data. The phenomenon of digital identities arises from the ability of big data applications to aggregate and analyse multidimensional data. Problems arise when an individual is unaware that his/her data are being used in this way or has no means to change the categories within which his/her digital identity has been placed. Further, an individual's identity is fluid over time. His/her preferences and interests change, rendering much personal data time and context dependent. Individuals also create silos for their online presence (e.g., a profile created on a professional networking platform versus a profile on a dating app). If this data is merged, the blurring of the boundaries between the different contexts may lead to inaccurate digital identities. In addition, these digital profiles open up the possibility for the violation of informational self-determination. For instance, data might be used for targeted advertising that aims to manipulate the individual (e.g., emotional advertising).

Making advertising more effective might constitute a legitimate business reason to analyse large data sets on customers. In this case, the benefits for the customers (e.g., seeing ads with relevant information) must be balanced against the drawbacks (e.g., digital "surveillance" by the company). From an ethical perspective, an intrusion into the customer's privacy seems justified, if he/she is informed of the magnitude of data collection, has consented to it, and has a realistic alternative to consenting. However, it is problematic if customers who insist on their right to informational self-determination are denied access to certain services because they refuse access to personal data or if they are charged substantially more, resulting in de-facto discrimination.

A further challenge relating to big data analysis is the potential violation of the solidarity principle that often guides the insurance industry. When aggregating data for risk management purposes, the principle of solidarity is open to violation if there is the possibility of extending the cost-by-cause principle. If a given risk (e.g., of lung cancer) can be attributed to a behaviour that is chosen freely (e.g., smoking), then the decision to engage in the risky behaviour may become a reason for denying solidarity. Companies could even require certain (positive) behaviours from individuals to mitigate risks. This form of influence might seem economically attractive (e.g., for insurance companies who wish to reduce risks). However, it is in direct conflict with the right to self-determination and free will (Loi et al. 2021).

These deliberations show that it is of central importance for companies to consider the ethics case at an early stage in the development of big data applications. This by no means leads in general to the inhibition of big data applications. Rather, it makes it possible to develop more sustainable big data applications that would have a long-term "license to operate" from the stakeholders. Such an approach is therefore recommendable from an economic perspective.

Consider the customer's point of view

A simple test criterion for assessing the "license to operate" of a big data application is the following: Would the customer consent to sharing his/her data if he/she knew what would be done with the data? If full transparency is treated as a standard baseline for development, companies must consider whether customers would be comfortable with the product or service that is to be developed utilising their data. This highlights the importance of maintaining transparency and clarity on the collection and use of personal data. Depending on the service in question, opt-in data solutions and the provision of acceptable alternatives may be attractive strategies.

This raises the question of the actual level of knowledge of the customers with respect to big data. The statements about a company's analysis and usage of an individual's data are often enshrouded in lengthy terms and conditions and legal jargon, not typically understandable by the average person. The algorithms used for big data analysis are usually proprietary to a company, meaning that the data used by the algorithms cannot be validated for quality, trustworthiness, or completeness. As a result, tensions emerge between a company's rights to preserve its algorithms (i.e., the intellectual property connected with them) and customers' rights to transparency.

Another consideration is what benefits customers would consider adequate in exchange for their data. Each interaction with online services creates a digital trace that generates and/or discloses some form of personal data. Typically, companies use the personal data collected from or about their customers for business purposes, with this data additionally serving as a basis for new revenue sources. This raises the question of the ownership and value of the data. Are the data generated through digital interactions considered creations in the sense of copyright law, or is this only the case when the data are analysed? The answers to these questions determine the attractiveness of the business case for the use of data. For example, it could be required to share revenues earned from data use with the customer. Anticipating the consumer reaction to the specific use of data can help avoid potential violations of property and ownership expectations.

Create transparency and freedom to choose

Big data applications cannot be widely and successfully implemented unless they are trusted and accepted by consumers and other stakeholders. This requires that companies provide transparent and comprehensible information about how they collect and use data.

With this in mind, the development of a big data application must involve a conscious, case-by-case ethical evaluation, considering whether there is a (potential) infringement of ethical values and, if so, whether the infringement can be justified. Whilst this may become burdensome for single (small and medium-sized) companies, it is recommended that collaborations for ethical evaluation be fostered and industry standards created to support this process (see, e.g., Christen et al. 2019b, 2020). At a meta level, it would be advisable to work towards standardisation in the terms and conditions relating to the collection, analysis, and use of big data, not only to guide company business practices but also to foster customers' capacity to provide informed consent. The goal should be to empower customers as well as society to better comprehend the scope and scale of data collection, analysis, and usage in the age of big data.

Acknowledgement:

This commentary is based on earlier works by the author and his colleagues. Language assistance by Eleanor Jehan is gratefully acknowledged.

Zusammenfassung:
Da dank Big Data immer mehr Daten zur Verfügung stehen und analysiert werden können, suchen private Unternehmen nach Möglichkeiten, diese für kommerzielle Zwecke zu nutzen. Diese Entwicklung weckt sowohl Hoffnungen als auch Befürchtungen. In diesem Kommentar wird das Thema aus wirtschaftsethischer Sicht beleuchtet. Anhand von Anwendungsfällen werden Handlungsempfehlungen für Unternehmen formuliert, die Big Data nutzen oder nutzen wollen.

Empfehlungen:
Big-Data-Anwendungen können nur dann erfolgreich umgesetzt werden, wenn sie in weiten Teilen der Gesellschaft auf Vertrauen und Akzeptanz stossen. Die Politik sollte den Rahmen vorgeben, unter dem Daten gesammelt, analysiert und genutzt werden können. Sie sollten nicht nur auf die Schaffung von (selbstregulierenden) Standards drängen, welche die Interessen von Unternehmen und Verbrauchern ausgleichen, sondern auch die Kunden in die Lage versetzen, fundierte Entscheidungen zu treffen.

Résumé
Les données étant de plus en plus disponibles et aptes à être analysées grâce à la technologie big data, les entreprises privées cherchent des moyens de les exploiter à des fins commerciales. Cette évolution suscite à la fois espoirs et inquiétudes. Dans ce commentaire, le sujet est abordé sous l'angle de l'éthique des affaires. Sur la base de cas pratiques, des recommandations d'action sont formulées à l'intention des entreprises qui utilisent le big data ou souhaitent le faire.

Recommandations:
Les applications big data ne peuvent être mises en œuvre avec succès que si elles bénéficient de la confiance et de l'acceptation d'une large partie de la société. Les décideurs politiques doivent définir le cadre dans lequel les données peuvent être collectées, analysées et utilisées. Ils doivent non seulement insister sur la création de normes (d'autorégulation) conciliant les intérêts des entreprises et des consommateurs, mais aussi donner à ces derniers les moyens de décider en connaissance de cause.

References

Christen, M., H. Blumer, C. Hauser, and M. Huppenbauer. 2019a. **The ethics of big data applications in the consumer sector.** In M. Braschler, T. Stadelmann, & K. Stockinger (eds.), *Applied Data Science: Lessons learned for the data-driven business* : 161–180. Cham, Switzerland: Springer.

Christen, M., F. Thouvenin, C. Hauser, et al. 2019b. *Big Data Ethics Recommendations for the Insurance Industry*. Zürich: NFP 75.

Christen, M., C. Heitz, T. Kleiber, and M. Loi. 2020. *Code of Ethics for Data-Based Value Creation*. Thun: Swiss Alliance for Data-Intensive Services.

Eggers, W., R. Hamill, and A. Ali. 2013. *Data as the new currency*. *Deloitte Insights*.

Hauser, C., H. Blumer, M. Christen, L. Hilty, M. Huppenbauer, and T. Kaiser. 2017. *Ethische Herausforderungen für Unternehmen im Umgang mit Big Data*. Zürich: SATW.

Helbing, D. 2015. *Thinking ahead-essays on big data, digital revolution, and participatory market society*. Cham: Springer.

Loi, M., C. Hauser, and M. Christen. 2021. **Highway to (digital) surveillance: When are clients coerced to share their data with insurers?**. *Journal of Business Ethics,* 175, 7–19. doi:10.1007/s10551-020-04668-1.

Mattioli D. 2012. On Orbitz, **Mac Users Steered to Pricier Hotels**. *Macaholics UNANIMOUS*: 20 (8)