UNIVERSITY OF PÉCS

Faculty of Law

Ph.D. Thesis

Big Data and Artificial Intelligence:
An examination of the existing legal framework from a privacy perspective

Author: Branka Mania

Supervisor: Gergely László Szőke

Version for preliminary debate submitted: January 2022

Table of contents

Abbreviations / Glossary

ACM	Association for Computing Machinery
AHEG	UNESCO’s Ad Hoc Expert Group
AI	Artificial Intelligence
ALKS	Automated Lane Keeping Systems
ANN	Artificial Neural Network
A/IS	Artificial Intelligence and autonomous systems
Art29WP	Article 29 Working Party
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für Datenschutz und Informationsfreiheit
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
CCTV	Closed Circuit Television
CalOPPA	California Online Privacy Protection Act
CCPA	California Consumer Privacy Act
CEPEJ	European Ethical Charter on the Use of AI in Judicial Systems
CETA	Comprehensive Economic and Trade Agreement
Charter	Charter of Fundamental Rights of the European Union
CDEI	Centre for Data Ethics and Innovation
CIPL	Centre for Information Policy Leadership
CJEU	Court of Justice of the European Union (before European Court of Justice)
CNIL	Commission Nationale de l'Informatique et des Libertés
COE	Council of Europe
Commission	European Commission
Convention	European Convention on Human Rights
COPPA	Children's Online Privacy Protection Act
Council	Council of Europe
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership

CRM	Customer Relations Management
DAAS	Data acquisition and archiving systems
DaPriM	Data Privacy Management project
DGA	Data Governance Act
Directive	Data Protection Directive
DMA	Digital Markets Act
DPA	Data Protection Agreement
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSA	Digital Services Act
DSK	Datenschutzkonferenz
DSRI	Deutsche Stiftung für Recht und Informatik
EAD	Ethically Aligned Design
EEA	European Economic Area
ECHR	European Convention on Human Rights
ECPAIS	IEEE’s Ethics Certification Program for Autonomous and Intelligent Systems
ECtHR	European Court of Human Rights
EDRi	European Digital Rights Association
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EFF	Electronic Frontier Foundation
EFTA	European Free Trade Association
e. g.	For example
ENISA	European Union Agency for Network and Information Security
EP	European Parliament
EU	European Union
FAT/ML	Fairness, Accountability, and Transparency in Machine Learning
FCRA	Fair Credit Reporting Act

FIPP	Fair Information Practice Principles
FRA	European Union Agency for Fundamental Rights
FTC	Federal Trade Commission
GAN	Generative Adverserial Networks
GAPPs	Generally Accepted Privacy Principles
GATS	World Trade Organization’s General Agreement on Trade and Services
GDD	Gesellschaft für Datenschutz und Datensicherheit e.V.
GLBA	Gramm-Leach-Bliley Act
GPAI	Global Partnership on AI
GDPR	General Data Protection Regulation
GPEN	Global Privacy Enforcement Network
HIPAA	Health Insurance Portability and Accountability Act
HLEG	High-Level Expert Group on Artificial Intelligence
IAF	Information Accountability Foundation
IAPP	International Association of Privacy Professionals
ICCPR	International Covenant on Civil and Political Rights
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICO	Information Commissioner’s Office
ICT	Information and communications technology
IDFA	ID for advertisers
i. e.	That is to say
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISMS	Information Security Management Systems
ISO	International Standards Organization
ISP	Internet Service Provider
ITU	International Telecommunication Union

IWGDPT	International Working Group on Data Protection in Telecommunications
LAWS	Regulations with regards to the use of lethal autonomous weapons systems
LIBE	EP’s Committee on Civil Liberties, Justice and Home Affairs
Lit.	Littera
MiFiD	Markets in Financial Instruments Directive
ML	Machine Learning
NGO	Non-governmental Organization
NLP	Natural Language Processing
NISD	Network and Information Security Directive
NIST	National Institute of Standards and Commerce
NITI	National Institution for Transforming India
OECD	Organization for Economic Development
ONE AI	OECD’s Network of Experts on AI
OWASP	Open Web Application Security Project
PAI	Partnership on AI
PECD	Privacy and E-communications Directive
PET	Privacy Enhancing Technologies
PII	Personally Identifiable Information
PIMS	Privacy Information Management System
PIN	Personal Identification Number
PSD2	Payment Services Directive
PSI	Public Sector Information
Recital	GDPR Recitals
Regulation	General Data Protection Regulation
R&D	Research and Development
SA	Supervisory Authority
SCAI	Partnership on AI’s Safety-Critical AI Working Group
SCC	Standard Contractual Clauses

SDG	Sustainable Development Goals
TCPA	Telephone Consumer Protection Act
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UGAI	Universal Guidelines for Artificial Intelligence
UK	United Kingdom
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNI	UNI Global Union
U.S.A.	United States of America

A. Introduction, hypotheses, and methodology

I. Introduction

The question behind this Thesis is how Big Data and data protection relate to each other in the sense of if, and to which extent, current data protection laws address risks of Big Data applications. To examine this issue, it first must be clarified what lies behind the buzzword Big Data, and what exactly is protected by data protection laws, especially because new technology may involve new risks, and because data processing nowadays in many cases is rarely limited to national borders or a single service provider. To complete the picture about this matter, the Thesis examines how the existing legal framework captures Big Data and potential risks involved in its applications.

In fact, Big Data involves algorithmic data processing as well as automated decision-making systems which can operate with little human intervention: from a business perspective, the use of algorithmic systems is very attractive as it leads to time and cost efficiency and allows for better analytics and forecasting as well as real-time insights. However, from an individual`s perspective, the use of Big Data, automated decision-making that results in so-called Artificial Intelligence may lead to serious consequences: the challenge already starts with errors that may occur during the design of algorithms, owing to underlying datasets being incorrect or due to wrong interpretation of outcomes which may lead to undesirable results.

The problem from a data protection perspective are effects like data aggregation and maximization, unpredictable as well as secondary (indefinite) use of personal information and the fact that complex data processing operations which are performed by self-learning machines and solely based on data-driven predictive models may not be transparent and explainable anymore. Any such processing is thus potentially opaque and may lack human oversight and control, meaning that basic data protection principles like accountability or transparency, lawfulness and fairness may be affected. Ditto for individual`s rights, because privacy self-management seems hard to achieve when there is information mismatch between data subjects and operators. In addition, the use of algorithmic technology is also criticized for having the potential for (secret) profiling and scoring or even surveillance and discrimination, which shows that there are various implications that go with the use of algorithmic technology.

This in turn leads to the question whether the current legal framework for data protection offers sufficient protections for the individuals behind data protection laws. To answer this question, the following has been examined: what is Big Data; what is Artificial Intelligence; what are the relevant legal (GDPR) definitions; what is the scope of applicable laws; what do data protection and data privacy protect; what is the current (international, EU, national, sectoral) data protection framework;

which other relevant sources of law such as product, liability, data-specific rules exist; which risks come with the use of Big Data, automated decision-making or profiling and the use of algorithms and Artificial Intelligence; do existing regulatory conditions and legal concepts capture these risks; which legislative, regulatory or non-governmental proposals and expert guidelines have been suggested for a future-proof AI regulation; which conclusions can be drawn.

The problem from an individuals' perspective is the so-called "*black-box effect*", the fact that complex data processing operations which are performed by self-learning machines which are solely based on data-driven predictive models may not be transparent and comprehensible anymore. Any such processing is thus imminently opaque and may lack human oversight, and since it is applied in real life, significant risks for individuals may arise: such processing may lead to secondary and unpredictable use of personal information, (secret) scoring and profiling, and it may moreover have the potential for discrimination and bias or even surveillance. These effects can thus pose serious threat to individuals' (online) identity and chances in life.

Transparency is a well-known concept, but this is not necessarily the same as explicability or replicability of individual decisions. It moreover does not guarantee to make "*true operators*" known, which would be important as many processors could be involved in the decision-making, but perhaps not the ones the front-end user of (online) applications get to see. Consent is another well-established concept in privacy, but how can consent work given the information mismatch between controller and individual, and how can privacy self-management work when in fact the privacy paradox, the inconsistency between peoples' concerns regarding privacy and their actual behavior when it comes to exercising their rights and choices every so often tells a different story. The principle of accountability is also a common thread running through data protection regulations, but the question is whether this goes far enough to ensure controller responsibility and liability as well as fairness, accuracy, validity, reliability, contestability and quality of results together with appropriate risk assessment which is accompanied human control, and intervention if need be. The examples of consent, transparency and accountability show that the viability of traditional data protection concepts may have become questionable. Consequently, an analysis is needed as to whether the existing legal framework that applies to the algorithmic, probabilistic, autonomous, real-time, etc. processing and decision-making that is based on personal, user, behavior, sensor, etc. information needs adjustment. In this context, this paper examines the afore-mentioned three pillars of data protection and provides for the following three main hypotheses:

II. Hypotheses

First, privacy self-management as a rights-based concept failed for a variety of reasons, starting with the fact that privacy self-management in many instances is only about a take-it-or-leave-it-approach, and deteriorated into a mere click-mechanism. Privacy self-management requires valid consent, but that is difficult to imagine given the existing information asymmetries and transparency obligations being restricted. In addition, the exercise of data subject rights neither leads to the desired protections not can it, depending on the circumstances, prevent admissible secondary use of personal information.

Second, the transparency principle needs to be further developed, moving away from an ad hoc or one-time or notice-level format information into the direction of meaningful information on underlying algorithms for all concerned data subjects, including labeling and open registries allowing the public to access relevant information such as details on risk evaluations, mitigation measures and information on sub-processors. This may increase the chances for the needed social debate for this important technology that has the potential to shape our lives, and it could also allow to better exercise individual's rights and foster individual engagement, which is a factor that should not be underestimated as a single person's commitment has brought down an entire international data transfer mechanism. The success of such initiatives can be compared to the functioning of the fourth pillar of the state which, in addition to the executive, legislative and judicial branches, can influence developments through reporting and public discussion.

Third, new controls and constraints are needed on top of documentation, self-evaluation, vendor management or consultation with internal or external counsels. This should include further mandatory checks which extend to all relevant controllers and processors, and possible risks should not only be judged from an individual's point of view but consider the societal perspective and include new values: Artificial Intelligence has the potential for mass surveillance, and the more individuals are concerned with the effects, the more this also becomes a societal matter. Digital workforce aspects already show that there is an important intersection between individual and societal issues, and the use of photos, biometric information and facial recognition are probably the best examples for personal issues expanding to societal issues: Some years ago, a single picture of a person would have been considered static personal information, in many cases falling under GDPR's household exemption due to personal data being processed by a natural person in the course of a purely personal or household activity. With today's technology, a single photo can be used to embarrass or blackmail somebody by producing a "*deep fake*", or to mislead the public or to influence voters by "*morphing faces*" within pictures, or to fool security systems by cloning biometric data taken from public events to gain illegitimate access to systems and data.

The case of Clearview AI showed that, what used to be the preserve of law enforcement identification services or subject to judicial review, became a flourishing private-sector business model since anyone may check anybody’s picture online to find out who the person is, where the person lives or works. Given the substantial risks, it is time to treat this technology like any other (potentially) hazardous technology, that is think about comprehensive regulation and risk mitigation, taking into consideration existing privacy, security, product, liability, machinery, consumer, e-commerce, employment, anti-discrimination as well as any other applicable data-, purpose-, or sector specific laws and corresponding legal initiatives around the use of Big Data and AI into consideration.

III. Methodology

Big Data and Artificial Intelligence have the potential to shape our lives, and it is thus worthwhile to examine whether the current legal framework matches and captures the possible risks involved in the use of such technology. Big Data and AI are already part of numerous apps, services, products, and data processing operations, and the question is whether there are gaps in the interpretation or application_of existing regulations, and if there is a need for further rules for the handling of Big Data and Artificial Intelligence and the use of automated decision-making or specific technology based on sensitive information such as biometric data.

For this purpose, this paper first takes a descriptive approach by explaining the history of data privacy and emergence of data protection laws and what they aim to protect. For the purposes of identifying potential discrepancies, the paper examines the main characteristics and explores on potential risks of Big Data and Artificial Intelligence and matches these with existing laws, starting with legal definitions which are relevant for the scope, and with a focus on regulations that include data protection provisions – be it on international, EU, sectoral or national level. In this context, this paper takes a critical, analytical and systematic approach by identifying and categorizing relevant sources of law, starting with the current legal framework up to legislative and regulatory proposals, including initiatives by non-governmental organizations and expert recommendations for the future regulation of Big Data and AI. By presenting and comparing various initiatives for the regulation of Artificial Intelligence, the paper elaborates on the need to further develop relevant legislation and standards for Big Data, Artificial Intelligence and ADM and automated or algorithmic decision-making.

B. History of privacy, development of data protection laws and the emergence of Big Data, Automated Decision Making, and AI

I. Brief history of the right to privacy

It is difficult to say when exactly the first ideas on the right to privacy came up. Some years ago, the Bavarian State Commissioner for Data Protection[1] organized an exhibition called "*From the oath of Hippocrates to Edward Snowden: a short journey through 2500 years of data protection*".[2] This title shows that the origins of data protection – or at least some aspects like patient confidentiality – are much older than one would suggest, and this does not only apply to the medical field: first basic ideas about privacy came up in the late Middle Ages and the early Renaissance: the confessional secret dates back to the fourteenth century and the banking secrecy dates back to the sixteenth century.[3] However, there were times in which, apart from any legal protection, even walls and single beds were regarded as a means of privacy.[4] Already in 1890, two lawyers from the United States, wrote an Article called "*The Right to Privacy*",[5] in which they argued that laws must be adapted to reflect technological change due to the increasing capacity of certain institutions to invade previously inaccessible aspects of personal activity. They defined the protection of the private as the foundation of individual freedom in the modern age and concluded that legal remedies had to be developed to enforce definite boundaries between public and private life.[6] Later on in his career as a judge, one of the authors explained[7] that the right to be let alone as the most comprehensive of rights. Basic concepts of respecting the right to privacy were set-out around 1950, decades before computer usage grew exponentially:

[1] The German state of Bavaria has two data protection authorities, one for the public sector, chaired by state commissioner (see their website at https://www.datenschutz-bayern.de/. Retrieved September 25, 2021), and one for the private sector, chaired by its president (see their website at https://www.lda.bayern.de/de/praesident.html. Retrieved September 25, 2021).

[2] Source: https://www.datenschutz-bayern.de/presse/20140331_Ausstellung.pdf. Retrieved September 25, 2021.

[3] Andreas Schneider: Die Datenschutzgrundverordnung. Presentation held in his role as representative of the Saxon Data Protection Commissioner at the KISA Forum on February 18 2018, available at https://www.kisa.it/de/datei/anzeigen/id/19667,3/datenschutzgrundverordnung.pdf. Retrieved September 25, 2021

[4] Greg Ferenstein: The birth and death of privacy: 3000 years of history told in 46 images. Article published November 25 2015, available at https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e#.8tcuzmf86. Retrieved September 25, 2021.

[5] Samuel Warren, Louis Brandeis: The Right to Privacy, Harvard Law Review, vol. 4, No. 5. 1890, pp. 193-220. Article available at http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C. Retrieved September 25, 2021.

[6] Warren and Brandeis (pp.193-195) explain how the protection of the individual developed: from the protection of property over the protection against noises, odors, dust and smoke to the protection of the individual's intangible property and feelings and finally the protection against "unauthorized circulation of portraits of private persons" and the "evil of the invasion of privacy by newspapers".

[7] Brandeis' dissent in the case Olmstead v. United States, available at https://my.ilstu.edu/~jkshapi/Brandeis_Olmstead%20Dissent.pdf. Retrieved September 25, 2021.

In 1948, the United Nations proclaimed the Universal Declaration of Human Rights in 1948 response to World War II.[8] The Universal Declaration of Human Rights sets out, for the first time, fundamental human rights to be universally protected, and this includes privacy.[9] Only two years later, the European Convention on Human Rights was adopted, and it included the right to respect for private and family life.[10] In addition, the EU enacted the Charter of Fundamental Rights of the European Union[11], and the specialty about this charter is that it explicitly also addresses the protection of personal data.[12] It is remarkable that the respect for private life and the right to data protection emerged much earlier than mass processing of personal data. It is also notable that even in specialist circles,[13] the Universal Declaration of Human Rights, the Charter and the Convention are sometimes better known or maybe even more recognized than the 1981 Council of Europe Data Protection Convention (108+).[14] This is not comprehensible insofar as this convention formulated several basic principles which are still valid today, for example, that personal data shall be processed lawfully, fairly and in a transparent manner and that personal data shall be accurate and kept up to date and collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes.[15] In addition, this convention is the only legally binding multilateral agreement in the field of personal data protection[16] - unlike the 1980 OECD guidelines on the protection of privacy and trans-border data flows of personal data, which are nonetheless a very important[17] contribution to the overall data protection framework. It can therefore be said that, in the time-period between World War II and the early 1980s, important (binding) international statutes have been created.

[8] Source: http://www.un.org/en/universal-declaration-human-rights/index.html. Retrieved September 25, 2021.

[9] UDHR Article 12 stipulates that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks".

[10] Text available at https://www.echr.coe.int/Documents/Convention_ENG.pdf. Retrieved September 25, 2021.

[11] Source: http://www.europarl.europa.eu/charter/pdf/text_en.pdf. Retrieved September 25, 2021.

[12] Article 8 of the Charter postulates that "*everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly, for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority".*

[13] The German consultancy Datenschutz Nord reported on this issue on March 19 2019 blog, available at https://www.datenschutz-notizen.de/die-konvention-nr-108-die-kleine-schwester-der-dsgvo-0222164/. Retrieved September 25, 2021.

[14] Official name: The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Convention text available at https://rm.coe.int/16808ade9d. Retrieved September 25, 2021.

[15] See Article 5 of the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data, available at https://rm.coe.int/16808ade9d. Retrieved September 25, 2021.

[16] Source: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018PC0451. Retrieved September 25, 2021.

[17] A continuous contribution: information on OECD's work on information security and privacy is available at http://www.oecd.org/internet/ieconomy/oecdprivacystatementgenerator.htm. Retrieved September 25, 2021.

II. Development of data protection law

As far as national legislation is concerned, some sources[18] claim that the 1973 Swedish Data Act was the world's first national data protection law. However, the Hessian Data Protection Act was passed in 1970[19] and may therefore be considered the first data protection law in Europe. It can generally be said that the first generation of data protection norms appeared in the 1970s, which is also true for the US as the 1970 Fair Credit Reporting Act[20] contained elements of data protection. Another example is the 1972 amendment of the Californian Constitution[21] which established an enforceable right to privacy including the ability of individuals to control the use and/or sale of their personal information. This first statutory codification wave did not use terms like privacy and was rather concerned about the state sector and public authorities. Well-known concepts such as technical and/or organizational rules for processing were included.[22] Apart from security safeguards, basic concepts such as transparency and principles which govern the collection, use, and dissemination of information about individuals including the right to individual participation were introduced not only in Europe, but also in the US based on the so-called Fair Information Practice Principles (FIPP).[23] Even though there is no comprehensive federal data protection act covering the private sector in the US until today,[24] many FIPP principles have been fully or partially implemented in specific laws,[25] and there are important sector-specific and/or business-model relevant regulations like the 1998 Children's Online Privacy Protection Act[26] (COPPA) and the 1996 Health Insurance Portability and Accountability Act (HIPAA).[27] Already in 1967, the Freedom of Information Act (FOIA) came into effect in the US

[18] Source: https://en.wikipedia.org/wiki/Data_Act_(Sweden). Retrieved September 25, 2021.

[19] Source: https://datenschutz.hessen.de/ueber-uns/geschichte-des-datenschutzes. Retrieved September 25, 2021.

[20] Privacy International: The keys to data protection – a guide for policy engagement on data protection. Article published August 2018, available at https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf. Retrieved September 25, 2021.

[21] The International Association of Privacy Professionals (IAPP) mentions this fact in the framework of their article about the emergence of the 2018 California Consumer Privacy: the article was last updated in February 2021 and is available at https://iapp.org/resources/article/california-consumer-privacy-act-of-2018/. Retrieved September 25, 2021.

[22] Detailed information on the history of data protection is provided by Viktor Mayer-Schönberger: Generational Development of Data Protection in Europe, in: Philip E. Agre, Marc Rotenberg (eds.): Technology and Privacy: The New Landscape, Massachusetts Institute of Technology Press 1998, Cambridge and London, pp. 219-241.

[23] Omer Tene, Jules Polonetsky: Big Data for All – Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property 2013, vol. 11, issue 5, p. 242.

[24] However, businesses have to comply with certain (consumer protection) rules and standards (e.g. unfair or deceptive acts or practices) which are enforced by the Federal Trade Commission, and which quite often have an intersection with data protection law. FTC's work and mandate is explained in greater detail at https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act. Retrieved September 25, 2021.

[25] Serge Gutwirth, Ronald Leenes, Paul de Hert: Data Protection on the Move – Current Developments in ICT and Privacy / Data Protection, Springer Science + Media Publishing Dordrecht, 2016, p. 181.

[26] The full text of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501–6505) is available at http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim. Retrieved September 25, 2021.

[27] Source: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html. Retrieved September 25, 2021.

which provides individuals with the right access documents from state agencies.[28] It is important to note, however, that the greatest difference between the US and the EU approach to data protection is that, under European law, a legal basis is always required for the processing of personal data, whereas in the US, the contrary is true, because data can generally be processed unless a law specifically forbids such an activity.[29] It can therefore be said that, within the EU, the most important data protection rule is that a prohibition (of the collection, of the use) of processing applies which is subject to permission (by law, by individual consent).

Further European countries passed their data protection bills in the late seventies, e.g., France in 1978, Luxembourg in 1979, and other countries like Portugal, Belgium and Spain followed later on in 1991 and 1992.[30] The second generation of data protection laws emphasized data subject rights, and the idea behind that was that the individual may be the best guarantee for successful enforcement of data protection laws.[31] In 1983, the German Federal Constitutional Court issued a fundamental decision regarding the census judgment. Ever since, this decision is considered a milestone of data protection in Germany as it introduced the concept of so-called "*informational self-determination*",[32] a decision which explicitly linked data protection to constitutional rights, and thus an idea which is considered to be one of the characteristics of the third generation of data protection norms.[33] The UK passed its data protection law in 1984, and Italy and Greece waited for the corresponding EU directive, thus avoiding the need to (re-)shape their national laws accordingly.[34] The fourth generation of data protection laws, among other things, abandoned the idea that only automated data processing requires protection[35] and introduced more detailed rules, for example for sensitive data,[36] and sector-specific regulations, for example for credit-reporting agencies.[37]

[28] Source: https://www.foia.gov/about.html. Retrieved September 25, 2021.

[29] Daniel Solove: Introduction – Privacy Self-Management and the Consent Dilemma, Harvard Law Review 2013, vol. 126:1880, p. 1897.

[30] Herbert Burkert: Privacy - Data Protection: A German/European Perspective, 1999 Proceedings of the second symposium Max Planck project group on the law of common goods, Wood Hall, Mass pp. 43-69, available at http://www.coll.mpg.de/sites/www/files/text/burkert.pdf. Retrieved September 25, 2021.

[31] Viktor Mayer-Schönberger: Generational Development of Data Protection in Europe, in: Philip E. Agre – Marc Rotenberg (eds.): Technology and Privacy: The New Landscape, Massachusetts Institute of Technology Press 1998, Cambridge and London, pp. 219-241.

[32] Source: https://openjur.de/u/268440.html. Retrieved September 25, 2021.

[33] Background information on the so-called third generation of data protection laws can be found in: Helmut Bäumler, Albert von Mutius: Datenschutzgesetze der dritten Generation: Texte und Materialien zur Modernisierung des Datenschutzrechts, Luchterhand Verlang Munich 1999.

[34] Herbert Burkert: Privacy - Data Protection: A German/European Perspective, 1999 Proceedings of the second symposium Max Planck project group on the law of common goods, Wood Hall, Mass. 43-69. Available at http://www.coll.mpg.de/sites/www/files/text/burkert.pdf. Retrieved September 25, 2021.

[35] Viktor Mayer-Schönberger, Ernst Brandl, Hans Kristoferitsch: Datenschutzgesetz, Linde Verlag Vienna 3rd edition 2014, p. 6.

[36] For instance, former § 3 (9) of the German Federal Data Protection Law which dealt with "special personal data" such as data about ethnic origin, political belief, health, etc.

[37] For example, former § 28 b of the German Federal Data Protection Law explicitly dealt with scoring; former § 30a of the German Federal Data Protection Law dealt with market and opinion research.

The mid-nineties were the starting point of a new law regime with regards to data protection for the European Union: The Data Protection Directive[38] was created in 1995 and introduced new terms like sensitive personal data and consent. In 2002, the EU adopted a directive on privacy and electronic communication,[39] and in 2009, the EU established an electronic communications regulation[40] in response to the fact that individuals' contact details such as email addresses and mobile numbers became a prime currency in conducting marketing and sales.[41] The EU also brought forward a directive on data retention[42] in 2006, however, this directive was declared invalid by the European Court of Justice in 2014 for violating fundamental rights. In the year 2014, the CJEU delivered another significant ruling:[43] the so-called Google Spain decision was about the possibility to demand that a search engine operator removes certain query results, a decision that was often quoted[44] as the right to be forgotten. Finally, after years of intensive discussions, the General Data Protection Regulation was approved in 2016. The Internet, the growing digitalization, new techniques and (social media) platforms as well as the increasing trans-border nature of data processing made data protection more and more an international topic, which led to an increased interest in the possibility of regulating data protection at an international level.[45] Given the overall dynamics of the topic, the evolution of data protection rules cannot be considered completed.

III. Emergence of Big Data, Automated Decision-Making, and Artificial Intelligence

Big Data and AI both represent the search for knowledge, and they are founded on a variety of disciplines such as logic, mathematics, and statistics: logic is the foundation for understanding

[38] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046. Retrieved September 25, 2021.

[39] Directive 2002/58/EC of the European Parliament and of the Council of July 12 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058. Retrieved September 25, 2021.

[40] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services, available at https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32009L0140. Retrieved September 25, 2021.

[41] International Network of Privacy Professionals: A brief history of data protection: How did it all start? Blog news published June 1 2018, available at https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/. Retrieved September 25, 2021.

[42] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF. Retrieved September 25, 2021.

[43] Source: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=EN. Retrieved September 25, 2021.

[44] Quoted and criticized, see Ignacio Cofone: Google v. Spain: a right to be forgotten? Chicago-Kent Journal of International and Comparative Law, vol. 15, no. 1, 2015, pp. 1-11.

[45] Christopher Kuner: The European Union and the search for an international data protection framework, Groningen Journal of International Law, vol. 2 (2) 2014, pp. 55-71.

parameters, mathematical thinking is critical for the explanation of input and outputs, and statistics allow for interpretation and evaluation through analysis. The evolution of Big Data and AI clearly goes hand in hand with the development of computer science: obviously, the speed of processing and cost efficiency of the needed infrastructure play an important role for the development of Big Data and AI. Notwithstanding quantum leaps in the area of Artificial Intelligence in the last decade, the first concept of machine learning dates back to the eighteenth century when Bayes developed a framework for reasoning about the probability of events known as the Bayesian inference; in the nineteenth century, Boole worked on logical reasoning, and in 1914, the first chess-playing machine that operated without human intervention was invented.[46] The starting point of data processing was probably the year 1889 when the first system which could read holes punched into paper cards was introduced.[47] As regards Big Data applications, the first approaches to modern[48] Big Data analysis[49] are almost one hundred years old: In 1927,[50] the German "*Schutzgemeinschaft für Absatzfinanzierung*"[51] based its decisions on a system for assessing payment behavior.[52] This was the foundation for SCHUFA,[53] Germany's first credit agency which based its decisions on scoring, an important use case for Big Data analytics in the financial sector.[54] The first major data project is created in 1937 and was ordered by the Roosevelt administration in the US, because, after the Social Security Act was enacted, the government had to keep track of data of millions of employees.[55] In 1941, the world's first fully automatic, general-purpose digital computer Z3 became operational; his inventor is nowadays considered a pioneer of computer science,[56] but given the overall circumstances of the 1940s and

[46] Gil Press: A Very Short History Of Artificial Intelligence. Article published December 30 2016, available at https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/. Retrieved September 25, 2021.

[47] The reason for the invention was that the previous US census took years due to manual processes, source: http://www.b-eye-network.com/blogs/vanderlans/archives/2013/02/is_big_data_the.php. Retrieved September 25, 2021.

[48] In contrast to accounting and the like, which was of course practiced for much longer.

[49] Not to be mixed up with the first attempts for statistical data analysis, which date back to the seventeenth century, see https://datafloq.com/read/big-data-history/239 for details. Retrieved September 25, 2021.

[50] In the same year, an Austrian-German engineer developed a means of storing information magnetically on tape, source: https://www.dataversity.net/brief-history-big-data/#. Retrieved September 25, 2021.

[51] The term can be translated as "Protective association for sales financing".

[52] Source: https://www.schufa.de/de/ueber-uns/unternehmen/geschichte-schufa/. Retrieved September 25, 2021.

[53] Foundation of the federal SCHUFA-System in order to cover the whole federal territory and not only the surroundings of big German cities, see: https://www.schufa.de/de/ueber-uns/unternehmen/geschichte-schufa/ for further details. Retrieved September 25, 2021.

[54] Stefanie Eschholz, Jonathan Djabbarpour: Big Data und Scoring in der Finanzbranche, ABIDA dossier published January 2015, available at http://www.abida.de/sites/default/files/06%20Scoring.pdf. Retrieved September 25, 2021.

[55] Background information on the project can be found at https://www.wired.com/2012/06/how-social-security-saved-ibm/?utm_campaign=datafloq&utm_medium=ref&utm_source=datafloq. In this regard, some consider the founder of IBM to be the "grandfather of big data": http://www.b-eye-network.com/blogs/vanderlans/archives/2013/02/is_big_data_the.php. Retrieved September 25, 2021.

[56] The German engineer Konrad Zuse has often been regarded as the inventor of the modern computer: Süddeutsche Zeitung, news entry published September 20 2016, available at https://www.sueddeutsche.de/digital/ausstellung-computer-pionier-konrad-zuse-seiner-zeit-voraus-1.3168630.

World War II, the potential of his work was not recognized and remained largely unnoticed.[57] The 1940s saw several groundbreaking publications in the field of artificial intelligence: McCulloch and Pitts 1943 article "*A Logical Calculus of the Ideas Immanent in Nervous Activity*" that become the inspiration for neural networks, Berkeley's 1949 publication "*Giant Brains Or Machines That Think*" about machines that can handle information with speed and skill similar to what a brain would be if it were made of hardware and wire instead of flesh and nerves,[58] and in 1950, Turing published his famous essay "*Computing Machinery and Intelligence*".[59] However, at that time, Turing did not have the resources needed to translate his vision into action.[60] Not only technological progress, but political and strategic factors were reasons for the further development of computers: during World War II, the UK was intensively working to crack Nazi codes and they developed a machine called Colossus[61] which scanned for patterns in encrypted messages. Shortly after World War II, the National Security Agency was founded in the US, and they were also assigned the task of decrypting messages.[62]

Many consider the 1956 Dartmouth summer research project the birth of the field of Artificial Intelligence where essential ideas behind AI have been investigated, i.e. ways in which machines could be made to simulate aspects of intelligence.[63] Apart from McCarthy, many other scientists researched on the concept of engineering machines to independently execute commands in the 1950s, e.g., Samuel who coined the term "*Machine Learning*"; Rosenblatt who developed an early artificial neural network called "*Perceptron*", or Simon and Newell who worked on one of the first AI programs called the "*Logic Theorist*".[64] Computers of this time reached a point where they could operate independently and collect and process data automatically.[65]

[57] The same is true for other pioneers, see http://ei.cs.vt.edu/~history/VonNeumann.html. Retrieved September 25, 2021.

[58] Gil Press: A Very Short History Of Artificial Intelligence. Article published December 30 2016, available at https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/. Retrieved September 25, 2021.

[59] Alan Turing's famous essay "Computing Machinery and Intelligence" is available at https://www.csee.umbc.edu/courses/471/papers/turing.pdf. Retrieved September 25, 2021.

[60] Stanford University: One Hundred Year Study on Artificial Intelligence (AI100). Report published September 2021, available at https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/AI100Report_MT_10.pdf. Retrieved September 25, 2021.

[61] Gregg Keizer: WWII's Colossus computer cracks codes once again. Article published November 15 2007, available at https://www.computerworld.com/article/2540136/wwii-s-colossus-computer-cracks-codes-once-again.html. Retrieved September 25, 2021.

[62] Keith Foote: A Brief History of Big Data. Article published December 14 2017, available at https://www.dataversity.net/brief-history-big-data/#. Retrieved September 25, 2021.

[63] Stanford University: One Hundred Year Study on Artificial Intelligence (AI100). Report published September 2021, available at https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/AI100Report_MT_10.pdf. Retrieved September 25, 2021.

[64] Gil Press: A Very Short History of Artificial Intelligence. Article published December 30 2016, available at https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/.

[65] Stanford University: One Hundred Year Study on Artificial Intelligence (AI100). Report published 2016, available at https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf. Retrieved September 25, 2021.

In 1961, the first industrial robots[66] have been introduced,[67] and in 1965, Feigenbaum and colleagues engaged in building the first knowledge repository tailored for specialized domains called "*DENDRAL*", which is considered the first expert system since it automated the decision-making process and problem-solving behavior of organic chemists.[68] Also in the mid-1960s „*ELIZA*", an interactive program that was capable of dialogue was developed,[69] and in the following years, further progress was made in the area of Robotics, for example with the development of the famous robots named "*Shakey*"[70] and "*Freddy*".[71] The 1970s were the era of the personal computing revolution: the first personal computers with floppy-drives as key components emerged: in this regard, many think of IBM or Microsoft, but the first personal computers have been introduced by other companies and came as kits, e.g., the MITS Altair 8800 or the IMSAI 8080.[72]

Despite promising ideas and approaches in previous decades, the era of the 1980s showed that there are gaps between theory and practice which resulted in little significant practical successes and lesser interest in terms of research and funding,[73] so that some describe this time as the winter of Artificial Intelligence.[74] However, another novelty paved the path forward: in 1989, the World Wide Web was invented,[75] and the 1990s saw major advancements in all relevant areas of AI, from reasoning and scheduling over data mining and natural language processing to gaming and visual reality, mainly

[66] "Robot" is derived from the word "rabota" which means work in Russian. The term was coined as early as 1929 by Czech writer Karel Capek, source: https://history-computer.com/karel-capek-and-the-robot-complete-history/. Retrieved September 25, 2021.

[67] The first industrial robot called "Unimate" was used in the assembly line at a General Motors plant, source: Robot Hall of Fame, available at http://www.robothalloffame.org/inductees/03inductees/unimate.html. Retrieved September 25, 2021.

[68] Background information on DENDRAL and the work of Feigenbaum, Lederberg, Buchanan and Djerassi can be found at Stanford University's Edward A. Feigenbaum Papers, available at https://exhibits.stanford.edu/feigenbaum/catalog?f%5Bauthor_other_facet%5D%5B%5D=DENDRAL. Retrieved September 25, 2021.

[69] Oliver Miller: A conversation with ELIZA, the electronic therapist. Article published August 1 2012, available at https://thoughtcatalog.com/oliver-miller/2012/08/a-conversation-with-eliza/. Retrieved September 25, 2021.

[70] "Shakey" was equipped with locomotion, perception and problem solving, source: Gil Press: A Very Short History Of Artificial Intelligence. Article published December 30 2016, available at https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/. Retrieved September 25, 2021.

[71] "Freddy" was one of the first general-purpose mobile robots to be able to reason about its own actions. Background information on Freddy are provided by the University of Edinburgh, School of Informatics on their website that deals with Artificial Intelligence at Edinburgh University, which is available at https://www.inf.ed.ac.uk/about/AIhistory.html. Retrieved September 25, 2021.

[72] Daniel Knight: Personal Computer History from 1975 to 1984. Article published June 26 2014, available at https://lowendmac.com/2014/personal-computer-history-the-first-25-years/. Retrieved September 25, 2021.

[73] With the exception of the Japanese government that invested millions in AI in a project aimed at improving artificial intelligence from 1982 to 1990, source: Catherine Gallagher: 25 stunning advances in artificial intelligence. Article published June 23 2019, available at https://stacker.com/stories/3336/25-stunning-advances-artificial-intelligence. Retrieved September 25, 2021.

[74] Daniel Fagella: Will There Be Another Artificial Intelligence Winter? Article published January 2 2019, available at https://emerj.com/ai-executive-guides/will-there-be-another-artificial-intelligence-winter-probably-not/. Retrieved September 25, 2021.

[75] Source: https://webfoundation.org/about/vision/history-of-the-web/. Retrieved September 25, 2021.

because fundamental limits of computer storage yielded to new hardware innovations.[76] As of the mid-90s, a remarkable (exponential) growth of computing performance took place: the top supercomputer in 2000 delivered more performance than the entire top 500 supercomputers combined in 1995.[77] Performance and storage power as well as rate at which data is growing are key factors for Big Data, and this rate does not seem to slow down as more and more individuals[78] as well as devices[79] are interconnected. Owing to these developments, applications of AI become more and more prevalent in the daily lives of humans, and technology advances further: in 2019, the world's first integrated quantum computing system for commercial use[80] was introduced, and researchers nowadays even work on quantum computing with molecules.[81] One of the special things about quantum computing[82] is that, despite the fact that the idea behind quantum computing is not new,[83] we are only now in the position to develop computers which are able to increase computational power far beyond what is achievable by conventional computers. Quantum computers would be able to exponentially speed up the rate of machine learning operations and that is why the further development of quantum computing is followed with great interest.

C. Definitions

I. Definitions of relevant legal terms

Since (changes to) definitions effect the material scope of the regulation as defined in GDPR Article 2, a series of terms has to be examined.[84] The same applies to eventual restrictions which may apply to special categories of data as well as potential limitations that may be applicable to certain methods of data processing, namely automated individual decision-making and profiling. Many of the core

[76] Catherine Gallagher: 25 stunning advances in artificial intelligence. Article published June 23 2019, available at https://stacker.com/stories/3336/25-stunning-advances-artificial-intelligence. Retrieved September 25, 2021.

[77] Source: https://royal.pingdom.com/incredible-growth-supercomputing-performance-1995-2010/. Retrieved September 25, 2021.

[78] A phenomenon arising from social media platforms like Facebook, Instagram and the like.

[79] A concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices: https://www.techopedia.com/definition/28247/internet-of-things-iot. Retrieved September 25, 2021.

[80] Source: https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use. Retrieved September 25, 2021.

[81] Source: https://www.kit.edu/kit/english/pi_2017_162_quantum-computing-with-molecules-for-a-quicker-search-of-unsorted-databases.php. Retrieved September 25, 2021.

[82] Characteristics and differences of quantum computers are summarized in the article: 18 Most Interesting Facts About Quantum Computers, which was published January 3 2022, and is available at https://www.rankred.com/interesting-facts-about-quantum-computers/. Retrieved January 22, 2022.

[83] Theoretical foundations of this technology were already discussed in the mid-70s, e.g., by Roman Ingarden: Quantum Information Theory, Reports on Mathematical Physics 1976, vol. 10, issue 1, pp. 43-72.

[84] As regards the relationship between GDPR's Articles and Recitals, the 2015 "Joint practical guide of the European Parliament, the Council and the Commission for persons involved in the drafting of European Union legislation" makes it clear that Recitals are drafted in such a way that their non-binding character becomes clear. The guide is retrieved from https://publications.europa.eu/en/publication-detail/-/publication/3879747d-7a3c-411b-a3a0-55c14e2ba732. Retrieved September 25, 2021.

definitions under the Data Protection Directive were not changed,[85] whereas GDPR expanded the scope of some terms[86] and added new definitions, for example for profiling. GDPR covers all of the terms explained in the below definitions. However, privacy and artificial intelligence (AI) are not mentioned, but as they are needed to complete the picture of Big Data, this section will also explain what is meant by privacy and how AI and underlying algorithms shall be interpreted.

1. Personal data

The Data Protection Directive defined personal data as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".[87] There was controversial discussion on whether, e.g., IP addresses fall within this definition of personal data.[88] GDPR Article 4 (1) states that, "*for the purposes of this regulation, personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*". GDPR thus contains a broad definition of personal data and makes clear that online identifiers and location data are also considered personal data. As a result, GDPR's material scope is also broader than the scope of the Data Protection Directive.[89] Other laws define personal data differently, e. g. the new California Consumer Privacy Act[90] according to which any information that "*identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household*"[91] is considered personal information. Despite obvious similarities, CCPA's definition of personal information is not identical to GDPR's definition of personal data, and it's a good example that terminology can be the starting point of discussions.

[85] For instance, the terms "controller" and "processor".

[86] Such as personal data and sensitive personal data.

[87] Article 2 (a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[88] See the corresponding judgment on IP-addresses by the European Court of Justice in 2016, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CJ0582&from=EL. Retrieved September 25, 2021.

[89] The same is true for the territorial scope: the Data Protection Directive only applied to European Union member states and non-EU members which are a part of the European Economic Area.

[90] The California Consumer Privacy Act (CCPA) was signed into law on June 28 2018, and went into effect on January 1 2020. Background information including a rulemaking fact sheet are available at https://www.oag.ca.gov/privacy/ccpa#:~:text=CCPA%20was%20signed%20into%20law%20on%20June%2028%2C,sale%20of%20personal%20information%20that%20businesses%20collect%2C%20. Retrieved September 25, 2021.

[91] CCPA, Section 1798.140(o)(1).

2. Anonymous data

Unlike pseudonymization,[92] GDPR does not define anonymization. From a data protection perspective, anonymization of data means processing it with the aim of irreversibly preventing the identification of the individual to whom it relates: data can be considered effectively and sufficiently anonymized if they have been treated in such a manner that the data subject is no longer identifiable.[93] The application of data privacy laws therefore stands and falls with anonymization. Anonymization is moreover valuable from a compliance point of view as it may be considered equal to the deletion of personal data,[94] which is important with regard to data retention and deletion periods. Anonymity is interpreted differently[95] as some refer to so-called computational anonymity, where a data controller (even in collaboration with third parties) would have difficulties to directly or indirectly identify data subjects, while others tend to refer to so-called perfect anonymity where such an endeavor would be impossible. The problem of re-identification is often also described as relative anonymity whose main criterion may be summarized as disproportionality of assignment to a person vs. absolute anonymity whose main criterion may be summarized as the impossibility of assignment to a person.[96] The Data Protection Directive dealt with anonymous data[97] to exclude such data from the scope of data protection legislation, and the same is true for GDPR:[98] Recital 26 (6) is also important for Big Data applications as it makes clear that GDPR "*does not concern the processing of (...) anonymous information (...) for statistical or research purposes*". This exception for statistical purposes is tempting to businesses but must be matched against the (rather absolute) definition of personal data as set forth in GDPR Article 4 (1). Furthermore, anonymization of data is anything but easy to achieve,[99] many data sets shall therefore rather be classified as pseudonymous data, meaning that it is still possible to single out individuals and/or to link records to them:

[92] GDPR Article 4 (5).

[93] Definition provided by the Irish Data Protection Authority, available at https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation. Retrieved September 25, 2021.

[94] The Austrian Data Protection Authority decided correspondingly in their decision in December 2018, which is available at https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html. Retrieved September 25, 2021.

[95] Detailed background information is provided by the Article 29 Working Party in their 2014 opinion (05/2014) on anonymization techniques, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Retrieved September 25, 2021.

[96] An overview on the discussion is provided by Nico Härting: DSGVO – gibt es Regelungen für anonyme Daten? Article published May 3 2016, available at https://www.cr-online.de/blog/2016/05/03/dsgvo-gibt-es-regelungen-fuer-anonyme-daten/. Retrieved September 25, 2021.

[97] Recital 26 of Directive 95/46/EC.

[98] GDPR Recital 26.

[99] Researchers of the Massachusetts Institute of Technology (MIT) published a study in December 2018 explaining that anonymous data can be re-identified. The corresponding press release is available at https://www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized. Retrieved September 25, 2021.

3. Pseudonymous data

GDPR dealt with the existing practice and defines pseudonymization as "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*".[100] As a result, personal data which has been subjected to technological measures to make them pseudonymous shall still be considered personal data as long as information can be attributed[101] to an identifiable person. On the one hand, this definition stresses GDPR's broad scope, which is a fact many may not welcome in view of the implementation effort. On the other hand, there is a variety of advantages for businesses when they process pseudonymous data: pseudonymization is explicitly mentioned[102] as an appropriate technique for data controllers to comply with GDPR's data protection principles; restrictions to data subjects' rights apply;[103] breach notification requirements may be impacted.[104] What is particularly interesting for Big Data applications is that profiling on the basis of pseudonymous data may be possible[105] without data subjects' consent as processing of such data is unlikely to significantly affect individuals, which is one of the admissibility criteria under GDPR Article 22 (1). As a result, it can be assumed that the GDPR shows strong incentives to employ data pseudonymization technologies.

4. Special categories of data

GDPR does not address or define all types of personal data that would generally be considered sensitive or worthy of protection. GDPR covers and defines special categories of data such as genetic,[106] biometric[107] or health[108] data and states that, as a basic rule, sensitive personal data must not be processed.[109] In comparison to the Data Protection Directive, the protection of genetic and biometric data is new. As a result, GDPR has a broader definition of so-called sensitive personal data. Moreover, GDPR Article 22 (4) prohibits automated individual decision-making including profiling if

[100] GDPR Article 4 (5).

[101] ICO (2018) believes that personal data that has been pseudonymised can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual: Overview of the General Data Protection Regulation, available at https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/. Retrieved September 25, 2021.

[102] GDPR Article 25: Pseudonymization is mentioned as an example of an appropriate technical measure in correspondence with the principles of data protection by design and data protection by default.

[103] GDPR Article 11 (2) affects individuals' rights of access, the right to correct and erase data as well as requests for data portability.

[104] GDPR Article 34 (3a) .

[105] Subject to a successful assessment of legitimate interests, GDPR Article 4 (1) lit. f.

[106] GDPR Article 4 (13) and Recital 34.

[107] GDPR Article 4 (14), for instance fingerprints, facial recognition, etc.

[108] GDPR Article 4 (15) and Recital 35.

[109] Unless there is a justification, for example individuals' explicit consent: GDPR Article 9 (2a).

it is based on special categories of personal data referred to in GDPR Article 9 (1), so that numerous categories of data[110] are generally not suitable for this type of data processing. If pseudonymous data is a good example for the possibility to conduct Big Data analyses, sensitive data may serve as an example for restrictions in this area.[111] But there are exceptions to this rule as GDPR Article 22 (4) also says that automated individual decision-making including profiling is admissible if it is based on explicit consent or if it is necessary for reasons of substantial public interest.[112]

5. Processing

GDPR defines processing as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".[113] If even erasure and deletion of personal data is considered as a data processing activity under the GDPR, these related data processing activities in the life cycle of personal information raise the question of the appropriate legal basis, which underlines that GDPR is about finding the right legal basis: just like the Data Protection Directive, GDPR works with prohibitions that are subject to permission, and the processing of special categories of data is a perfect example in this regard. The definition of processing is also very broad and makes it clear that the applicability of GDPR is not limited to so-called automated processing as handwritten records may also fall under GDPR. While any use of computers, smartphones, cameras, scanners or Internet and e-mail can lead to the applicability of the GDPR if personal data are concerned, non-automated processing of personal data is only covered by the scope of application if the data are (or are to be) stored in a filing system as defined in GDPR Article 4 (6).[114]

6. Profiling

The Data Protection Directive did not contain a definition of profiling; the GDPR introduced a new definition of profiling: "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation,*

[110] Racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; data concerning health; data concerning a natural person's sex life or sexual orientation; biometric data for the purpose of uniquely identifying a natural person: GDPR Article 9 (1).

[111] Moreover, large scale processing of sensitive personal data triggers the need to undertake data protection impact assessments, see GDPR Article 35.

[112] In addition, suitable measures to safeguard the data subject's rights and freedoms and legitimate interests must be in place.

[113] GDPR Article 4 (2).

[114] Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

health, personal preferences, interests, reliability, behavior, location or movements".[115] Profiling means massive processing of personal data in order to identify patterns that allow for the automatic categorization of individuals and aims at predictive data mining.[116] Profiling moves away from the use of personal data as we know it, because, instead of collecting personally identifiable data, a digital persona is created which is based on information algorithms created with the help of attributes which are not directly related to individuals.[117] While the probabilistic nature of profiles is desired, their inherent opacity[118] together with their potential for discrimination[119] is considered problematic. An important legal development in this regard is that many countries are coming up with privacy laws of their own[120] and these laws foresee, amongst other things, rules on automated decision making and profiling similar to the ones in the GDPR.[121]

7. Automated decision-making

Even though GDPR combines both topics in the same Article, profiling and automated individual decision-making must be distinguished: Profiling is based on automated processing with the objective to evaluate personal aspects about a natural person, however, only automated decision-making has the ability to make decisions by technological means without human involvement. GDPR stipulates that "*the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*".[122] Automated decision-making presupposes that there is no human intervention[123] at all, so that mere pre-selection processes (decision support systems) do not fall under

[115] GDPR Article 4 (4).

[116] Gloria Gonzalez Fuster, Serge Gutwirth, Eriak Ellyne: Profiling in the European Union – a high-risk practice, Inex Policy Brief No. 10, published June 2010, available at https://www.ceps.eu/system/files/book/2010/06/INEX%20PB10%20Fuster%20et%20al.%20on%20Profiling%20in%20the%20EU%20e-version.pdf. Retrieved September 25, 2021.

[117] Serge Gutwirth, Paul De Hert: Regulating profiling in a democratic constitutional state, in: Profiling the European citizen, Springer 2008, p. 300. The article is also available at http://www.vub.ac.be/LSTS/pub/Dehert/Dehert_365_restricted.pdf. Retrieved September 25, 2021.

[118] Tal Zarsky: The Trouble with algorithmic decisions: An analytic roadmap to examine efficiency and fairness in automated and opaque decision making. Article published October 14 2015, available at https://journals.sagepub.com/doi/abs/10.1177/0162243915605575. Retrieved September 25, 2021.

[119] This problem was reviewed by the Article 29 Working Party in their 2017 guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Retrieved September 25, 2021.

[120] For instancr, Brazil, see Renato Leite Monteiro: GDPR matchup – Brazil's General Data Protection Law. Article published October 4 2018, available at https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/. Retrieved September 25, 2021.

[121] For example, Virginia, see Sarah Rippy: Virginia passes the Consumer Data Protection Act. Article published March 3 2021, available at https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/. Retrieved September 25, 2021.

[122] GDPR Article 22 (1).

[123] To qualify as human intervention, the controller must ensure that the decision is carried out by someone who has the competence to change the decision: Peter Gola: Bundesdatenschutzgesetz 2012, para. 6 a BDSG, note 6.

the rule.[124] The problem is where to draw the line between (generally admissible) pre-selection and (potentially inadmissible) decision-making: the question is which (interim) results[125] can be considered to have the quality of a decision in the sense of the Regulation, i.e. a decision "*which produces legal effects concerning him or her or similarly significantly affects him or her*". There is consensus that this question can only be answered on a case-by-case-basis since all circumstances have to be considered, but there are dissenting opinions[126] as to whether or not marketing activities similarly significantly affect data subjects.[127] Recital 71 names two typical examples of automated individual decision-making: e-recruitment processes and (refusal) of an online credit application, which shows that automated individual decision-making is relevant whenever dynamic (real-time) results are needed.[128]

In addition, there are several exceptions[129] to the above rule that individuals have the right not to be subject to a decision based solely on automated processing, e.g., if such processing is based on data subjects' explicit consent, or if the processing is necessary for entering into or performance of a contract between the data subject and a data controller, or if it is allowed by Union or member state law to which the controller is subject.[130] Each of these exceptions is problematic, for the following reasons: consent seems problematic due to factors like lack of transparency and/or information asymmetries and imbalance of powers. As regards the necessity of processing for entering into or performance of a contract between the data subject and a data controller, the problem is that the exception actually applies to scenario which recital 71 considers a typical use case of the norm, namely credit applications.[131] The permissibility of national rules[132] dilutes GDPR's overall goal to harmonize the legal framework, it increases legal uncertainties caused by the necessary interpretation

[124] Stephan Dreyer, Wolfgang Schulz: Was bringt die Datenschutzgrundverordnung für automatisierte Entscheidungssysteme? Bertelsmann Stiftung Publishing 2018, p. 19.

[125] Any such decision must be the result of automated processing: Spiros Simitis: Bundesdatenschutzgesetz 2006, para. 6 a BDSG, note 26.

[126] Some believe that the economic and practical significance of the decision play a role as well as the sustainability of the impairment, whereas annoying or uncomfortable consequences of an automated decision should not be regarded as a significant impairment: Stephan Dreyer, Wolfgang Schulz: Was bringt die Datenschutzgrundverordnung für automatisierte Entscheidungssysteme? Bertelsmann Publishing 2018, p. 20. Marketing activities could thus be considered as annoying, but not significant in the sense of GDPR Article 22.

[127] According to the Commission, sending out advertising material does not have a significant adverse effect on data subjects. However, it should not be overlooked that this view dates back to 1992, a time when it was not at all foreseeable what the extent of targeted advertising would be like some years ago: Spiros Simitis: Budesdatenschutzgesetz 2006, para. 6 a, note 24.

[128] For instance in the area of differential pricing, which is considered a significant effect if prohibitively high prices effectively bar someone from certain goods or services: Article 29 Working Party in their 2017 guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Retrieved September 25, 2021.

[129] All of them are, according to Recital 71 "subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision."

[130] Provided that such a law also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, see GDRP Aarticle 22 (2b).

[131] Stephan Dreyer, Wolfgang Schulz: Was bringt die Datenschutzgrundverordnung für automatisierte Entscheidungssysteme? Bertelsmann Stiftung Publishing 2018, p. 21.

[132] For example, the new German BDSG provides a corresponding exception for insurance contracts in § 37 (1).

of national laws in the light of higher-ranking EU law, and it makes compliance more difficult for those controllers who do not merely fall under one jurisdiction. At first sight, the Regulation also foresees for a limit for the admissibility of automated decision-making as GDPR Article 22 (4) prohibits the use of special categories of personal data within the meaning of GDPR Article 9 (1) for automated decision-making. But this does not apply if the data subject has given explicit consent or when processing is necessary for reasons of substantial public interest.[133] GDPR Article 9 (2) names a whole catalogue of exemption clauses, and from an entrepreneurial point of view, it is likely that the following two exceptions will arouse interest: processing of sensitive data is admissible if it relates to personal data which are manifestly made public by the data subject,[134] and processing of special categories of data is admissible if it is "*necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) based on Union or Member State law which shall be proportionate to the aim pursued (and) respect the essence of the right to data protection".*[135] It can therefore be assumed that companies may concentrate on the investigation of and focus on scientific and statistical purposes in connection with Big Data applications and automated decision-making. In any event, in order to perform automated decision-making in a compliant manner, the controller has to implement suitable measures[136] to safeguard data subjects' rights and freedoms and interests and to assess and document[137] the endeavor.

Finally, it should be noted that with regard to GDPR Article 22, there is controversy about the ambiguity of the norm, as to whether or not the rule shall be interpreted as a prohibition[138] in the sense that the controller must respect legal limitations, or if it shall be considered an individual right.[139] The difference being that, exercising a right requires action of the data subject, while a prohibition offers protection by default. The latter seems favorable as, otherwise, automated decisions could be legitimized based on implicit consent, which does not comply with the idea of consent as a specific, freely given and informed indication of a data subject's choices.[140] Therefore, the concept of consent must be examined as well:

[133] Datenschutzkonferenz Kurzpapier Nr. 17, pp. 2 and 3. Paper published March 27 2018, available at https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_17_Besondere-Kategorien.pdf. Retrieved September 25, 2021.

[134] GDPR Article 9 (2) lit. e.

[135] GDPR Article 9 (2) lit. j.

[136] GDPR Article 22 (4).

[137] GDPR Article 35 (1, 3, 7).

[138] For instance, Isak Mendoza and Lee A. Bygrave: The right not to be subject to automated decisions based on profiling, University of Oslo, Legal Studies, Research Paper Series No. 2017-20, available at https://ssrn.com/abstract=2964855. Retrieved September 25, 2021.

[139] Some authors stress that Article 22 and its predecessors do not prohibit the use of automated individual decisions: Bettina Berendt, Sören Preibusch: Toward accountable discrimination-aware data mining- the importance of keeping the human in the loop, Big Data. 2017, vol. 5, Nr. 2, pp. 135-152, available at https://www.ncbi.nlm.nih.gov/pubmed/28586238. Retrieved September 25, 2021.

[140] Even though the authors refer to the Data Protection Directive and not to GDPR, their argument is still valid: Servge Gutwirth, Paul De Hert: Regulating profiling in a democratic constitutional state, in: Profiling the European citizen, Springer 2010, p. 283, available at http://www.vub.ac.be/LSTS/pub/Dehert/Dehert_365_restricted.pdf. Retrieved September 26, 2021.

8. Consent

Consent generally plays an important role in data protection and is frequently used to justify the processing of personal data. Recital 32 describes conditions for consent as set forth in GDPR Article 7: "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement*". Consequently, Recital 32 explicitly mentions that inactivity cannot constitute consent; consent can only be given unambiguously. What remained the same is that, like the Data Protection Directive, GDPR also requires explicit consent for sensitive personal data.[141] But GDPR brought some changes with regard to consent, beginning with seemingly simple topics like form requirements: GDPR does not at all insist on a written form requirement; the contrary is true, but Recital 42 makes it clear that there is a burden of proof that consent exists, and that is why controllers have to think about how to best comply with the challenge of demonstrating that the data subject has given consent to the processing operation. The issue of form requirements also led to sector- and scenario-specific variations in national jurisdictions:[142] As a general rule,[143] former § 4a (1) of the German Federal Data Protection Law required written form for consent. However, § 13 (2) of the German Tele-Media Act[144] allowed for electronic consent, for example, by clicking a checkbox. In addition, § 26 (2) of the new German Federal Data Protection Law again stipulates the written form in an employment context. Another particularity is that GDPR introduced special conditions applicable to child's consent in relation to information society services.[145] This is truly remarkable since the GDPR did not even consider such practice-relevant topics as marketing[146] or employee data protection[147] with own Articles. Generally speaking, consent is key when the exercise of control over own data is in question,

[141] GDPR Article 9 (2 a).

[142] In comparison (and as a general rule), former § 4 a (1) of the German Federal Data Protection Law required written form for consent (with exceptions depending on the circumstances of the individual case). However, § 13 (2) of the German Tele-Media Act allowed for electronic consent, e.g., by clicking a checkbox and the like.

[143] With exceptions depending on the circumstances of the individual case. It is questionable how a deviation from the written form requirement could be argued in the employment environment when in fact employees are either permanently present or can be reached via Intranet, Email, by post. If time pressure was to serve as an argument, this fails due to fact that this way, the voluntary nature of consent is in doubt.

[144] The German Telemedia Act (TMG) will soon to be replaced with the "Telecommunications Telemedia Data Protection Act" (TTDSG). This new law is intended to bundle the parts of the German Telecommunications Act (TKG) and the German Telemedia Act (TMG) that are relevant to data privacy into one central law. Background information on this legal development is provided by the consultancy bITs in their blog "TTDSG passiert Bundesrat – endlich verbindliche Regelungen für Cookies" published June 3 2021, available at https://www.bits.gmbh/ttdsg-passiert-bundesrat-endlich-verbindliche-regelungen-fuer-cookies/. Retrieved September 26, 2021.

[145] GDPR Article 8 and Recital 38.

[146] Only Recital 47 deals with marketing by saying that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest".

[147] Processing of personal data in the employment context is covered in Article 88 GDPR. GDPR delegates the topic to member states as "*member states may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data (...)*".

and an important condition to exercise control is transparency.[148] That is why a data subject requires all necessary information to make a free decision, and this seems difficult when automated decision-making is applied. As a consequence, one of the major issues regarding consent in the framework of automated decision-making, especially when it is based on profiling, is the question whether or not sufficient information was provided to the data subject:

Given the complex matter, even if the data controller fulfills existing transparency requirements and provides the data subject with information concerning the logic involved in making the decision, it remains questionable whether the fulfillment of this legal obligation is enough for the data subject to realize how an automated decision may (and will) affect him.[149] It is difficult to imagine valid consent as consent must be intelligible in order to be specific; clear reference has to be made to the scope and the consequences of the data processing.[150] From a business perspective it must be considered that, for reasons of intellectual property and competitive advantage, functionality and logic of an algorithm are often kept secret and therefore not[151] or only partially disclosed. Moreover, Recital 43 explicitly stresses that "*in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller*". This is most probably the case for all Big Tech players such as Meta (formerly known as Facebook)[152] or Google. Recital 43 also underlines that consent is presumed not to be freely given if the performance of a contract or the provision of a service is made conditional on the consent of the data subject to the processing of personal data. Another factual problem arises from the fact that automated decision-making which is based on profiling does not have to cover exclusively the personal data of the data subject that consented to this type of data processing, but that it might also involve personal data of other individuals.[153] Consent can neither cover other people's personal data not can it be applied in an open-ended set of processing activities. Furthermore, consent can be revoked at any time, and in the framework of automated individual decision-making, additional

[148] Detailed background information is provided by the Article 29 Working Party in their 2011 opinion (15/2011) on consent, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf. Retrieved September 26, 2021.

[149] Laurens Nauds: The Right not to be Subject to Automated Decision-Making: The role of explicit consent. Article published August 2 2016, available at https://www.law.kuleuven.be/citip/blog/the-right-not-to-be-subject-to-automated-decision-making-the-role-of-explicit-consent/. Retrieved September 26, 2021.

[150] The requirements of consent are explained in the 2011 opinion (15/2011) of the Article 29 Working Party on consent, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf. Retrieved September 26, 2021.

[151] In Germany, a popular example was the case of SCHUFA, one of the main credit bureaus. The issue was how their score is calculated and displayed. Background information is available at https://www.internet-law.de/2014/02/das-urteil-des-bgh-zum-schufa-scoring-im-volltext.html. Retrieved September 26, 2021.

[152] Facebook Inc. changed its name to Meta Platforms Inc., source: https://economictimes.indiatimes.com/tech/technology/facebook-is-now-meta-a-look-at-other-corporate-rebranding-efforts/articleshow/87353823.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst. Retrieved January 22, 2022.

[153] Veleria Ferraris et al: The impact on profiling on fundamental rights. Article published December 22 2013, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366753. Retrieved September 26, 2021.

data subject rights apply.[154] As a result, using consent as legal grounds for data processing is sometimes much more difficult and much less recommendable than many businesses might assume. However, many companies still opt for consent[155] as they believe this is both, a legally admissible and safe way to obtain legal grounds for the desired data processing.

9. Other relevant definitions including risk and harm

Apart from the above definitions, GDPRs furthermore defines other important terms such as controller, processor, recipient and third party. These terms are important for assigning responsibility: a controller is a natural or legal person (…) which, alone or jointly with others, determines the purposes and means of the processing of the personal data.[156] A processor is a natural or legal person (…) which processes personal data on behalf of the controller.[157] A third party is a natural or legal person (…) other than the data subject, controller, processor or persons who, under the direct authority of the controller or processor are authorized to process personal data.[158] A recipient, on the other hand, is a natural or legal person to which the personal data are disclosed.[159] Joint controllership is given when two or more controllers jointly determine the purposes and means of the processing.[160] Given the complexity of modern data processing activities and the variety of service providers involved, the differentiation needed to identify and distinguish these players is not always easy to accomplish.

Due to the fact that Big Data, automated decision making and Artificial Intelligence may involve risk from a data subject perspective, it is important to know what GDPR says about risk: Recital 75 deals with risks to the rights and freedoms of natural persons and explains that "*the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political*

[154] The data subject has the right to contest the decision, to express his or her point of view and to obtain human intervention on the part of the controller, see Laurens Nauds: The Right not to be Subject to Automated Decision-Making: The role of explicit consent. Article published August 2 2016, available at https://www.law.kuleuven.be/citip/blog/the-right-not-to-be-subject-to-automated-decision-making-the-role-of-explicit-consent/. Retrieved September 26, 2021.

[155] Nico Härting describes this as a "consent fetish" during his presentation in the framework of the 2012 annual DSRI academy summit. The presentation is available at https://rsw.beck.de/cms/?toc=ZD.60&docid=338853. Retrieved September 26, 2021.

[156] GDPR Article 4 (7).

[157] GDPR Article 4 (8).

[158] GDPR Article 4 (10).

[159] GDPR Article 4 (9).

[160] GDPR Article 26 (1).

opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analyzing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects." GDPR as such does not define risk, it only provides interpretative guidance on what may constitute risk and lists examples, and the fact that privacy violations may be given without privacy harms[161] and the fact that relevant terms like risk, threat, harm, injury or violation are often used interchangeably or evaluated in a different context (e.g., regulator perspective as opposed to the individual's or court perspective) adds to the problem. Regulators dealt with the issue of informational injuries[162] and various scholars tried to explain risk and provide a typology of privacy harms,[163] e.g., by distinguishing privacy harms as follows: physical, economic, reputational, emotional; due to disturbance, vulnerability, loss of autonomy, control, informed choice or based on thwarted expectations, chilling effects or discrimination. Another approach was to explain which risks exist in which stages of data processing,[164] starting with information collection: surveillance (e.g. monitoring) and interrogation (e.g. questioning) and during data processing: aggregation (e.g. combining of datasets), identification (e.g. linking of information), secondary use (e.g. using data for other purposes), insecurity (e.g. carelessness in protecting information from leaks), exclusion (e.g. failure to let the individual know about information others have about them) and in the event of information dissemination, where the following risks have been identified: breach of confidentiality (e.g. breaking the promise to keep information confidential), disclosure (e.g. revealing truthful information), distortion (e.g. disseminating false or misleading information about an individual), blackmail (e.g. threatening to disclose information), increased accessibility (e.g. amplifying the accessibility of personal information) and appropriation (e.g. using an individual's identity to serve the aims and interests of another), and finally invasion where intrusion (e.g. disturbing an individual's tranquility) can be distinguished from decisional interference (e.g. interfering with an individual's decision making).

[161] Ryan Calo: The boundaries of privacy harm, Indiana Law Journal 2011, vol. 86, no. 3.

[162] Maureen Ohlhausen for the Federal Trade Commission: Painting the Privacy Landscape: Informational Injury in FTC privacy and data security cases. Article published September 19 2017 and is available at https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf. Retrieved September 26, 2021.

[163] See Daniel Solove's famous book: Understanding Privacy, Harvard University Press 2008.

[164] Taxonomy of Privacy infographic provided by Enterprivacy Consulting Group, published August 3 2017, available at https://enterprivacy.com/2017/08/03/taxonomy-of-privacy-infographic/. Retrieved September 26, 2021.

One further aspect to consider is that Big Data, ADM and AI do not only involve potential risks for individuals but may also lead to societal harms,[165] e.g., by accelerating growth and prosperity for some, and at the same time leading to significant changes in the employment sector for others or by leading to greater connectivity on the one hand but also greater vulnerability on the other owing to a much larger "*cyber-physical attack surface*."[166] Risk generally always also depends on the context, the operational environment as well as the type of data, the device in question as well as access and data location, retention and preservation.[167] In addition, risk may also be based on (weak) business processes and governance, miscommunication and conflict of interest as well as resource and project management, and issues of stewardship, values and ethics.[168] Finally, Big Data and AI applications also have a political dimension and human rights implication.[169] A definition of risk the privacy community came up with is that "*privacy risk equals the probability that a data processing activity will result in an impact, threat to or loss of (in varying degrees of severity) a valued outcome (for example rights and freedoms).*"[170]

GDPR takes a risk-based approach, for example by saying that technical and organizational measures must match the processing with regards to "*the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*,"[171] and GDPR also deals with high risk since impact assessments are needed for high risk data processing activities.[172] However, it is difficult to draw the line between (i.e. low) risk and high (or unacceptable) risk, but the fact that many European supervisory authorities issued guidance in accordance with GDPR Article 35 (4) and provided "*list(s) about which (...) processing operations (...) are subject to the requirement for a data protection impact assessment*" helps in practice when it comes to defining

[165] Danielle Keats Citron, Daniel Solove: Privacy harms. George Washington Law School Public Law and Legal Theory Paper No. 2021-11.
[166] National Intelligence Council: Global Trends 2040 – a more contested world, published March 2021, available at https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf. Retrieved September 26, 2021.
[167] Mike Dutch: A Data Protection Taxonomy, paper for the Storage Networking Industry Association (SNIA), Article published June 2010, available at https://www.snia.org/sites/default/files/A_Data_Protection_Taxonomy_V51.pdf. Retrieved September 26, 2021.
[168] Government of Canada: Guide to risk taxonomies, last modified March 29 2016, available at https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/taxonomies.html#toc2. Retrieved September 26, 2021.
[169] Catelijne Muller: The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law, report for the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI). Article published June 24 2020, available at https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da. Retrieved September 26, 2021.
[170] Center for Information Policy Leadership: Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. CIPL's paper was published in December 2016 and is available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf. Retrieved September 26, 2021.
[171] GDPR Article 32 (1).
[172] GDPR Article 35.

and documenting high-risk processing activities based on general criteria such as large-scale processing, systematic monitoring, or the use of new technology.[173]

10. Challenges with definitions and terminology

Risk is a good example of challenges as regards definitions and terminology since these seemingly simply questions raise issues in relation to scope and applicability: the notion of risk is a key element when it comes to assessing potential consequences of data processing activities. While it is clear that risks can be manifold, GDPR's comprehensive protective purpose which is laid down in the above-mentioned detailed catalogue of examples for potential risks is viewed critically for many reasons: some say that "*no life risk of this world remains unmentioned in Recital 75*"[174] and that this ultimately leads to the question where data protection ends. This is all the more true given the fact that more and more data qualify as personal information, because combining of data sets and the like may lead to linkability of information and identifiability of natural persons, meaning that literally any handling of data would become subject to data protection laws.[175] Others stress that data protection law, unlike other areas of law, does not dispose of limiting, restrictive criteria to help balance rights and freedoms and interest[176] and this way, allow for legal certainty. Most importantly, GDPR uses a variety of terms, and it is questionable if that means that those terms can be used interchangeably. It also leads to the question which concept is behind that terminology in the sense of what exactly is to be protected by GDPR: rights, freedoms, interests, privacy, data protection, informational self-determination, informational integrity or a combination?[177] GDPR mentions rights and freedoms fifty times, and fundamental rights and freedoms around a dozen times, whereas other terms like vital or legitimate interests, human dignity or compelling legitimate grounds are used in specific scenarios. The list of protected interests seems erratic and it appears that literature has not yet taken the time to examine GDPR's wording in order to define protected interest. In addition, further legal initiatives around the globe add new terminology (definitions) which result in further complexity und uncertainty.

[173] GDPR Recital 91 provides background on the "necessity of a data protection impact assessment".

[174] Niko Härting: Wann ist eine Datenverarbeitung eigentlich „erforderlich"? Article published February 1 2019, available at https://www.cr-online.de/blog/2019/02/01/wann-ist-eine-datenverarbeitung-eigentlich-erforderlich/. Retrieved September 26, 2021.

[175] Omer Tene, Jules Polonetsky: Privacy in the age of big data – a time for big decisions, Stanford Law Review 2012, vol. 64:63, p. 66.

[176] Winfried Veil: Die Schutzgutmisere des Datenschutzrechts (Teil I). Article published February 6 2019, available at https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/. Retrieved September 26, 2021.

[177] Winfried Veil: Zum Schutzgut der DSGVO – eine naïve Wortlautanalyse. Article published April 22 2021, available at https://www.cr-online.de/blog/2021/04/22/zum-schutzgut-der-ds-gvo-eine-naive-wortlautanalyse/. Retrieved September 26, 2021.

II. Definition of privacy

As opposed to the "*protection of fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*",[178] there is no appearance of the term privacy in GDPR. It is hence unclear what exactly is meant by privacy, so to speak the essence of what is to be protected: is data protection a subset, an expression of the right to privacy, or does it provide additional protection?[179] Existing legal bases are not helpful: the term privacy appears frequently, e.g., in the United Nations Universal Declaration of Human Rights[180] or the OECD Privacy Guidelines as well as various other resolutions and guidelines at international level. Other norms operate with terms such as private and family life,[181] but there is no universal definition or privacy. Current legislation does not offer a conclusive definition of the term privacy or private data; data protection is thus rather achieved through the regulation of the conditions under which personal data may be processed.[182] If privacy is about the right to keep personal matters and relationships secret[183] and being apart from company or observation,[184] then privacy is about separating private from public life. Given that this depends on the era, the degree of technical development as well as the social and cultural environment of the individual, it is comprehensible that the concrete idea of privacy differs and develops, and the notion of privacy as we know it has only emerged in the past 150 years.[185] Perhaps a suitable and catchy definition of privacy would be "*control over knowledge about oneself*",[186] but the problem is that data subjects do not exercise control as the so-called privacy paradox shows, and moreover, it is quite often not possible to predict in advance which personal information will be claimed as private, since such claims are made on an ex post facto basis and also depend on contextual factors.[187] Social media is a good example for the shift of private life to public as, some years ago, it would have been unimaginable to share so many private details with so many people. The unanimity with which the claim for privacy is represented stands in contrast to the diversity of answers to the question of which

[178] GDPR Article 1 (2).

[179] Juliane Kokott and Christoph Sobotta examine this question: The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Vol. 3, Issue 4, pp. 222–228, available at https://academic.oup.com/idpl/article/3/4/222/727206. Retrieved September 26, 2021.

[180] GDPR Article 12.

[181] Article 8 of the European Convention on Human Rights.

[182] Karen McCullagh: Protecting privacy through control of personal data processing – a flawed approach, International Review of Law, Computers and Technology 2009, vol. 23, no. 1, p. 13.

[183] Cambridge Dictionary definition, available at https://dictionary.cambridge.org/de/worterbuch/englisch/privacy. Retrieved September 26, 2021.

[184] Merriam-Webster definition, available at https://www.merriam-webster.com/dictionary/privacy. Retrieved September 26, 2021.

[185] Winfried Veil: 21 Thesen zum Irrweg der DSGVO. Article published May 23 2018, available at https://www.cr-online.de/blog/2018/05/23/21-thesen-zum-irrweg-der-ds-gvo/#anker4. Retrieved September 26, 2021.

[186] Charles Fried: Privacy, Yale Law Journal 1968, vol. 77, p. 482, available at https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5894&context=ylj. Retrieved September 26, 2021.

[187] Karen McCullagh: Protecting privacy through control of personal data processing – a flawed approach, International Review of Law, Computers and Technology 2009, vol. 23, no. 1, p. 22.

value(s) should actually be protected.[188] In this regard, some pursue the idea of data ownership, others stress informational self-determination or emphasize defense against surveillance or the instrumental character of data protection as risk prevention, while others are primarily concerned with combating power asymmetries between organizations (state, companies, service providers) and individuals (citizens, customers, patients, clients).[189] Numerous attempts to define privacy failed because the definitions were too narrow or too broad or because they focused on certain aspects, but some authors developed characteristics of privacy such as the right to be let alone, the control of personal information, limited access to the self, as well as secrecy and intimacy.[190] Others discussed levels that affect privacy such as the political, the socio-cultural and the personal level:[191] they defined the right to privacy as the right of individuals to determine for themselves when, how, and to what extent information about themselves is communicated to others, including when such information will be obtained and what uses will be made of it by others. Moreover, technology must be taken into consideration as well in order to grant protection not only by the state or authorities, but also by businesses which process personal data. GDPR embraces this idea by setting standards for data protection by design and by default in GDPR Article 25. Perhaps a contemporary definition of privacy is the absence of harmful use[192] with regards to the individuals concerned with the data processing – an idea that is consistent with the Regulation’s risk-oriented approach and the fact that the production, collection and use of data is growing at fast pace, which is why some declare the regulation of data collection to be a losing battle.[193]

The difference between privacy and data protection needs to be clarified, because these terms cannot be considered identical even though they are quite often used interchangeably. The terms can have different meanings depending on context, industry or jurisdiction: There are two systems which ensure the protection of fundamental human rights in Europe, the European Convention on Human Rights (Convention) and the Charter of Fundamental Rights of the European Union (Charter). The protection

[188] Rainer Stentzel: Das Grundrecht auf ...? Auf der Suche nach dem Schutzgut des Datenschutzes in der Europäischen Union, PingG, issue 5, pp. 185-191, available at https://www.pingdigital.de/ce/das-grundrecht-auf/detail.html. Retrieved September 26, 2021.

[189] Winfried Veil: 21 Thesen zum Irrweg der DSGVO. Article published May 23 2018, available at https://www.cr-online.de/blog/2018/05/23/21-thesen-zum-irrweg-der-ds-gvo/#anker4. Retrieved September 26, 2021.

[190] Daniel Solove: Conceptualizing Privacy, California Law Review Vol. 90, No. 4, pp. 1132-1140, available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview. Retrieved September 26, 2021.

[191] Alan Westin: Social and political dimensions of privacy. Journal of Social Issues Vol 59, No. 2, pp. 431-434, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.455.4866&rep=rep1&type=pdf. Retrieved September 26, 2021.

[192] Karen McCullagh: Protecting privacy through control of personal data processing – a flawed approach, International Review of Law, Computers and Technology 2009, vol. 23, no. 1, p. 23.

[193] The opinion of a data protection expert from Australia Karen McCullagh interviewed for her 2009 article: Protecting privacy through control of personal data processing – a flawed approach, International Review of Law, Computers and Technology 2009, vol. 23, no. 1, p. 22.
Karen McCullagh: Protecting privacy through control of personal data processing – a flawed approach, International Review of Law, Computers and Technology 2009, vol. 23, no. 1, p.22.

of personal data and privacy are closely linked in the jurisprudence of both, the European Court of Human Rights (ECtHR)[194] and the Court of Justice of the European Union (CJEU), but their personal and substantive scopes diverge:[195] Article 8 of the Convention and Article 7 of the Charter stipulate that everyone has the right to respect for private and family life, home and communications, and Article 8 of the Charter specifically deals with protection of personal data. This shows that privacy and data protection are not the same. The General Data Protection Regulation is, as the name says, about data protection, and given the numerous duties processors must implement,[196] one may say that data protection is about a (management) system of data processing practices for the protection of privacy, meaning that companies ensure protection whereas individuals ensure privacy by controls to which they are entitled as data subjects. Privacy includes private and family life, home and correspondence. It is a recognized fundamental human right and as such addresses the state and its bodies; data protection addresses the state[197] as well as companies and, depending on the case, even individuals as they may also be controllers or processors.[198]

III. Definition of Artificial Intelligence

Big Data is based on algorithms, and algorithms are best described as step-by-step procedures for the calculation, evaluation and automated reasoning as well as decision-making which are based on data processing.[199] The difference between Artificial Intelligence and former Big Data analytics is that AI programs do not rely on a linear data analysis; instead they learn from the data which allows them to respond intelligently and to adapt their outputs accordingly.[200] A prominent definition of AI is that Artificial Intelligence is the "*activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment*"[201]. John McCarthy who is believed to be the father of AI coined the term Artificial Intelligence as "*the science*

[194] The final arbitrator on the Convention.

[195] Juliane Kokott, Christoph Sobotta: The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, vol. 3, issue 4, pp. 222–228, available at https://academic.oup.com/idpl/article/3/4/222/727206. Retrieved September 26, 2021.

[196] Winfried Veil: Accountability – Wie weit reicht die Rechenschaftspflicht der DSGVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, Zeitschrift für Datenschutz vol. 1 2018, pp. 9-16, available at https://rsw.beck.de/rsw/upload/ZD/ZD_01-2018_-_Beitrag_Veil_1.pdf. Retrieved September 26, 2021.

[197] GDPR Article 2 (2) names exceptions.

[198] GDPR Article 4 (7) and (8): controller or processor means a natural or legal person.

[199] European Union Agency for Fundamental Rights: Handbook on European Data Protection Law 2018 edition, p. 351, available at https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law. Retrieved September 26, 2021.

[200] ICO: Big data, artificial intelligence, machine learning and data protection, p. 6, available at https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Retrieved September 26, 2021.

[201] Nils Nilsson, The Quest for Artificial Intelligence: A History of Ideas and Achievements, Cambridge University Press 2010.

and engineering of making intelligent machines."[202] Others define AI as a "*set of techniques that seek to approximate cognitive tasks*" or as "*systems that act rationally to achieve goals via perception, planning, reasoning, communicating, decision making and acting*."[203] Other definitions distinguish general and narrow Artificial Intelligence, the latter refers to AI systems "*that addresses specific application areas such as playing strategic games, language translation, self-driving vehicles and image recognition*", whereas general AI means "*a notional future artificial intelligence system that exhibits apparently intelligent behavior at least as advanced as a person across the range of cognitive, emotional, and social behaviors*."[204] Big Data, Artificial Intelligence and so-called machine learning are often used interchangeably, but there are important differences: Big Data is about innovative forms of high-volume, high-velocity and high-variety information processing which is cost-effective and enables enhanced insight and decision making.[205] Artificial Intelligence refers to systems which perceive their environment and which are able to perform various tasks with some degree of autonomy to achieve specific goals.[206] There is no single or generally accepted definition of AI, but the term Artificial Intelligence is used to describe computer systems that are able to learn from own experiences and solve complex problems in different situations.[207] Scientists speak of AI whenever a non-biological system mimics cognitive functions and this way shows behaviors which were thought to be unique to natural persons.[208]

D. Characteristics, types, benefits and risks of Big Data and AI

I. Characteristics of Big Data

There are numerous definitions of Big Data, but rather than searching for the perfect definition, it makes more sense to turn to the characteristics of Big Data and to understand the value chains:[209] It

[202] Andy Peart: Homage to John McCarthy, the Father of Artificial Intelligence. Article published October 29 2020, available at https://www.artificial-solutions.com/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence. Retrieved September 26, 2021.

[203] Valerie Thomas on behalf of the Regulatory Institute: Report on Artificial Intelligence part I: the existing regulatory landscape. Report published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/. Retrieved September 26, 2021.

[204] For instance, section 3 of H.R.4625 of the Future of Artificial Intelligence Act of 2017 which is available at https://www.congress.gov/bill/115th-congress/house-bill/4625/titles. Retrieved September 26, 2021.

[205] Definition of big data provided by the Gartner IT glossary, available at http://www.gartner.com/it-glossary/big-dataA. Retrieved September 26, 2021.

[206] European Commission's 2018 factsheet on Artificial Intelligence, available at https://ec.europa.eu/digital-single-market/en/artificial-intelligence. Retrieved September 26, 2021.

[207] Norwegian Data Protection Authority: Artificial intelligence and Privacy 2018, p. 5, available at https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf. Retrieved September 26, 2021.

[208] FRA's Handbook on European Data Protection Law 2018 edition, p. 351, available at https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law. Retrieved September 26, 2021.

[209] Nikolaus Forgo et al.: The principle of purpose limitation in big data, p. 21.

can generally be said that Big Data is about the analysis[210] of vast amounts of data at high speed (ideal: 'real-time') with the aim of making it economically viable. The reason for that is that, in today’s business landscape, data management can be a major determinant of success. Big data applications are characterized by large and growing amounts of data (e.g. sensor, log, clickstream, transaction or location data, search queries, social network interactions), data diversity (types, sources, formats), the speed of the evaluation (ideal: real time) and the quality of the results and forecasts obtained out.[211] Big Data lives on a large, diverse, complex and growing and pool[212] which can only be addressed with new (corresponding) techniques and a suitable infrastructure to cope with such datasets. Big Data is therefore different from old school data management, particularly because nowadays, the performance of computational tasks place in an affordable and convenient way as processing of data is much cheaper and sharing of data is much easier.[213] It became popular to characterize Big Data by volume, variety and velocity,[214] terms which are all commencing with the initial letter “*V*”, and ever since, the number of terms grew from the initial three “*Vs*” to more than forty.[215] However, only the most common vectors shall be presented in the framework of this paper:

1. Volume: size of data

The volume of data is increasing at a staggering rate[216] as more people use data-collecting devices and more devices are connected to the internet, which results in the generation of billions of terabytes of (man-human, man-machine and machine-machine) data per day.

2. Variety: type of data

Databases were designed to process a smaller volume of structured data, and the challenge with Big Data is that it includes various sources and formats of (un-)structured data, audio, video, social media information,[217] and that the level of completeness differs.

[210] Analyses are actually the second step since big data applications can be divided into the following stages and steps: acquisition, data processing / evaluation: Forgo et al.: The principle of purpose limitation and big data, p. 21.

[211] Helbing, Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, KuR 2015, p. 145.

[212] Mario Martini: Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz in: Hill/Martini/Wagner: Die digitale Lebenswelt gestalten, Baden-Baden 2015, pp. 99-169.

[213] Christopher Kuner, Fred Cate, Christopher Millard, Dan Svantesson: The Challenge of Big Data for Data Protection, International Data Privacy Law 2012, vol. 2, no. 2, p. 47.

[214] Doug Laney (2001) for Gartner in: 3D Data Management – controlling Data Volume, Velocity, and Variety. Article published February 2001, available at http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf. Retrieved September 26, 2021.

[215] Tom Shafer: The 42 V's of Big Data and Data Science. Article published April 1 2017, available at https://www.elderresearch.com/blog/42-v-of-big-data. Retrieved September 26, 2021.

[216] Figures and background information provided by Gary Price. His 2014 article refers to the EMC Digital Universe Study. Study published April 16 2014 and is available at https://www.infodocket.com/2014/04/16/how-large-is-the-digital-universe-how-fast-is-it-growing-2014-emc-digital-universe-study-now-available/. Retrieved September 26, 2021.

3. Velocity: speed of data

Not only the volume of data is increasing, but also the rate at which data is generated.[218] The rapidly increasing speed at which new data is being created[219] also affects the need for that data to be digested and analyzed in near real-time.

4. Veracity: quality of data

Veracity is about how truthful a data set may be. It has to do with improving the accuracy of Big Data by removing undesired factors like duplication, inconsistencies, abnormalities or bias. It is therefore very important[220] from a decision and intelligence viewpoint.

5. Variability: meaning of data

Variability is different from variety as variability focuses on properly understanding and interpreting the correct meanings of raw data. This is particularly important in the framework of natural language processing.[221]

6. Volatility: duration of usefulness of data

Volatility refers to how long data is available, how long it is valid and how long it should be stored.[222] In a world of real-time data, the point at which data is no longer relevant to the current analysis has to be determined.[223]

[217] David Gewirtz: Volume, velocity, and variety - understanding the three V's of big data. Article published March 21 2018, available at https://www.zdnet.com/article/volume-velocity-and-variety-understanding-the-three-vs-of-big-data/. Retrieved September 26, 2021.

[218] Tom Shafer: The 42 V's of Big Data and Data Science. Article published April 1 2017, available at https://www.elderresearch.com/blog/42-v-of-big-data. Retrieved September 26, 2021.

[219] For instance, in the framework of online gaming where millions of users operate concurrently or the large amount of photo material which is uploaded daily to social media platforms, or stock exchange operations where trading movements are reflected within microseconds, etc.

[220] Cassandra McNeill: Veracity – the most important "V" of Big Data. Article published August 29 2019, available at https://www.gutcheckit.com/blog/veracity-big-data-v/. Retrieved September 26, 2021.

[221] For example, the word "great" is associated with something positive whereas "greatly" (disappointed) has a negative meaning, see Eileen McNulty in her 2014 article: Understanding Big Data - the Seven V's, the article was published on May 22 2014 and is available at https://dataconomy.com/2014/05/seven-vs-big-data/. Retrieved September 26, 2021.

[222] Nancy Tai: Dimensions of Big Datarticle published July 27 2018, available at http://www.klarity-analytics.com/2015/07/27/dimensions-of-big-data/. Retrieved September 26, 2021.

[223] In this regard, storage limitations and legal requirements also play a role.

7. Value: importance of data

Big Data is about turning volume to value, other characteristics seem rather meaningless if businesses cannot derive economic value and competitive advantage[224] from Big Data. Value is the return resulting from the data management. The above characteristics do not represent an exhaustive description of Big Data applications. To complete the above enumeration to a certain extent, below is an overview of the most used features in large data applications:[225]

Volume	Quantity of collected and stored data
Velocity	The transfer rate of data between source and destination
Value	Business value to be derived from Big Data
Variety	Different type of data (pictures, videos, audio) are returned
Variability	Differentiation between noisy data and important data
Veracity	Analysis of captured data is virtually worthless if it’s not accurate
Validity	Accuracy of data used to extract result in the form of information
Volatility	Question of how long is the stored data is useful for the user
Virality	Rate at which the data is spread and received by different users
Viscosity	Time difference when the event occurred and when it was described
Vagueness	Ambiguity about data found; interpretation issues with results found

Even though it is still very common to link Big Data and AI to large volumes of data, some scientists believe that the future of artificial intelligence will be about less data, not more:[226] they claim that the training on mountains of data will soon be replaced since such systems have serious limitations, for example in cases in which little data exists or in instances where computers can be easily stumped.[227] They believe that companies will rely less on bottom-up data and more on top-down reasoning which

[224] Husam Barham: Achieving competitive advantage through big data – a literature review. Conference paper for the 2017 International Conference on Management of Engineering and Technology (PICMET) at Portland, Oregon, USA. The paper is available at https://www.researchgate.net/publication/318351614_Achieving_Competitive_Advantage_Through_Big_Data_A_Literature_Review. Retrieved September 26, 2021. Retrieved September 26, 2021.

[225] The overview is based on an article by Arockia Panimalar, Varnekha Shree and Veneshia Kathrine who describe the evolution of the vectors in their 2017 article: The 17 V’s of Big Data, International Research Journal of Engineering and Technology 2017, Vol. 4, Issue 9, pp. 329-333, available at https://www.irjet.net/archives/V4/i9/IRJET-V4I957.pdf. Retrieved September 26, 2021.

[226] James Wilson, Paul Daugherty, Chase Davenport: The Future of AI Will Be About Less Data, Not More. Article published January 14 2019, available at https://hbr.org/2019/01/the-future-of-ai-will-be-about-less-data-not-more. Retrieved September 26, 2021.

[227] At present, smart phone facial recognition systems are sometimes unable to recognize “morning faces”, i.e. a puffy, haggard look on first awakening; autonomous driving is tricky as such cars have difficulties to recognize children or pedestrians wearing costumes; so-called CAPTCHAs are easy for humans, but hard for computers.

resembles the way humans approach problems and tasks, e.g., by using common sense and ready expertise.

II. Types of Big Data analytics

As regards Big Data analytics, a general distinction can be made between three dominant types of analytics, each of them offering different findings: descriptive, predictive and prescriptive analytics.[228] Descriptive analytics use data aggregation and data mining to create reports, dashboards or scorecards in order to provide insight into the past. Predictive analytics use statistical models and forecasts techniques to discover explanatory patterns, and that is why such tools can predict an outcome with a significant probability of accuracy and provide businesses the ability to forecast future developments. Prescriptive analytics use optimization and simulation algorithms to provide advice on possible outcomes. The possibilities to make use of Big Data applications are countless, however, Big Data applications can roughly be divided in the following groups:[229] customer analytics, operational analytics, analytics which are used to (further) develop data-driven products and services as well as tools which are used for compliance purposes and fraud detection. These objectives are often grouped in a different manner, depending on whether or not transactional data are in question, such as: decision science to improve the decision-making process; performance management which is typically done by business intelligence tools using dashboards, reports; data exploration which makes use of statistics to allow for predictive modeling as well as (social) analytics to measure awareness, engagement and word of mouth, the success of (online) campaigns, etc.[230]

1. Operational Analytics and Forecasting

Operational analytics refers to business analytics which focus on improving existing operations and to get more transparent information for business planning purposes.[231] As such, the idea of improving of business operations is anything but new. The difference nowadays is that Big Data allows for a more detailed and timely insight into operations, which is important for monitoring and maintenance of

[228] Explanations and definitions of these terms can be found in James Blackman’s 2018 article: Operational intelligence, three ways – descriptive, predictive and prescriptive. Article published December 11 2018, available at https://enterpriseiotinsights.com/20181211/channels/fundamentals/descriptive-predictive-prescriptive-analytics. Retrieved September 26, 2021.

[229] A summary on big data use cases is provided by Datameer in their 2016 E-book: Top Five High-Impact Use Cases for Big Data Analytics. E-book published 2016, available at http://orcp.hustoj.com/wp-content/uploads/2016/01/eBook-Top-Five-High-Impact-UseCases-for-Big-Data-Analytics.pdf. Retrieved September 26, 2021.

[230] Salvatore Parise, Bela Iyer, Dan Vesset: Four strategies to capture and create value from big data, published in Ivey Business Journal, July/August issue 2012, online version available at http://www.iveybusinessjournal.com/topics/strategy/four-strategies-to-capture-and-create-value-from-big-data#.Uwm-L4XHjWh. Retrieved September 26, 2021.

[231] Definition provided by Technopedia: https://www.techopedia.com/definition/29495/operational-analytics. Retrieved September 26, 2021.

systems or supply chain management etc. A higher level of operational analytics can be achieved when so-called data warehouse optimization is used: A data warehouse[232] is a data-service platform, a repository for all data an enterprise holds in various operational systems with the aim to capture data from diverse sources in order to allow for access and analysis rather than for transaction processing. The advantage[233] of such a unified database is that it allows for a unified approach for organizing and representing data; that is has a robust infrastructure; ideally with a high level of security and scalability; that it is accessible across the company for all divisions and that it enables contingency plans in terms of business continuity.

2. Customer Analytics and Marketing

There is a myriad of uses cases when customer analytics are in question: the segmentation of customers based on behavior patterns, the creation of 360-degree customer views, the analysis of customer sentiments, the delivery of personalized customer services based on customer profiles in real time, e.g., by so-called robo-advisor services or chat-bots,[234] the recommendation of next-best products to buy or the prevention of customer churn,[235] The prevention of customer churn is good example of how Big Data analytics are used as a basis for follow-up measures: an organization conducts a data analysis and identifies potentially critical moments in the customer relationship, for example by analyzing the ratio between the term and the amount of a loan in relation to the time at which loans were repaid in advance. The analysis is the first step for the creation of an efficient marketing mix as only those customers will be contacted where data indicated that there is a risk of early repayment, resulting in financial loss for the bank. As far as data protection is concerned, the first step may well work with aggregated data without the need to process personal data, but the second step is legally much more demanding as customer contacts are covered not only by data protection, but also by competition law.[236] Another important use case is social media – from advertising to speech and content moderation.

[232] Background information on the term enterprise data warehouse is provided by Jamens Kobielus: The Enterprise Data Warehouse – defined, refined, evolving with the times. Article published April 8 2008, available at https://go.forrester.com/blogs/08-04-08-the_enterprise_data_warehouse_edw_defined_refined_evolving_with_the_times/. Retrieved September 26, 2021.

[233] Features provided by Technopedia: https://www.techopedia.com/definition/26204/enterprise-data-warehouse. Retrieved September 26, 2021.

[234] Examples provided by Karsten Egetoft: Data-Driven Analytics: Practical Use Cases For Financial Services. Article published published January 29 2019, available at https://www.digitalistmag.com/customer-experience/2019/01/29/data-driven-analytics-practical-use-cases-for-financial-services-06195123/. Retrieved September 26, 2021.

[235] An exhaustive overview over big data use cases is provided by Alexander Bekker: Twenty Big Data Use Cases. Article published March 6 2018, available at https://www.experfy.com/blog/twenty-big-data-use-cases. Retrieved September 26, 2021.

[236] And, depending on the case and the jurisdiction in question, further laws might apply, for example, in the framework of unsolicited telephone calls or commercial e-mails. Such communications, as opposed to postal advertising which was priviledged under German data protection law, always required specific legal checking.

3. Data-driven products and services

A prominent example of analytics which are used for data-driven products and services is pricing. Average Internet users are not aware that neither the content[237] which a website displays nor the prices it indicates are the same to every user. Online shops are technically capable to offer each website customer a different price, a practice called personalized pricing:[238] customers can be recognized with the help of so-called cookies[239] which can categorize customers in order to group them as an either price-sensitive or a price-insensitive person. It can be argued that European data protection law applies to personalized pricing, meaning that companies are required to inform people about the specific purpose of processing their personal data.[240] The lawfulness of price personalization under the GDPR on the basis of consent, the necessity for pre-contractual or contractual measures, and the data controller's legitimate interests has been the subject of numerous publications.[241] Moreover, the Privacy and Electronic Communications Regulation (PECR) also covers cookies and the use of similar technologies for storing or accessing information, including technologies like device fingerprinting.[242] As a result, such an approach is as tempting as it is legally demanding.

4. Fraud prevention and compliance issues

Fraud prevention is a good example of how Big Data applications can help businesses to achieve legal compliance as, e.g., the banking sector is obliged to perform background checks and to permanently screen transactions in order to fulfill requirements which arise from various sanction lists.[243] Big Data analytics can also be very helpful when companies want to detect suspicious activities in order to prevent and fight fraud. This is especially important to e-commerce as there are specific challenges in the area of distance selling, for example the identification of the customer, address verification, credit

[237] So-called "responsive web-design", see http://blog.freedomscientific.com/responsive-web-design-why-one-site-can-behave-differently-on-different-pcs-and-browsers/ for background information. Retrieved September 26, 2021.

[238] Frederik Zuiderveen Borgesius, Joost Poort: Online Price Discrimination and EU Data Privacy Law, Journal of Consumer Policy Vol. 40, issue 3, pp. 347–366, available at https://www.researchgate.net/publication/318511438_Online_Price_Discrimination_and_EU_Data_Privacy_Law. Retrieved September 26, 2021.

[239] ICO describes cookies as "a small file of letters and numbers that is downloaded on to your computer when you visit a website. Cookies are used by many websites and can do a number of things, e.g. remembering your preferences, recording what you have put in your shopping basket, and counting the number of people looking at a website", source: https://ico.org.uk/your-data-matters/online/cookies/. Retrieved September 26, 2021.

[240] Frederik Zuiderveen Borgesius, Joost Poort: Online Price Discrimination and EU Data Privacy Law, Journal of Consumer Policy vol. 40, issue 3, pp. 347–366.

[241] For instance, Richard Steppe: Online price discrimination and personal data: A General Data Protection Regulation perspective, Computer Law & Security Review, vol. 33, issue 6, pp. 768-785, DOI: 10.1016/j.clsr.2017.05.008.

[242] See ICO at https://ico.org.uk/your-data-matters/online/cookies/. Retrieved September 26, 2021.

[243] Ernst & Young: Effective screening controls for sanctions and AML risk management. Published April 12 2018, available at https://vdocuments.net/effective-screening-controls-for-sanctions-and-aml-risk-screening-controls-for.html Retrieved September 26, 2021.

assessment and the like.[244] Because companies do not want to risk customer dissatisfaction through service delays or payment rejections, they turn to device or geo-location or even social media data analysis to perform real-time-checks for suspicious activities[245] so that the (online) customer journey is neither interrupted nor disturbed. This approach is comprehensible from a business point of view in terms of protection from possible financial risks arising from fraud.[246] But it should not be forgotten that such procedures are questionable[247] with regard to transparency requirements vis-à-vis data subjects; an average buyer does not suspect that a simple online order leads to a variety of background checks including devices and online activities, and it might therefore not cross his mind to read (extensive) privacy notices prior to the purchase.

5. Sense-making

In the context of Big Data analytics, a new class of analytic capability emerged which may be characterized as (general purpose) sense-making. This approach relates to a new type of technology which helps organizations to make decisions faster and better. Unlike master data management which helps businesses to gain control over information in order to have consistent and reliable master data records, sense-making is about making sense of "*their diverse observational space, ranging from data they own and control (e.g. structured master data) to data they do not or cannot control (e.g. externally-generated and less structured social media*".[248] Sense-making suggests that an organization can only be as smart as the sum of its observations collected across various enterprise systems,[249] and this is where Artificial Intelligence comes into play:

III. Types of Artificial Intelligence

1. Rule-based Artificial Intelligence

There are many forms of Artificial Intelligence; traditional algorithmic AI is rule-based, and therefore often compared to a recipe, including more or less of ingredients, and therefore leading to more or less

[244] Examples of retail use cases are provided by Igor Bobriakov: Top 10 Data Science Use Cases in Retail. Article published July 22 2018, available at https://medium.com/activewizards-machine-learning-company/top-10-data-science-use-cases-in-retail-6483accc6042. Retrieved September 26, 2021.

[245] For instance, the German company named RiskIdent. Background information on their services and the way they work can be found at their homepage: https://riskident.com/de/technologie/. Retrieved September 26, 2021.

[246] Also offered by the German company Arvato Financial Solutions as explained on their homepage: https://finance.arvato.com/de/financial-solutions/fraud-management/fraud-detection.html. Retrieved September 26, 2021.

[247] The question is also whether or consent or legitimate interests shall serve as legal basis.

[248] Background information on the issue is provided by Jeff Jonas: Master Data Management vs. Sensemaking, Article published November 11 2011, available at http://jeffjonas.typepad.com/jeff_jonas/2011/11/master-data-management-mdm-vs-sensemaking.html. Retrieved September 26, 2021.

[249] Ann Cavoukian, Jeff Jonas: Privacy by design in the age of big data. Article published June 8 2012, available at https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf. Retrieved September 26, 2021.

accurate results. Rule-based Artificial Intelligence is the simplest form of AI[250]: knowledge is achieved by applying a set of rules.

2. Search and Planning Algorithms

In the age of Internet, probably the most prominent examples of Artificial Intelligence are algorithms that are used frequently to search for all kinds of goods, items, hints or suggestions. Search algorithms are very useful type of AI, but their problem-solving capacities can be limited depending on their ability to take constraints into account. That is why search algorithms are often combined with planning (and / or scheduling) algorithms.[251]

3. Symbolic Artificial Intelligence including Expert Systems

Symbolic Artificial Intelligence was the main area of interest in the early decades of AI research[252] and the first important step to design computers to assist humans in with complex decisions. This approach is also known as classical Artificial Intelligence and encompasses all AI methods that are based on symbolic, i.e. human-readable representations of problems, logic and search.[253] Since this type of AI helps experts in various professional domains to make their decisions, such symbolic AI systems are called Expert Systems. Expert Systems are knowledge repositories used to gather human expertise and to replicate that knowledge[254]. The first such system was already introduced in 1965.[255] Even though Symbolic Artificial Intelligence led to significant advances in the understanding of cognition, symbolic AI has fallen by the wayside as Neural Networks gained traction.[256]

[250] Background information on various types of Artificial Intelligence is provided by Tricentis in their article: AI Approaches Compared: Rule-Based Testing vs. Learning, available at https://www.tricentis.com/artificial-intelligence-software-testing/ai-approaches-rule-based-testing-vs-learning/. Retrieved September 26, 2021.

[251] Debby Nirwan: Using Forward-search algorithms to solve AI Planning Problems. Article published September 19 2020, available at https://ai.plainenglish.io/using-forward-search-algorithms-to-solve-ai-planning-problems-361ad4910239. Retrieved September 26, 2021.

[252] Ranjeet Singh: The Rise and Fall of Symbolic AI. Article published September 14 2019, available at https://towardsdatascience.com/rise-and-fall-of-symbolic-ai-6b7abd2420f2. Retrieved September 26, 2021.

[253] Eleni Ilkoua, Maria Koutrakia provide background information on Symbolic AI in their 2020 paper: Symbolic vs. Sub-symbolic AI Methods: Friends or Enemies? Proceedings of the CIKM 2020 Workshops, October 19-20, Galway, Ireland. The paper is available at http://ceur-ws.org/Vol-2699/paper06.pdf. Retrieved September 26, 2021.

[254] Indranil Das: How To Implement Expert System in Artificial Intelligence? Article published September 18 2019, available at https://www.edureka.co/blog/expert-system-in-artificial-intelligence/#ExpertSystemInArtificialIntelligence. Retrieved September 26, 2021.

[255] The first Expert System that used AI to solve problems within a specialized domain that normally requires human expertise was developed in Stanford by Edward Feigenbaum and others, source: https://entitledopinions.stanford.edu/edward-feigenbaum-artificial-intelligence. Retrieved September 26, 2021.

[256] Sebastian Bader, Pascal Hitzler explain the differences of Symbolic AI and Neural Networks: Dimensions of Neural-symbolic Integration - A Structured Survey. Article published November 10 2005, available at https://arxiv.org/pdf/cs/0511042.pdf. Retrieved September 26, 2021.

4. Knowledge Engineering

Knowledge Engineering is a field of Artificial Intelligence that aims at imitating the way humans think and approach problems; Knowledge Engineering is used in decision support software and similar to Expert Systems[257], it imitates the judgment of human experts by codifying knowledge as rules and relationships between data,[258] but is specific insofar as it tries to provide solutions for today's information explosion: e.g., in the area of taxation[259], it is hard to keep pace with ever-changing rules and regulations. This is a where Knowledge Engineering could help by using various algorithms, from Natural Language Processing to interpret laws to graph representations to find the relationships of new rules to previous instances. However, a challenge in the field of Knowledge Engineering is the capture of tacit knowledge[260]: it was soon discovered that human experts also rely on collateral data and that the interaction between explicit and tacit knowledge is vital for the creation of new knowledge.

5. Robotics

Robotics are used in various domains: they can be used in the industry to handle material, they can be used in the medical sector able to perform complex surgeries, and they can be used or for exploration purposes or even for the military as robots (including drones) can reach inaccessible, hazardous zones or to identify and destroy life-threatening objects. Especially these military use cases show the ethical implications of certain types of Artificial Intelligence; data protection is a lesser issue here, and there are further legal issues, for example the handling of machine data, non-personal information, data ownership or questions of own legal personality. It can be generally said that Robotics heavily rely on electrical and mechanical engineering and given the fact that robots in many industrial use cases must be capable of using vision to locate and assemble goods, advances in Robotics will very likely rely on progress in the field of Computer Vision and other forms of machine perception:

[257] Background information can be found in "The Journal of Knowledge Engineering" which publishes papers on various aspects of Knowledge Engineering, including Expert Systems, source: https://web.archive.org/web/20080612045810/http://www.blackwellpublishing.com/journal.asp?ref=0266-4720&site=1. Retrieved September 26, 2021.

[258] Michael Radwin: Knowledge Engineering demystified, expert paper for the Future of Privacy Forum issued February 8 2021.

[259] Gang Wang: Tech Talk: Intuit's AI-Powered Tax Knowledge Engine Boosts Filers' Confidence. Article published March 6 2019, available at https://www.intuit.com/blog/social-responsibility/tech-talk-intuits-ai-powered-tax-knowledge-engine-boosts-filers-confidence/?q=knowledge+engineering++taxation&qs=n&form=QBRE&sp=-1&pq=knowledge+engineering+taxation&sc=0-30&sk=&cvid=C86F17EA921A4662B0AEE8187B558298. Retrieved September 26, 2021.

[260] Dag Prawitz: Tacit Knowlege - an Impediment for AI? in: Göranzon et al.: Artifical Intelligence, Culture and Language: On Education and Work. The Springer Series on Artificial Intelligence and Society. Springer Verlag Berlin Heidelberg 1990, available at https://doi.org/10.1007/978-1-4471-1729-2_7. Retrieved September 26, 2021.

6. Computer Sensing and Vision

Another form of Artificial Intelligence is Computer Sensing where computers are designed with a range of sensors to enable them to see, listen or taste to assess their environment and, e.g., measure distance or acceleration and speed, temperature as well as light. This type of AI is thus used for augmented machine perception, and at present, Computer Vision is probably the most prominent form of Computer Sensing: computers are able to perform certain tasks like image and video captioning much better than humans could, and far beyond human perception[261]. Owing to the fact that the application domains of this type of AI include biometrics and face recognition[262], Computer Vision is one of the most problematic forms of Artificial Intelligence from a privacy perspective: while promising medical advancements seem possible by iris diagnostics with the help of AI which even go beyond diagnosing mere ocular diseases,[263] the same AI could cause serious challenges when used in a different setting, for example in the area of augmented reality in the employment context, allowing for the collection of employees' biometric and health data. Computer Vision is also one of the most challenging disciplines from a technical point of view, and that is why Computer Sensing is often combined with other types of AI, including rule-based and symbolic Artificial Intelligence as well as so-called Machine Learning:

7. Machine Learning

The emergence of Machine Learning (ML) is the reason why millions of users globally enjoy their smart devices and specialized (fitness, banking, weather, etc.) apps without really being able to tell what this type of AI is about. In fact, many people use the terms Machine Learning and Artificial Intelligence interchangeably. But ML is a new form of AI that can be distinguished from traditional Artificial Intelligence since it gives computers the ability to learn from and improve with experience by focusing on learning through patterns and building rules a from examples.[264] Some describe AI as

[261] Stanford University: One Hundred Year Study on AI (AI100) 2016, Report published September 2021, available at https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf. Retrieved September 26, 2021.

[262] Facial and character recognition techniques generally have a potential for bias and discrimination, and the ClearView case showed how easy it has become to use a single piece of information to identify and track individuals: the company scraped more than three billion facial images from social media sites. The scope of the matter and the lack of legal basis cause the European Commission to consult with national data protection authorities on how to proceed in the case: Samuel Stolton: After Clearview AI scandal, Commission 'in close contact' with EU data authorities. Article published February 12 2020, available at https://www.euractiv.com/section/digital/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/. Retrieved September 26, 2021.

[263] Ursula Schmidt-Erfurth, Amir Sadeghipour, Bianca Gerendas, Sebastian Waldstein, Hrvoje Bogunović: Artificial intelligence in retina. Article published August 1 2018, available at https://pubmed.ncbi.nlm.nih.gov/30076935/. Retrieved September 26, 2021.

[264] Ben Dickson: Why the difference between AI and machine learning matters. Article published October 8 2018, available at https://bdtechtalks.com/2018/10/08/artificial-intelligence-vs-machine-learning/. Retrieved September 26, 2021.

the intelligence and Machine Learning as the implementation of the compute methods which support it.[265] One could therefore speak of Machine Learning as the art of having computers perform without being programmed in a specific way.[266] Introduced in 2014[267], so-called Generative Adversarial Networks (GANs) are the newest variation of Machine Learning: two neural networks contest with each other, i.e. the second neural network (discriminator) evaluates the other network (generator) in a game to create and refine data (results).

8. Supervised and Unsupervised Learning

Machine Learning can be roughly separated into supervised and unsupervised (predicted) learning[268] as there are several ways to train algorithms: in a supervised learning model, the algorithm is provided with and learns from a labeled dataset for which the correct outcome is provided so that the network can learn to map inputs to observations and make necessary adjustments to learn for the future. An unsupervised model works with no or minimal human supervision and computers must look for patterns within an unlabeled (unclassified) dataset. Another name for unsupervised learning is knowledge discovery because unsupervised learning is used to find hidden patterns. Between these two main methodological types of Machine Learning lies so-called semi-supervised learning where a system is provided with a small set of labeled examples, and also uses unlabeled information within the same dataset for evaluation and analyzing purposes.

9. Reinforcement Learning

Alongside with supervised learning and unsupervised learning, Reinforcement Learning is one of three basic Machine Learning paradigms and has been around for some time already: Reinforcement Learning is built on observation[269] to allow for making optimal decisions and complete tasks within an uncertain environment using experiences. The focus of Reinforcement Learning is thus rather experience-driven decision-making than pattern recognition[270]: Reinforcement Learning aims at

[265] Statement provided by Intel's head of machine learning, Nidhi Chappell, quoted in Lee Bell's article: Machine learning versus AI: what's the difference? Article published December 1 2016, available at https://www.wired.co.uk/article/machine-learning-ai-explained. Retrieved September 26, 2021.

[266] UK House of Lords 2018 report on AI: AI in the UK: ready, willing and able?, The text is available at https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf. Retrieved September 26, 2021.

[267] Ian Goodfellow et al.: Generative Adversarial Networks, Proceedings of the International Conference on Neural Information Processing Systems (NIPS 2014), pp. 2672–2680, available at https://papers.nips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf. Retrieved September 26, 2021.

[268] Isha Salian: SuperVize Me: What's the Difference Between Supervised, Unsupervised, Semi-Supervised and Reinforcement Learning? Article published August 2 2018, available at https://blogs.nvidia.com/blog/2018/08/02/supervised-unsupervised-learning/. Retrieved September 26, 2021.

[269] Diana Borsa, Bilal Piot, Rémi Munos, Olivier Pietquin: Observational Learning by Reinforcement Learning. Article published June 20, 2017, available at https://arxiv.org/abs/1706.06617. Retrieved September 26, 2021.

[270] Stanford University: One Hundred Year Study on Artificial Intelligence (AI100), Report published September 2021, available at

independent learning and performance of human-like goal-oriented tasks. There are more and more practical use cases in this area, and it is likely that Reinforcement Learning will play a vital role in future Robotics.

10. Neural (Connectionist) Networks

An Artificial Neural Network (ANN) is inspired by the idea of imitating the human brain: computers are built in a manner suggestive of the connections between neurons in a human brain by using silicon and wires which act similar as dendrites and neurons:[271] Neural Networks use processors which are interconnected and are able to learn by a process of trial and error. One of the pioneers in this area defined a neural network as a computing system made up of a number of simple but highly interconnected processing elements that process information by their dynamic state response to external inputs.[272] The emergence of Artificial Neural Networks was a crucial aspect for the advancement of Artificial Intelligence.

11. Deep Learning

Deep Learning is part of Machine Learning[273] and uses Neural Networks that work with artificial neurons.[274] This area of Artificial Intelligence uses Neural Networks that are layered in a manner that allows for interaction between input and output values, i.e., passing back and forth input and output data with the help of mathematical functions so that new information is generated. This type of processing has helped with object and activity recognition and enabled progress in specific areas of perception, e.g., audio or speech.[275]

https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf. Retrieved September 26, 2021.

[271] Background information about ANN is provided by Oludare Abiodun et. Al: State-of-the-art in artificial neural network applications: A survey, Heliyon, Vol. 4, Issue 11 2018, available at https://www.sciencedirect.com/science/article/pii/S2405844018332067. Retrieved September 26, 2021.

[272] On July 1 2019, The University of California at San Diego published an article about the life-time achievements of Dr. Hecht-Nielsen. The article is available at https://qi.ucsd.edu/news-article.php?id=3089. Retrieved September 26, 2021. Dr. Hecht-Nielsen authored the first textbook on the subject, Neurocomputing, in 1989 (see https://www.semanticscholar.org/paper/Theory-of-the-backpropagation-neural-network-Hecht-Nielsen/f4457792a247c0eb6c6fb11a1d92f6f45b82acc1 for details).

[273] Connor Shorten: Machine Learning vs. Deep Learning. Article published on September 7 2018, available at https://towardsdatascience.com/machine-learning-vs-deep-learning-62137a1c9842. Retrieved September 26, 2021.

[274] Nagesh Singh Chauhan: Introduction to artificial neural networks. Article published October 13, 2019, available at https://towardsdatascience.com/introduction-to-artificial-neural-networks-ann-1aea15775ef9. Retrieved September 26, 2021.

[275] Stanford University: One Hundred Year Study on Artificial Intelligence (AI100). Report published September 2021, available at https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf. Retrieved September 26, 2021.

12. Natural Language Processing

Natural Language Processing (NLP) which is often combined with automatic speech recognition is one of the most common forms of Artificial Intelligence: "*Siri*", "*Alexa*", "*Cortana*" are prominent examples of (home-based) assistants, and the growing Internet connectivity of devices and appliances (Internet of Things) will further reinforce this. "*Google Translate*" and "*DeepL*" are good examples of how far machine translation has come in the recent years, and this also demonstrates that AI has become part of people's everyday life. The shift in NLP is to move away from systems that allow for real-time interaction with, e.g., customers to genuine dialogue.

The above-mentioned instances do not represent an exhaustive description of all types of Artificial Intelligence. To summarize the above enumeration to a certain degree, below is an overview of the most used types of Artificial Intelligence:[276]

Symbolic AI	Human-readable logic problems
Rule-based AI	Deductions based on curated rules
Search	Steps from initial state to goal
Planning & Scheduling	Multi-dimensional strategies and action sequences
Computer Sensing	Using human sense-based inputs
Robotics	Mobile AI and multi-sensing
Expert Systems	Complex solutions through reasoning
Knowledge Engineering	Technology behind expert systems
Machine Learning	Improvements through experience
Deep Learning	Using multiple layers of neural networks
Reinforcement Learning	Learning to a complex task
Natural Language Processing	Understanding and interpreting language
Neural Networks	Learning by making connections

IV. Use cases of Artificial Intelligence

There are countless use cases of Artificial Intelligence:[277]

[276] The overview is based on a document provided by Brenda Leong of the Future of Privacy Forum called "The spectrum of Artificial Intelligence". The infographic was published December 14, 2020 and is available at https://fpf.org/blog/the-spectrum-of-artificial-intelligence-an-infographic-tool/. Retrieved September 26, 2021.

[277] An overview on use cases is provided by BITKOM, the German Association for Information Technology, Telecommunications and New Media in their 2019 guideline: Konkrete Anwendungsfälle von KI & Big-Data in der Industrie. Report published 2019, available at https://www.bitkom.org/sites/default/files/2020-02/200203_lf_ki-in-der-industrie_0.pdf. Retrieved September 26, 2021.

Retail	Virtual mirrors, cashless stores
Mobile	Voice to text, smart personal assistants
Hospitality	Predictive supply chain, concierge services
Media	Automated journalism, identification of fake news
Insurance	Risk identification, client support, personalized pricing
Cyber-security	Incident detection and accelerated incident response
Gaming	Improved visual quality, 3D-Avatars, thought-controlled gaming
Education	Plagiarism detection, digital learning interfaces, virtual teachers
Banking & Finance	Fraud prevention, credit decision making, client segmentation
Smart homes	Personal assistants, home security, automated good ordering
Transport	Travel time reduction through traffic analytics, autonomous vehicle
Agriculture	Robot harvesting, computer vision to monitor soil health and needs
Real Estate	Market and price analysis, client segmentation, targeted advertising
Entertainment	Music and TV suggestions, search optimization, personalization
Defense	Target identification, autonomous weapons, simulations, training
Communications	Spam filters, real-time translation, emotion analysis, text suggestions
Online Shopping	Search recommendations, customer services and sales chat-bots
Social Networks	Photo recognition, chat-bots, friendship suggestions, personalization
Workplace	Robotics, automated checks in factories, enhanced recruitment
Healthcare	Virtual doctors, surgery robots, drug discovery, enhanced diagnostics
Politics & government	Targeted campaigning, public opinion monitoring, predictive policing

V. Benefits and challenges of Big Data and Artificial Intelligence

Big Data and AI applications are attractive for companies since allow for analytics, customer insights, forecasting, decision-making, and the optimization of processes, products, quality and services.[278] Big Data and AI can help to better understand market conditions and customer needs and such applications are therefore valuable for product development and overall innovation to achieve the desired competitive advantage; the same applies to necessary adjustments to reflect external and internal developments that can be better monitored with corresponding tools, even for reputation control.[279]

[278] Pricewaterhouse Cooper's 2021 AI Predictions Survey. Survey published October 2020, available at https://www.pwc.com/us/en/tech-effect/ai-analytics/ai-predictions.html. Retrieved September 26, 2021.

[279] Background information on why social media sentiment analysis is important is provided by New Generation Applications Ltd. in their August 29 2017 news, which is available at their website: https://www.newgenapps.com/blog/the-secret-way-of-measuring-customer-emotions-social-media-sentiment-analysis. Retrieved September 26, 2021.

From a company perspective, Big Data and AI are particularly useful for increasing productivity, managing inventory manufacturing, delivery and distribution and fostering preventive maintenance.[280] This technology can thus improve operational efficiency and optimize business outcomes.[281] Big Data and AI have proven to be valuable: so-called smart grids, traffic management as well as the medical sector as well as mobile and online applications are further important uses,[282] and based on existing experience thus far, it can generally be said that the use of Big Data and AI typically goes along with time reductions and cost savings.[283] In the last years, there has been an increased awareness with regards to these benefits, and this resulted in corresponding investments in the relevant infrastructure. Consequently, retail and insurance companies as well as financial institutions and governments use Big Data for various purposes, e.g., for the improvement and tailoring of products and services, for the assessment of churn rates, creditworthiness or other risks including detection of potential fraud and abuse, and they all follow their own Big Data value chain, from data collection to storage and analysis and the use of the results.[284] The maturation of Big Data and AI software was also an important factor for the growing success of such applications. It can therefore be concluded that Big Data and AI drive growth for those companies that know how to take advantage of "*data-driven decision-making*"[285] for their business. Conversely, the inability of an organization to benefit from the information it possesses can result in what is called "*enterprise amnesia*".[286]

Despite of the existing potentials of Big Data and Artificial Intelligence in terms of analytics, mining, reporting, simulation and visualization, it should not be forgotten that evaluations that are based on Big Data and AI do not automatically lead to correct or meaningful results: e.g., a correlation was proven between the rise in stock market prices and Superbowl results; the same applies to the correlation between the susceptibility of Angina Pectoris and the individuals with the zodiac sign

[280] Alexander Bekker provides a comprehensive overview over big data use cases in his article: Twenty Big Data Use Cases. Article published MAY 17 2021, available at https://www.experfy.com/blog/twenty-big-data-use-cases. Retrieved September 26, 2021.

[281] Further details are provided by Karsten Egetoft in his article: Data-Driven Analytics: Practical Use Cases For Financial Services. Article published available at https://www.digitalistmag.com/customer-experience/2019/01/29/data-driven-analytics-practical-use-cases-for-financial-services-06195123. Retrieved September 26, 2021.

[282] Omer Tene, Jules Polonetsky: Big data for all – privacy and user control in the age of analytics, Northwestern Journal of Technology and Intellectual Property, vol. 11, issue 5, pp. 245-250.

[283] Pricewaterhouse Cooper's 2021 AI Predictions Survey. Survey published October 2020, available at https://www.pwc.com/us/en/tech-effect/ai-analytics/ai-predictions.html. Retrieved September 26, 2021.

[284] International Working Group on Data Protection in Telecommunications: Working Paper on Big Data and Privacy principles under pressure in the age of Big Data analytics, p.18. WP published May 6 2014, available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2014/06052014_en.pdf. Retrieved September 26, 2021.

[285] Omer Tene, Jules Polonetsky: Big data for all – privacy and user control in the age of analytics, Northwestern Journal of Technology and Intellectual Property, vol. 11, issue 5, p. 243.
Jeff Kelly: Big Data Vendor Revenue and Market Forecast 2012-2017, available at http://wikibon.org/wiki/v/Big_Data_Revenue_and_Market_Forecast_2ß12-2017. Retrieved September 26, 2021.

[286] Ann Cavoukian, Jeff Jonas: Privacy by design in the age of big data. Article published June 8 2012, available at https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf. Retrieved September 26, 2021.

Aquarius.[287] It is difficult to capture meaningful results for algorithms as algorithms do not dispose of social skills[288] or the intuition to discard patterns if need be. This is especially true for behavioral analytics since human behavior is not only guided by reason, but often driven by emotions. To provide a very simple example, it cannot necessarily be assumed that the frequency of clicking on certain messages is in an indicator for their importance to the user.[289]

Furthermore, it can be discussed whether the cited benefits of Big Data and Artificial Intelligence for businesses are also benefits for the users whose data are concerned, as all uses entail potential disadvantages or even threats: health data management is valuable, but dependent on very sensitive data, and that is why any corresponding Big Data or AI application has to be thought through and dealt with great care. Traffic management is desirable but could lead to seamless tracking of motion patterns based on geo-location data; the same is true for data collected from mobile devices: there have been reports that operating systems are transmitting a lot of user data even if users deliberately switch off certain services such as location-based services.[290] So-called smart meters electricity suppliers started using some years ago are very useful for billing purposes. But smart meters are able to transmit power consumption levels within short intervals, and a result, suppliers have detailed information about the intensity of the usage of household devices – sensors work so precisely that they can even capture which TV channels have been watched.[291] Smart meters thus allow for a detailed at customer usage behavior, and that implies a considerable risk for privacy.[292] In addition, smart meters are also a good example for unexpected results, another possible characteristic of Big Data – and secondary use of personal information in privacy terms: consumption data clearly show whether and how many people have been present in certain premises for a certain period of time. Therefore, smart meter data could be used in tax matters and may serve as evidence if a taxable (primary) residence is in question.

Big Data and Artificial Intelligence can generally only create value if the delivered results and conclusions are meaningful. However, the problem is that any decision-making process is based and dependent on a high number of other, underlying decisions, and that makes the process vulnerable to

[287] Mario Martini: Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz in: Hill/Martini/Wagner: Die digitale Lebenswelt gestalten, Baden-Baden 2015, pp. 99-169.

[288] Niko Härting: Internetrecht, Dr. Otto Schmidt publishing Cologne, fifth edition 2014, p. 626.

[289] Niko Härting: Internetrecht, Dr. Otto Schmidt publishing Cologne, fifth edition 2014, p. 627.

[290] A corresponding study was conducted by Douglas C. Schmidt: Google Data Collection, Article published August 2018, available at https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf. Retrieved September 26, 2021.

[291] Researchers recently confirmed this result in the framework of the Data Privacy Management project (DaPriM) funded by the federal government. They summarized their findings in a working paper which was published in 2011: Hintergrund und experimentelle Ergebnisse zum Thema,, Smart Meter und Datenschutz, Münster University of Applied Sciences, available at http://1lab.de/pub/smartmeter_sep11_v06.pdf. Retrieved September 26, 2021.

[292] Jens-Matthias Bohli, Christoph Sorge and Osman Ugus offer an overview on the problem in their 2010 paper: A Privacy Model for Smart Metering, 2010 IEEE International Conference on Communications Workshops, Capetown, 2010, pp. 1-5.

errors which vary in complexity, their consequences and in the extent to which they can be influenced. It is important to note that various errors can occur in every single phase of the design and decision process:[293] errors can already occur during the design phase of algorithms or when the automatic decision-making system is constructed; operationalization errors can lead to results which cannot be interpreted in a meaningful manner. Finally, errors may occur when users fail to recognize poor data and/or when they misinterpret results.

The factual challenge is that, on top of a multitude of legal questions that arise when Big Data and Artificial Intelligence are in question, there is a high potential for failure as every single phase of the automatic decision-making process is theoretically error-prone: even correct data may lead to wrong decisions, because users' conclusions may be wrong, and because users can influence results by the way the dataset is defined or by the way the algorithm is written.[294] After all, decision-making with the help of Big Data and AI in many cases still means interpretation of results by individuals, and this is where (human) mistakes come into play. In this context, it is important to note that some authors[295] claim that next generation smart information management systems can reduce false positives and false negatives because they are able to deal with plausible variations and that context-accumulating systems will automatically determine if new observations reveal something of sufficient interest to provoke a reaction rather than data scientists asking questions to the system. Businesses will for sure welcome such developments, but from a data protection perspective, privacy-enhancing elements and responsible innovation should be underlined in order to prevent privacy harms for individuals.

VI. Potential risks of Big Data and Artificial Intelligence

1. Data aggregation and maximization

Since Big Data lives on processing of large and growing datasets, the principle of data minimization as set forth in GDPR Article 5 (1) lit. c may well be affected since Big Data is about turning volume to

[293] Katharina Zweig, Sarah Fischer, Konrad Lischka: Wo Maschinen irren können – Verantwortlichkeiten und Fehlerquellen in Prozessen algorithmischer Entscheidungsfindung, Bertelsmann Stiftung Gütersloh, pp. 21-28. Report published February 2018, available at https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/WoMaschinenIrrenKoennen.pdf. Retrieved September 26, 2021.

[294] Omer Tene, Jules Polonetsky: Big data for all – privacy and user control in the age of analytics, Northwestern Journal of Technology and Intellectual Property, vol. 11, issue 5, pp. 239, available at https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Retrieved September 26, 2021.

[295] Lisa Sokol and Jeff Jonas: Data finds data in: Beautiful Data – the stories behind elegant data solutions by Toby Segeran and Jeff Hammerbacher, O'Reilly Media 2009. The introduction of the above-quoted chapter Lisa Sokol and Jeff Jonas wrote is available at https://jeffjonas.typepad.com/jeff_jonas/2009/07/data-finds-data.html. Retrieved September 26, 2021.

value.[296] Fact is that more and more data is being generated and processed: 2.5 quintillion bytes of data are created each day, and that pace is accelerating with the growth of the Internet of Things.[297] Big Data and AI are on the rise: 77 percent of the devices we use today feature one form of AI or another; owing to AI, global GDP may grow to $ 15 trillion by 2030 and the overall AI market is expected to be almost $ 60 billion by 2025.[298] In the next ten years, almost 70 percent of all companies will adopt at least one type of AI.[299] AI's potential is so broad that some speak of it as the fourth industrial revolution.[300]

2. Secondary use and use of collateral data

(Compatible) reuse of personal data is admissible[301] to the extent the conditions of GDPR Article 6 (4) are met,[302] i.e. considering the nature of the data in question, the context in which the data were collected, the relationship between the purposes for which the data have been collected and the purposes of further processing, the impact of the envisaged data processing on the data subjects, and the safeguards applied by the controller. Since a major characteristic of many AI applications is a certain degree of autonomy with systems being able to perform in an unsupervised manner, it is questionable whether such data processing operations meet all these requirements. Another problem of Big Data applications is that, quite often, external data are processed. The upload of address books to social media platforms is a simple, but good example of this risk: whenever a user uploads his individual contacts to a social media platform, the platform receives a full set of contact data, and the concerned individuals behind those data do not know anything about this, not to mention that they never consented to such information sharing. This type of data processing is not transparent and can

[296] Nikolaus Forgo et al.: The principle of purpose limitation in Big Data in: Marcelo Corales, Mark Fernwick, Nikolaus Forgo (eds.): New Technology, Big Data and the Law, Springer Publishing 2017, p.21.

[297] Bernard Marr: How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. Article published on May 21, 2018, available at https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#2152235f60ba. Retrieved October 22, 2021.

[298] "AI Statistics About Smarter Machines" – figures presented by Techjury on January 28, 2019 in their blog which is available at https://techjury.net/stats-about/ai/. Retrieved October 22, 2021.

[299] McKinsey Global Institute: Notes from the AI Frontier – Modeling the Impact of AI on the World Economy. Discussion paper issued in September 2018, available at https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/MGI-Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economy-September-2018.ashx. Retrieved October 22, 2021.

[300] EDPS: EU Guidelines on Ethics in Artificial Intelligence, p. 2, available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf, Retrieved October 22, 2021.

[301] Article 6 of the former EU Data Protection Directive was also stressing compatibility, and according to the United Nations Guidelines Concerning Computerized Personal Data Files, personal data collected must remain relevant and adequate to the purposes specified at the time the data was collected. The Guidelines are available at https://www.refworld.org/pdfid/3ddcafaac.pdf. Retrieved October 22, 2021.

[302] The Directive on open data and the re-use of public sector information provides the legal framework for government-held data (public sector information), available at https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information. Retrieved October 22, 2021.

hardly be considered lawful: it is true that users upload the data; the platform was not actively collecting or harvesting data, but the platform as the controller acted as an enabler since it was the platform which implemented and activated the corresponding functionality – while another useful feature, (at least) information of concerned data subjects through communication channels the platform can dispose of, is not a default. However, some platforms used e-mail addresses which were uploaded by other users for other (own) purposes, which courts considered to be illegal advertising.[303] Mergers & acquisitions are also a typical example of how companies may end up breaching data protection[304] (and/or consumer protection, competition or anti-trust) laws.

3. Opaqueness

One problem in the field of AI is that quite often, quite important factors are unknown, e.g., details of the processing, the decisive (set of) operators behind the algorithm, etc. Some argue that there are three distinct types of opaqueness which can be distinguished:[305] intentional opacity when the inner workings of the system are deliberately concealed; illiterate opacity when the inner workings are opaque since only those with expert knowledge understand how it works; intrinsic opacity due to a fundamental mismatch between how humans and how algorithms understand the world. The ability of AI to act autonomously and in unforeseeable ways adds to the fear that decisions about individuals may made by a "*Kafkaesque system of unreviewable decision-makers*".[306] Another imminent problem is that the outcome of AI applications is based on statistical correlations, not causality, and that is why some believe that AI shall attempt to identify causal relationships.[307] Interestingly, even companies

[303] On January 14, 2016, the German Federal Supreme Court has ruled that the "find friends" feature of Facebook, which is also used to email people who are not registered on Facebook, constitutes unlawful (harassing) advertising: decision Az. I ZR 65/1, available at http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=73328&linked=pm. Retrieved October 22, 2021.

[304] As regards the transfer of data from WhatsApp to Facebook, the administrative court in Hamburg ruled that Facebook Germany must not use personal information from WhatsApp users. Due to the fact that Facebook provided incorrect information about (the possibility of) linking WhatsApp phone numbers to Facebook accounts, the company was fined 110 million euros by the European Commission: news entry published May 18 2017 in Zeit online: Übernahme von WhatsApp: Facebook muss 110 Millionen Euro Strafe zahlen: https://www.zeit.de/digital/datenschutz/2017-05/datenschutz-facebook-whatsapp-uebernahme-eu-kommission-strafe. M & As have already been subject to national fines: press release of the Bavarian SA published August 30 2015, available at https://www.lda.bayern.de/media/pm2015_10.pdf. Retrieved October 22, 2021.

[305] Jenna Burrell How the machine 'thinks': Understanding opacity in machine learning algorithms, Big Data & Society 2016, pp. 1-12, available at https://doi.org/10.1177/2053951715622512. Retrieved October 22, 2021.

[306] Neil Richards and Jonathan King: Three Paradoxes of Big Data, Stanford Law Review Online 2013, vol. 66:41, p. 42, available at http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big-data (Retrieved October 22, 2021). The autors quote Daniel Solove who uses the term Kafkaesque in his book "The digital person: Technology and Privacy in the Information Age" NYU Press 2004.

[307] Matt Kusner, Joshua Loftus, Chris Russell, Ricardo Silva: Counterfactual Fairness, presented and published at the 31st Conference on Neural Information Processing Systems (NIPS 2017), available at https://papers.nips.cc/paper/6995-counterfactual-fairness.pdf. Retrieved October 22, 2021.

engaged in the "*fight against black box algorithms*"[308] with a new set of open source software to help understand how Artificial Intelligence is making decisions.

4. Human oversight

A variety of factors contribute to the problem that human oversight is an issue in the framework of Big Data, ADM and AI applications: the specialty about AI is that systems are able to autonomously perform certain tasks to achieve specific goals,[309] that they can recognize meanings by extracting characteristics and patterns[310] and learn (and teach) themselves without being programmed in a specific way. Processing operations may therefore lead to decisions which are opaque since they lack transparency and reproducibility, and that also questions the fairness and reliability of results which may be incorrect or even inappropriate (biased). If data is merged from various datasets, traceability is yet another issue to consider which conflicts with controllers' accountability.[311] A worst case scenario would be that unknown (secret) processing takes place and that the controller lost control or is simply not aware of what is going on. The fact that many services are outsourced to a multitude of specialized vendors further contributes to the potential risk that human oversight may be threatened; in many cases, it may therefore be difficult to define the true operators.

5. Information mismatch

Companies must be transparent about the processing of personal data,[312] but they are not obliged to provide detailed information about the data processing. For example, GDPR Article 13 (2) lit. f limits the transparency obligation to information about "*the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*". Details about the significance as well as envisaged consequences of the processing are relative insofar as dynamic processing may perhaps not allow for

[308] IBM introduced a "Fairness 360 Kit" to help AI developers to see inside their AI creations via a set of dashboards: Introducing AI Fairness 360, published in IBM's Research Blog on September 19 2018, available at https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/. Retrieved October 22, 2021.

[309] European Commission's 2018 factsheet on Artificial Intelligence, available at https://ec.europa.eu/digital-.single-market/en/artificial-intelligence. Retrieved October 23, 2021.

[310] Isha Salian: SuperVize Me: What's the difference between supervised, unsupervised, semi-supervised and reinforcement learning? Article published on August 2, 2018, available at https://blogs.nvidia.com/blog/2018/08/02/supervised-unsupervised-learning/. Retrieved October 23, 2021.

[311] See GDPR Article 5 (2).

[312] GDPR Article 12, 13, 14. See also the new California Consumer Privacy Act (CCPA), which creates new consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses. Background information on CCPA can be found on the website of the State of California Department of Justice, Office of the Attorney General at https://oag.ca.gov/privacy/ccpa. Retrieved October 23, 2021.

foreseeing all relevant consequences.[313] Details about the underlying logic are relative insofar as meaningful information is not the same as comprehensibility or reproducibility of decisions and insofar as businesses may refer to trade secrets in order not to disclose underlying algorithms they use.[314] Another point that adds to the mismatch is the dilemma of information asymmetry between users and (Internet) service providers.[315]

6. Privacy self-management

Lack of transparency is also related to data subject rights: there is good reason why GDPR Article 12 covers both, transparent information and modalities for the exercise of data subject rights, because being aware who holds which data is a prerequisite for exercising individual rights. GDPR stresses the right to information in the framework of multi-purpose processing since GDPR Article 13 (3) requires that individuals be (repeatedly) informed if the controller "*intends to further process personal data for a purpose other than that for which the personal data were collected*". A draft version of the ePrivacy Regulation pursues the same goal by introducing the duty to remind users of their right to withdraw their consent unless users decide not to receive such reminders.[316] Information requirements are not only common to European law but are also part of so-called Fair Information Practice Principles (FIPP) which have been adopted in many US-laws.[317] FIPPs and many other privacy frameworks[318] have in common that individuals must be able to know which information is held about them and correct records of personal information if need be. Even if lack of transparency is not the problem, transparency as such is problematic since the ineffectiveness of transparency requirements seems to be proven by now: people are as badly informed as they are overtaxed with long and complex privacy

[313] Whenever processing operations are subject to ongoing change, data protection risk assessments will be an ongoing process, and not a one-time exercise, Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of Regulation 2016/679 (WP 248), p. 13.

[314] German SCHUFA, one of the countries' leading credit agencies that bases its decisions on scoring successfully filed a law suit: the German Federal High Court of Justice ruled in 2014 that SCHUFA cannot be forced to explain in detail how scores are determined: Gerrit Hornung reports on the decision in his article: Datenverarbeitung der Mächtigen bleibt intransparent, published January 19 2014, available at https://www.lto.de/recht/hintergruende/h/bgh-urteil-vizr15613-schufa-scoring-ermittlung-kreditwuerdigkeit-algorithmus-geschaeftsgeheimnis-auskunft/. Retrieved October 23, 2021.

[315] Masooda N Bashir, Carol Hayes, April D. Lambert, Jay P Kesan: Online privacy and informed consent: The dilemma of information asymmetry, Proceedings of the Association for Information Science and Technology 2015, vol. 52, issue 1, pp. 1-10, available at https://doi.org/10.1002/pra2.2015.145052010043.

[316] Kristof Van Quathem: New Draft ePrivacy Regulation Released. Article published October 14, 2019, available at https://www.insideprivacy.com/international/european-union/new-draft-eprivacy-regulation-released/. Retrieved October 23, 2021.

[317] Omer Tene, Jules Polonetsky: Big Data for All – Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property 2013, vol. 11, issue 5, p. 242.

[318] For example Paragraph 12 and 13 of OECD's Privacy Guidelines, which are available at https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf or Principle 23 of APEC's Privacy Framework (which are available at https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework). Retrieved October 23, 2021.

notices;[319] people routinely turn over their data for small benefits;[320] people care much more about price-sensitive information than about data protection information;[321] people are much more concerned about social privacy than about institutional privacy,[322] and if people are about to decide about their privacy preferences, they tend to make their lives easy and accept all default settings[323] rather than taking their time to really comprehend and decide on relevant settings. Even worse, certain Apps take advantage of psychological (behavioral) patterns[324] that can reinforce loss of user control.[325]

7. Increase of paradoxes

There is much enthusiasm around Big Data as it is believed to be a powerful tool which enables detailed insight into many different economically valuable aspects of life. However, this seems to be only true for Big Data users since Big Data applications, pools and sensors are predominantly in the hands of powerful intermediary institutions, meaning that large corporate entities[326] are privileged at the expense of individuals.[327] This "*power paradox*" is accompanied by the "*transparency paradox*": Big Data lives on small data inputs which, when viewed in isolation, appear unimportant and unsuspicious. The problem is that especially online data collection is much more far reaching and much more detailed than users would expect, and that underlying tools and techniques that are used for decision-making are opaque.[328] Therefore, some compare interactions with Big Data platforms with a poker game "*where one of the players has his hand open and the other keeps his cards*

[319] Fred Cate, Viktor Mayer-Schönberger: Notice and consent in a world of Big Data, International Data Privacy Law 2013, vol. 3, no. 2, p. 67.

[320] Daniel Solove: Introduction: Privacy self-management and the consent dilemma, Harward Law Review 2013, vol. 126:1880, p. 1886.

[321] Daniel Solove: Introduction: Privacy self-management and the consent dilemma, Harward Law Review 2013, vol. 126:1880, p. 1898.

[322] Alison Young, Anabel Quan-Haase: Privacy protection strategies on Facebook – the Internet privacy paradox revisited, Information, Communication & Society 2013, p. 201.

[323] Lokke Moerel summarizes situations in which people are least likely to make good choices in: Big Data protection – how to make the draft EU future proof. Tilburg University press, Tilburg 2014, p. 48, available at https://pure.uvt.nl/ws/portalfiles/portal/2837675/oratie_Lokke_Moerel.pdf. Retrieved October 23, 2021.

[324] Nancy Cheever, Larry Rosenblatt, Mark Carrier and Amber Chavez: Out of sight is not out of mind: The impact of restricting wireless mobile device use on anxiety levels among low, moderate and high users, Computers in Human Behavior 2014, vol. 37, pp. 290-297.

[325] Sometimes even to the point of addiction, see Jan-Keno Janssen, Sylvester Tremmel: Die Psycho-Tricks der App-Entwickler. Article published October 15 2019, available at https://www.heise.de/ct/artikel/Die-Psycho-Tricks-der-App-Entwickler-4547123.html?seite=all. Retrieved October 23, 2021.

[326] Or governments: For instance, the Syrian government lifted restrictions on the usage of Facebook, Twitter, and the like only to secretly profile, track, or even round up dissidents: Stephan Faris, The Hackers of Damascus, Bloomberg Businessweek, article published November 14 2012, available at http://www.businessweek.com/articles/2012-11-15/the-hackers-of-damascus. Retrieved October 23, 2021.

[327] Some authors call this the power paradox, see Neil Richards and Jonathan King: Three Paradoxes of Big Data, Stanford Law Review Online 2013, Vol. 66:41, p. 44. Article published September 3 2013, available at http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big-data. Retrieved October 23, 2021.

[328] Cookie information practices are a prominent example: often available, but rarely meaningful.

close".[329] *Transparency is a topic GDPR explicitly stresses,*[330] but transparency and consent seem to be an unfortunate issue since privacy self-management in many instances is about a take-it-or-leave-it-approach[331] or a mere click-mechanism.[332] Even though the Court of Justice of the European Union clarified some questions regarding the use of cookies,[333] and the ePrivacy Regulation is yet to come[334] so that there is still a lack of clarity with regard to consent requirements.[335] The described phenomenon is summarized under the term "*control paradox*" which also deals with the problem that affording more control to users does not help them to better protect their privacy.[336] The opposite effect is true:[337] not only does affording more control to users not lead to better protection of their data – this may even induce them to reveal more sensitive information: if people feel that they have control over their data, they tend to provide more data about themselves.[338] Similar effects are known from other fields, e.g., in the framework of the introduction of the safety belt legislation: people felt more secure with safety belts and drove less carefully.[339] Another effect may be described as the "*trust paradox*": people are nowadays so used to relying on all kinds of Apps as "*single source of truth*" that they there does not seem to be any more room left for own decision making,[340] and that has a direct impact on how we deal with both, our own responsibility and others' trustworthiness in the event that an App's decision is challenged.

[329] Omer Tene, Jules Polonetsky: Big Data for All – Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property 2013, vol. 11, issue 5, p. 255.

[330] GDPR Article 5 (1) lit. a.

[331] Giovanni Buttarelli: We need to talk about terms and conditions. Article published April 29 2019, available at https://edps.europa.eu/press-publications/press-news/blog/we-need-talk-about-terms-and-conditions_en. Retrieved October 23, 2021.

[332] Daniel Solove discussed the issue in his publication: Privacy Self-Management and the Consent Dilemma, Harvard Law Review 2013, pp. 1880-1903.

[333] The court ruled that storing cookies requires internet users' active consent. The corresponding press release is available at https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125en.pdf. Retrieved October 23, 2021.

[334] Nicloas Herrmann: ePrivacy-Verordnung in der Krise – Die Suche nach einem Plan B. Article published November 25 2019, available at https://www.datenschutzbeauftragter-info.de/eprivacy-verordnung-in-der-krise-die-suche-nach-einem-plan-b/. Retrieved October 23, 2021.

[335] The draft ePrivacy Regulation faced much criticism: Ingo Dachwitz and Alexander Fanta: EU-Staaten wollen Verlagen einen Blankoscheck für Online-Tracking gewähren. The article provides background information on the draft ePrivacy regulation. Article published November 18 2019, available at https://netzpolitik.org/2019/eu-staaten-wollen-verlagen-einen-blankoscheck-fuer-online-tracking-gewaehren/. Retrieved October 23, 2021.

[336] Lokke Moerel: Big Data protection – how to make the draft EU future proof. Tilburg University press, Tilburg 2014, p.46, available at https://pure.uvt.nl/ws/portalfiles/portal/2837675/oratie_Lokke_Moerel.pdf. Retrieved October 23, 2021.

[337] Susanne Barth, Menno de Jong: The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior: a systematic literature review. Journal of Telematics and Informatics, vol. 34, issue 7, pp. 1038-1058.

[338] Laura Brandimarte, Alessandro Acquisti, George Loewenstein: Misplaced Confidences – Privacy and the Control Paradox. Article published August 9 2012, available at http://www.futureofprivacy.org/wpcontent/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf. Retrieved October 23, 2021.

[339] Wiel Janssen: Seat-belt wearing and driving behavior – an instrumented-vehicle study. Accident Analysis and Prevention 1994, vol. 26, issue 2, p. 261. A summary of the study is available at http://www.ncbi.nlm.nih.gov/pubmed/8198694?dopt=Abstract. Retrieved October 23, 2021.

[340] Steven Tanimoto writes about how the loss of user responsibility is linked to users getting lazy and losing own problem-solving capacities when they trust "system judgments" in his 2010 book: The elements of Artificial Intelligence, Computer Science Press 2010, p. 478.

The control paradox goes hand in hand with the so-called "*security paradox*":[341] data protection and data security are inseparable, and that is why security measures such as access controls are principally indispensable from both, a controller and user perspective. But any such measures require the processing of log-in data, and the general risk is that the more data are processed, the larger the risks that data are somehow compromised. Depending on the case, only name and password are required, but more and more often, users are required to provide a fingerprint in the framework of the authentication process, and that may lead to severe risks: nowadays many devices require the use of biometric data,[342] but the problem is that, unlike a password, there is no reset process for a unique fingerprint, and what is worse: such data can be manipulated very easily.[343] For instance, access to a used object is sufficient to reproduce a fingerprint, and if fingerprints are a mandatory part of official ID-documents,[344] then the individual concerned has a serious problem when such data is abused. As a consequence, supposed security mechanisms themselves may lead to further risks. Even the COVID-19-pandemic is an example of such potential paradoxes when people "*give up private information (... and) weigh up the costs and benefits in a "Privacy Calculus*"."[345]

The paradox at implementation level is that, even if stakeholders are determined to comply with privacy standards, the introduction of an AI system may lead to privacy problems since there is a risk for potential trade-offs between different data protection principles. In this regard, the UK's Information Commissioner's Office[346] explains that such tensions may arise between accuracy and fairness vs. privacy, and fairness vs. accuracy as well as explicability vs. accuracy and security, e.g., more data may lead to more accuracy, but at the expense of individual's privacy; if AI is tailored to avoid discrimination (if certain indicators are removed to that AI is fair), this may have an impact on accuracy; if AI is tested to see if it may be discriminatory, it needs to be tested by using data that is labeled by protected characteristics, but that may be restricted under privacy laws that govern the processing of special category data; providing detailed explanations about the underlying logic of

[341] Lokke Moerel: Big Data protection – how to make the draft EU future proof. Tilburg University press, Tilburg 2014, p. 46, available at https://pure.uvt.nl/ws/portalfiles/portal/2837675/oratie_Lokke_Moerel.pdf. Retrieved October 23, 2021.

[342] Given the sensitivity of biometric data and the insufficiency of investigating alternatives, the Amsterdam District Court ruled that a company cannot require its employees to log in to the cash register system through fingerprint scanners. The decision is available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:6005. Retrieved October 23, 2021.

[343] An election poster of German chancellor Dr. Angela Merkel was enough to present how easily an iris scan can be manipulated: Stefan Krempl: CCC-Tüftler hackt Merkels Iris und von der Leyens Fingerabdruck. Article published December 28 2014, available at https://www.heise.de/security/meldung/31C3-CCC-Tueftler-hackt-Merkels-Iris-und-von-der-Leyens-Fingerabdruck-2506929.html. Retrieved October 23, 2021.

[344] The EU Commission proposed making fingerprints mandatory in ID cards, source: Reuters online news published April 17 2018, available at https://www.reuters.com/article/us-eu-security/eu-commission-proposes-making-fingerprints-mandatory-in-id-cards-idUSKBN1HO23A. Retrieved October 23, 2021.

[345] Paul Garrett et al: Privacy and health: the lesson of COVID-19. Article published February 4 2021, available at https://pursuit.unimelb.edu.au/articles/privacy-and-health-the-lessons-of-covid-19. Retrieved October 23, 2021.

[346] Reuben Binns, Valeria Gallo: Trade-offs. Article published July 25 2019, available at https://ico.org.uk/about-the-ico/news-and-events/ai-blog-trade-offs/. Retrieved October 23, 2021.

complex AI systems may lead to disclosure of information that can be used to infer private information about the individuals whose personal data was used to build the AI system.

8. (Re-)Identification and identity

Even though one single piece of information may not very telling,[347] combined datasets tell more about the person and enable to form a picture of the individual; therefore, aggregated information can reveal new facts about a person the individual did not expect to be known when the original (isolated) data was collected.[348] It is frightening to see how little information is needed to associate information to an individual: a study of credit card records showed that only four spatiotemporal points are enough to uniquely re-identify 90 percent of individuals and that knowing the price of the underlying transaction increases the risk of re-identification by 22 percent.[349] Identification of a person is not necessarily a risk, but if one thinks of the importance of the protection of witnesses[350] and whistleblowers[351] and the relevance of anonymous speech,[352] this shows that the issue of identification may be linked to fundamental rights. The predictive nature of Big Data applications may lead to individuals being identified, and the trouble in this regard is that individuals face difficulties to control the access and use of their personal data and that they thus do not have sufficient autonomy to determine, maintain and develop their identity.[353] Big Data and AI can make individuals' identities potentially more vulnerable, simply because more and more data is available, shared with service providers around the world, and stored in various tools – and any of these systems could be hacked, which may, e.g., enable identity theft. Identity[354] theft is a growing issue since advances in digital technology have aggravated the problem. Identity threats and the potential for discrimination are interconnected: in many instances, individuals can neither know nor influence the outcome of

[347] The recent Clearview case has already proven the opposite: the App can identify individuals based on a single photo. The German newspaper "Süddeutsche" called the case a "nightmare for privacy", a "software that shocks": Article by Jannis Brühl and Simon Hurtz published January 20 2020, available at https://www.sueddeutsche.de/digital/gesichtserkennung-clearview-app-polizei-gesicht-1.4764389. Retrieved October 23, 2021.

[348] Daniel Solove: Understanding Privacy, p. 118, Harvard University Press, Cambridge Massachusetts 2008.

[349] Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh, Alex Pentland: Unique in the shopping mall: On the reidentifiability of credit card metadata, Science 2015, vol. 347, issue 6221, pp. 536-539.

[350] And the related right not to incriminate oneself, a generally recognized international standard which is key part of a fair procedure: https://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf. Retrieved October 23, 2021.

[351] Recently, the Council of the European Union adapted new rules for the protection of whistleblowers. Press release published October 7 2019 and is available at https://www.consilium.europa.eu/en/press/press-releases/2019/10/07/better-protection-of-whistle-blowers-new-eu-wide-rules-to-kick-in-in-2021/ (Retrieved October 23, 2021). Member states will have two years to transpose the new rules into their national law.

[352] Daniel Solove: Understanding Privacy, p. 125, Harvard University Press, Cambridge Massachusetts 2008.

[353] Jacques Bus, Carolyn Nguyen: Personal Data Management – A Structured Discussion in: Mireille Hildebrandt, Kieron O'Hara, Michael Waidner, eds.: The value of personal data, Digital Enlightenment Yearbook, IOS Press Amsterdam, 2013, p. 272, available at https://www.academia.edu/6325541/Personal_Data_Management_A_Structured_Discussion. Retrieved October 23, 2021. Retrieved October 23, 2021.

[354] The term identity is used as a reference to the self and in the technical sense of the complete set of attributes that defines a person.

evaluations in relation to their preferences, performance or creditworthiness. Consequently, some authors address the problem[355] and some institutions call for a prohibition of so-called secret profiling.[356] The core problem is that the outcome of any such evaluation is based on correlations rather than causes,[357] and therefore, some speak about data protection as protection against probability.[358]

9. Potential for discrimination

The probabilistic nature of individual decision-making and profiling is highly desired, but their inherent opacity[359] together with their potential for discrimination[360] is problematic: price discrimination by online-shops is just one such example,[361] which can be judged from various perspectives, e.g., data protection and consumer protection as well as competition law.[362] There are far more examples for in-transparency in practice with much more impact on people's lives. One instance is that nowadays, employers may well turn down job candidates based on social media information without providing candidates with an opportunity to comment on their findings. A study[363] explains how important this trend has become: it showed that a Meta (formerly known as Facebook) profile is better at predicting job performance than an IQ test. Under the GDPR, any data subject has the right to request information and, under certain conditions, the right to object[364] "*on grounds relating to his or her particular situation*", but the key problem is that individuals unlike businesses do not dispose of enough information to defend themselves not just against the data processing as such (which may be

[355] Daniel Solove: Understanding Privacy, p.133, Harvard University Press, Cambridge Massachusetts 2008.

[356] For instance, the Universal Guidelines on AI issued 2018 by the Public Voice, available at https://thepublicvoice.org/ai-universal-guidelines/. Retrieved October 23, 2021.

[357] Mireille Hildebrandt: Slaves to Big Data. Or Are we? Keynote during the 9th Annual Conference on Internet, Law & Politics on June 25, 2013 in Barcelona, available at http://works.bepress.com/mireille_hildebrandt/52. Retrieved October 23, 2021.

[358] Lokke Moerel: Big Data protection: How to make the draft EU Regulation on Data Protection Future Proof. Tilburg University 2014, p. 9, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126164. Retrieved October 23, 2021.

[359] Tal Zarsky: The Trouble with algorithmic decisions: An analytic roadmap to examine efficiency and fairness in automated and opaque decision making, Science, Technology, & Human Values 2016, vol. 41(1), pp. 118-132, available at https://pdfs.semanticscholar.org/9b4d/bc901010a790d88c8be2370f8c9557895956.pdf?_ga=2.57485485.60694232.1562929501-1933874839.1562929501. Retrieved October 23, 2021.

[360] This problem was reviewed by the Article 29 Working Party in their 2017 guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Retrieved October 23, 2021.

[361] Ira Rubinstein: Big Data: The End of Privacy or a New Beginning? International Data Privacy Law 2013, vol. 3, no. 2, p. 77. Rubinstein explores on more types of discrimination. Apart from price discrimination, he also discusses threats to autonomy and covert discrimination.

[362] Non-discrimination is a fundamental right according to Article 21 of the EU Charter of Fundamental Rights. The text of the norm is available at https://fra.europa.eu/en/charterpedia/article/21-non-discrimination. Retrieved October 23, 2021.

[363] Donald Kluemper, Peter Rosen and Kevin Mossholder: Social Networking Websites, Personality Ratings and the Organizational Context - More than Meets the Eye?, Journal of Applied Social Psychology, vol. 42, issue 5, pp.1143-1172.

[364] See GDPR Article 21 (1).

legitimate under GDPR Article 6 (1) lit. f, but against "*being sorted in the wrong bucket*,"[365] resulting in individuals not succeeding at their jobs or their mortgage. And there are even more dramatic examples such as facial recognition bias,[366] bias in recidivism scoring systems,[367] bias in welfare[368] or bias in healthcare – detected years after the algorithm had been used.[369] The potential of information injustice and information inequality leads to the problem that the right to data protection does not help against certain risks and effects of the new economy.[370] Even if individual automated decision-making would be completely prohibited, this only refers to decisions which have been taken by tools and applications without any human intervention. As a result, all the IT-implementation effort needed to escape this limitation is to incorporate a mechanism which is to be used by a competent employee who confirms the decision – probably based on an algorithmic suggestion the system provided: Consequently, the 2019 expert opinion of the German Data Ethics Commission distinguishes between algorithm-based (suggestion-only), algorithm-driven (limited leeway) and fully automated decisions.[371]

10. Potential for surveillance

The potential for surveillance is another important factor to consider when AI technology is used. Video surveillance and facial recognition are very sensitive topics,[372] and the case of Clearview

[365] Omer Tene: Privacy: For the Rich or for the Poor? Concurring Opinions. Article published July 26 2012, available at http://www.concurringopinions.com/archives/2012/07/privacy-for-the-rich-or-for-the-poor.html. Retrieved October 23, 2021.

[366] National Institute of Standards and Technology: NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software. Demographics study on face recognition algorithms could help improve future tools. Background information on the study has been published on December 19, 2019, and is available at https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. Retrieved October 23, 2021.

[367] Julia Angwin, Jeff Larson, Surya Mattu, Lauren Kirchner: Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. Article published May 23 2016, available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Retrieved October 23, 2021.

[368] John Henley, Robert Booth: Welfare surveillance system violates human rights, Dutch court rules. Article published February 5 2020, available at https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules. Retrieved October 23, 2021.

[369] Heidi Ledford: Millions of black people affected by racial bias in health-care algorithms. Article published October 24 2019 (updated October 26 2019), available at https://www.nature.com/articles/d41586-019-03228-6. Retrieved October 23, 2021.

[370] Lokke Moerel: Big Data protection: How to make the draft EU Regulation on Data Protection Future Proof. Tilburg University 2014, p. 43, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126164. Retrieved October 23, 2021.

[371] Expert opinion of the Data Ethics Commission of the German Federal Government's Ministry of the Interior, for Building and Home Affairs (Gutachten der Datenethikkommission der Bundesregierung) 2019, p. 24, available at https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=3D63214EEC7EB10049F7C59E63B89F53.1_cid287?__blob=publicationFile&v=4. Retrieved October 23, 2021.

[372] The EU is considering a temporary ban in public places for up to five years until safeguards to mitigate the technology's risks are in place. Article by Anthony Spadafora: EU calls for five-year ban for facial recognition. Article published January 20 2020, available at

demonstrated how easy it is to identify and trace[373] individuals. The fact that some countries introduced so-called social scoring that tracks and evaluates all aspects of life[374] shows the societal and political dimension such techniques may involve. Apart from obvious forms of surveillance like CCTV, other techniques may have much more impact on people's lives, but people are hardly aware of that: the discussion[375] around cookie consent shed some light to the fact that tracking users' behavior is of economic interest, but there is little consciousness about the fact that a considerable part of today's digital economy is not simply about advertising, but about "*using human experience as free raw material for translation into behavioral data and usage for hidden commercial practices"*[376] which some authors summarize as *"the age of surveillance capitalism"*.[377] Such concentration of data[378] and knowledge may enforce surveillance powers. The issue of is of such importance that organizations like Amnesty International who campaign to end abuses of human rights[379] are dealing with the topic, saying that "*Europe's biometric surveillance industry is out of control – a multi-billion Euro industry that is flourishing by selling its wares to human rights abusers. The current EU export regulation system is broken and needs fixing fast.*"[380] Therefore, the European Parliament and EU member states started discussing agreements to toughen export rules for European tech companies that sell technology which could be used for espionage and surveillance.[381] However, some still believe that it is "*misleading to assume that all applications of AI can be made compatible with European values, when some applications inherently threaten human rights*."[382]

https://www.techradar.com/news/eu-calls-for-five-year-ban-on-facial-recognition. Retrieved October 23, 2021.

[373] See the company statement on their website: "*ClearView have built a reputation for meeting the stringent demands of police and law enforcement agencies*", which is available at https://clearview-communications.com/products/law-enforcement. Retrieved October 23, 2021.

[374] Nicole Kobie: The complicated truth about China's social credit system. Article published June 7 2019, available at https://www.wired.co.uk/article/china-social-credit-system-explained. Retrieved October 23, 2021.

[375] The latest draft of the ePrivacy Regulation was again rejected, see Jennifer Baker: How the ePrivacy Regulation talks failed ... again. Article published November 26 2019, available at https://iapp.org/news/a/how-the-eprivacy-regulation-failed-again/. Retrieved October 23, 2021.

[376] Shoshanna Zuboff: The Age of Surveillance Capitalism – The Fight for Human Future at the New Frontier of Power. Profile Books, 2019.

[377] Shoshanna Zuboff: The Age of Surveillance Capitalism – The Fight for Human Future at the New Frontier of Power. Profile Books, 2019.

[378] The recent German Facebook case showed that antitrust issues may be a factor to consider, however, the antitrust authority's ruling that social-media giant abused its dominance was reversed: Article by Sara Germano published August 26 2019, available at https://www.wsj.com/articles/facebook-wins-appeal-against-german-data-collection-ban-11566835967. Retrieved October 23, 2021.

[379] Source: https://www.amnesty.org/en/. Retrieved October 23, 2021.

[380] Merel Koning: EU companies selling surveillance tools to China's human rights abusers, blog post for Amnesty International published on September 21 2020, available at https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers/. Retrieved October 23, 2021.

[381] Laurens Cerulus: Europe to crack down on surveillance software exports. Article published October 15 2020, available at https://www.politico.eu/article/europe-to-curtail-spyware-exports-to-authoritarian-countries/. Retrieved October 23, 2021.

[382] AccessNow: Europe's approach to artificial intelligence: how AI strategy is evolving. Report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf. Retrieved October 23, 2021.

11. Human Rights and democracy

The potential for discrimination and the potential for surveillance are closely linked to human rights risks, and the case of Cambridge Analytica[383] is probably the best example of the political dimension the use of Artificial Intelligence may have. Phenomena like fake news or hate speech show that it is worthwhile examining this technology from a human rights perspective. Consequently, organizations like Human Rights Watch,[384] ARTICLE 19,[385] Amnesty International and AccessNow[386] as well as Data & Society[387] dealt with the analysis of AI and governance from a human rights standpoint and stressed the importance of political participation and freedom of expression. Moreover, in the framework of non-discrimination and equality, the issue of accessible design i.e. disability rights approach was discussed.[388] There is good reason why the issue of human rights is part of literally all national Artificial Intelligence strategies and either mentioned explicitly in the framework of the concept of trustworthy AI or referenced because "*human rights are often assumed to form the foundation of policy whether or not it is explicitly stated*".[389] At European level, various institutions dealt with human rights implications AI may have and issued corresponding papers, for example, the Committee of Ministers adopted recommendations on human rights impacts of algorithmic systems and acknowledged that there are "*significant human rights challenges attached to the increasing reliance on algorithmic systems in everyday life, such as regarding the right to a fair trial; the right to privacy and data protection; the right to freedom of thought, conscience and religion; the right to freedom of expression; the right to freedom of assembly; the right to equal treatment; and economic and social rights*".[390] The Council of Europe was very active and provided various papers: a recommendation regarding human rights impacts of algorithmic systems[391] and a study on human

[383] Facebook transferred millions of user profiles to the data mining company of Cambridge Analytica. Background information on the case can be found at the website of the Electronic Privacy Information Center (EPIC): https://epic.org/privacy/facebook/cambridge-analytica/. Retrieved October 23, 2021.

[384] The article "UK: Automated benefits system failing people in need – the government's flawed 'Universal Credit' Algorithm pushing people into poverty" was published on the Human Rights Watch website on September 29 2020, and provides further background information on the issue. The article is available at https://www.hrw.org/news/2020/09/29/uk-automated-benefits-system-failing-people-need. Retrieved October 23, 2021.

[385] Source: https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artif icial-Intelligence-1.pdf. Retrieved October 23, 2021.

[386] Amnesty International and Access Now issued the "Toronto Declaration" in 2018 which is available at https://www.torontodeclaration.org/. Retrieved October 23, 2021.

[387] Source: https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf. Retrieved October 23, 2021.

[388] Mike Latonero: Governing Artificial Intelligence: upholding human rights & dignity. Paper for Data & Society published 2018, available at https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf. Retrieved October 23, 2021.

[389] Global Partners Digital: National Artificial Intelligence Strategies and Human Rights: A Review. Paper published April 15 2020, available at https://www.gp-digital.org/publication/national-artificial-intelligence-strategies-and-human-rights-a-review/. Retrieved October 23, 2021.

[390] Source: https://rm.coe.int/09000016809e1154. Retrieved October 23, 2021.

[391] Source: https://rm.coe.int/09000016809e1154. Retrieved October 23, 2021.

rights dimensions of automated data processing techniques and possible regulatory implications.[392] In addition, the Council of Europe established an ad hoc Committee on Artificial Intelligence (Committee on Artificial Intelligence of the Council of Europe: CAHAI) whose mission is to engage in broad multi-stakeholder consultations to examine the feasibility of a legal framework for the development, design, and application of artificial intelligence, based on Council of Europe's standards on human rights, democracy, and the rule of law.[393] CAHAI's 2020 report[394] focused on the impact on AI various human-rights-related aspects embedded in ECHR such as liberty, security and fair trial,[395] private and family life as well as physical, psychological and moral integrity,[396] freedom of expression,[397] freedom of assembly and association[398] as well as prohibition of discrimination.[399] CAHAI's report also dealt with red lines such as AI-enabled (personal, physical or mental) tracking, assessment, profiling, scoring or nudging through biometric or behavior recognition, AI-powered mass surveillance, deep fakes and human-AI interfaces. It also addresses potential new human rights if "*current human rights, democracy and the rule of law fail to adequately protect us*" and discussed that there may be a need for a

- *"A right to human autonomy, agency and oversight over AI,*
- *A strengthened right to privacy to protect against AI-driven mass surveillance,*
- *A separate right to physical, psychological and moral Integrity in light of AI profiling*
- *Adapting the right to data privacy to protect against indiscriminate, society-wide online tracking of individuals, using personal and non-personal data (which often serves as a proxy for personal identification)*
- *A right to transparency / explainability of AI outcomes including the right to an explanation of how the AI functions, what logic it follows, and how its use affects the interests of the individual concerned, even if the AI-system does not process personal data, in which case there is already a right to such information under GDPR."*

While banal at first glance, even seemingly simple use cases like an online search show that the use of AI can have an impact on the freedom of information: if Artificial Intelligence is tailored and trained

[392] Source: https://rm.coe.int/algorithms-and-human-rights-study-on-the-human-rights-dimension-of-aut/1680796d10. Retrieved October 23, 2021.

[393] AccessNow: Europe's approach to artificial intelligence: how AI strategy is evolving. Report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf. Retrieved October 23, 2021.

[394] Catelijne Muller: The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law, report for the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI), published June 24 2020, available at https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da. Retrieved October 23, 2021.

[395] ECHR Art. 5 and 6.

[396] ECHR Art. 8.

[397] ECHR Art. 10.

[398] ECHR Art. 11.

[399] ECHR Art. 14, protocol 12.

to provide suitable suggestions, that may on the one hand help pursue with the online research, but on the other hand, certain results may be disregard, and this way, important information could be withhold. In the event that Artificial Intelligence is used in a manipulative manner, that may have a political dimension, for example in the context of persuasion (e.g. creation of targeted propaganda) or deception (e.g. manipulation of videos) or analysis (e.g. evaluation of human behavior, moods and beliefs) and may thus undermine the ability of democracies to sustain truthful public debates.[400] This is not only true for totalitarian states, any state and any political party nowadays can take advantage of using AI for elections to maximize the effectiveness of email or social media campaigns.[401] Voter influencing is core of every electoral campaign, but "*well-functioning democracies require a well-informed citizenry, an open social and political discourse and absence of opaque voter influence*."[402] Against this background, one of the pioneers of data privacy concluded that "*we have come to realize that how well democracies balance the competing demands of privacy, disclosure, and surveillance will exert a major influence on the quality of civic life in the 21st century, and that shaping this balance will now have to be done in the context of continuing terrorist threats and actions. In short, privacy is a quality-of-life topic worth the best scholarship, thoughtful advocacy, and continuing attention of us all*."[403]

12. Socio-economic impacts

The debate on the impact of Artificial Intelligence on the economy in general and employment in specific and how Big Data and AI applications will influence and change the job market[404] are already going on for a long time. Since AI helps with the transformation of businesses, AI will necessarily also have an impact on workforce: we have come to a point where not only monotonous tasks in production lines and factories or activities related to customer care can be automated, complex operations can be automated as well – even the legal profession may be severely impacted by this new kind of virtual workforce, because duties like document classification, summarization, comparison,

[400] Miles Brundage et al: The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Article published February 2018, available at https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217. Retrieved October 24, 2021.

[401] Manu Siddharth Jha: Want to Win an Election? Use AI And Machine Learning. Article published April 23 2020, available at https://www.mygreatlearning.com/blog/how-ai-and-machine-learning-can-win-elections/#:~:text=Artificial%20Intelligence%20for%20the%20Benefit%20of%20the%20Voter,help%20them%20make%20up%20their%20minds%20about%20candidates. Retrieved October 24, 2021.

[402] Catelijne Muller: The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law, report for the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI). Report published June 24 2020, available at https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da. Retrieved October 24, 2021.

[403] Alan Westin: Social and Political Dimensions of Privacy, Journal of Social Issues, vol. 59, no. 2, 2003, pp. 431-453, available at https://www.sfu.ca/~palys/Westin-2003-Social&PoliticalDimensionsOfPrivacy.pdf. Retrieved October 24, 2021.

[404] Dennis Späth: Artificial Intelligence is transforming the workforce as we know it. Article published March 18 2019, available at https://workplaceinsight.net/artificial-intelligence-is-transforming-the-workforce-as-we-know-it/. Retrieved October 24, 2021.

knowledge extraction, discovery and retrieval are more and more based on technology and automation, and less on human work.[405] That is why some raise concerns regarding AI in the employment context[406] or started discussing unconditional basic income.[407] Others claim that "*robots will take your jobs, government will have to pay your wage*",[408] *draw red lines* explain that the answer what the future of work may look like is more difficult to answer:[409] that workforce will face growing disparities with middle-wage earners losing ground, and that internationally, the lack of access to new technologies in least developed countries will increase inequalities between countries even further. The impact on AI on the digital economy was also raised by a number of international institutions, for example UNI, the global union federation for national and regional trade unions which is concerned with protecting workers' rights[410] or the Committee on Artificial Intelligence of the Council of Europe: their 2020 report on the impact of AI on human rights, democracy and the rule of law[411] also addressed the issue of social and economic rights, and G20's human-centered AI principles[412] not only stress that AI shall be fair, transparent and accountable and that it shall respect privacy, equality, diversity – it also underlines that Artificial Intelligence shall respect internationally recognized labor rights. Fact is that nowadays, even getting a job starts with AI because resume screenings and background checks are very often being automated, and the draft AI Regulation addresses employment and recruitment issues and classifies AI applications used for such purpose / in this sector as high-risk[413] with all its consequences. In addition, existing directives on non-discrimination in the employment context based

[405] George Krasadakisd: Artificial Intelligence: The Impact on Employment and the Workforce. How is AI replacing jobs? Which roles and industries will be most impacted? How can societies get prepared? Article published January 2018, available at https://medium.com/innovation-machine/artificial-intelligence-3c6d80072416. Retrieved October 24, 2021.

[406] John Barnett: Will AI Revolution Lead to Mass Unemployment? What artificial intelligence might mean for your job and industry. Article published April 25 2017, available at https://www.business.com/articles/john-barnett-artificial-intelligence-job-market/#:~:text=Well%2C%20the%20real%20answer%20lies%20somewhere%20in%20between.,will%20result%20in%20huge%20losses%20and%20then%20layoffs. Retrieved October 24, 2021.

[407] Doug Bolton: The rise of artificial intelligence could put millions of human workers out of jobs - could a basic income be a solution? Article published February 19 2016, available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/basic-income-artificial-intelligence-ai-robots-automation-moshe-vardi-a6884086.html. Retrieved October 24, 2021.

[408] Catherine Clifford quotes Elon Musk in her article for CNBC published November 4 2016 (updated January 29 2018), available at https://www.cnbc.com/2016/11/04/elon-musk-robots-will-take-your-jobs-government-will-have-to-pay-your-wage.html. Retrieved October 24, 2021.

[409] United Nations Department of Economic and Social Affairs commented on this issue in their blog post: Will robots and AI cause mass unemployment? Not necessarily, but they do bring other threats. The article was published on September 13 2017, and is available at https://www.un.org/development/desa/en/news/policy/will-robots-and-ai-cause-mass-unemployment-not-necessarily-but-they-do-bring-other-threats.html. Retrieved October 24, 2021.

[410] Source: https://uniglobalunion.org/. Retrieved October 24, 2021.

[411] Catelijne Muller: The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law, report for the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI), published June 24 2020, available at https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da. Retrieved October 24, 2021.

[412] Source: https://www.mofa.go.jp/files/000486596.pdf. Retrieved October 24, 2021.

[413] The law firm Hunton Andrews Kurth provides details on the proposed AI Act in their 2021 blog post: European Commission publishes proposal for Artificial Intelligence Act, article published April 22 2021, available at https://www.huntonprivacyblog.com/2021/04/22/european-commission-publishes-proposal-for-artificial-intelligence-act/. Retrieved October 24, 2021.

on religion or belief, disability, age or sexual orientation[414] or equal treatment of men and women in matters of employment and occupation[415] must be taken into consideration as well.

13. Liability

A technology like AI that is characterized by systems operating in an autonomous manner leads to yet another issue with regards to AI: liability. While accountability as a value and privacy principle is stressed in the majority of publications, fewer texts deal with the fact that AI has the potential to challenge the traditional notions of legal personality including agency and responsibility.[416] In this context, the European Parliament published a study on robotics[417] that deals with liability law solutions in respect of autonomous robots. Moreover, the European Commission published a report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics[418] and its Expert Group on Liability and New Technologies issued another report[419] on liability for AI and other emerging technologies in which it explains key findings with regards to questions like new duties of care, strict and vicarious liability, the burden of proof for both, causation and damage, as well as insurance issues. The idea of a legal personality for AI and the potential of damages caused by autonomous robots are not the only issues to consider since there are also product liability implications[420] and AI might furthermore call for changes to copyright laws.[421] If algorithmic decision-making is used in criminal proceedings without human involvement, AI may furthermore have to be

[414] Council Directive 2000/78/EC of 27 November 2000 against discrimination at work on grounds of religion or belief, disability, age or sexual orientation establishing a general framework for equal treatment in employment and occupation is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0078. Retrieved October 24, 2021.

[415] Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0054. Retrieved October 24, 2021.

[416] Mihalis Kritikos: Artificial Intelligence ante portas: legal and ethical reflections, p. 1, EPRS briefing, available at https://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-artificial-intelligence-ante-portas.pdf. Retrieved October 24, 2021.

[417] European Civil Law Rules on Robotics, published in 2016, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf. Retrieved October 24, 2021.

[418] European Commission: Report to the European Parliament, the Council and the European Economic and Social Committee on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, published February 19 2020, available at https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX:52020DC0064. Retrieved October 24, 2021.

[419] At this stage, the report does not provide specific recommendations as to how these recommendations should be implemented into EU or national laws. The full report was published November 21, 2019, available at https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608. Retrieved October 24, 2021.

[420] John Villasenor: Products liability law as a way to address AI harms. Article published October 31 2019, available at https://www.brookings.edu/research/products-liability-law-as-a-way-to-address-ai-harms/. Retrieved October 24, 2021.

[421] On October 30, 2019, the US Patent and Trademark Office requested comments on intellectual property protection for AI innovations, see Federal Register 2019, vol. 84, no. 210, which is available at https://www.govinfo.gov/content/pkg/FR-2019-10-30/pdf/2019-23638.pdf. Retrieved October 24, 2021.

examined and assessed in the light of due process requirements.[422] AI can thus be examined from various legal perspectives, ranging from data protection, tort liability, copyright authorship and criminal law[423] – a multitude of areas of liability arises from different use cases of AI. From an individual's perspective, the question would be whom to turn to: a court[424] or a regulator[425] or a company, and if so, which one: from a GDPR perspective, there are controllers, processors and joint controllers; from a DGA perspective there are data holders and data users, and there is not just data but "*representations of acts, facts or information and any compilation of the same including sound as well as visual or audiovisual recording*,"[426] and looking at the categorization of relevant players in the context of the draft AI regulation, the situation becomes even more complex as there are providers, manufacturers, distributors, importers, users – how should an average person without corresponding expertise be able to tell who is responsible for which part and under which conditions, particularly now that the European Court of Justice has clarified the competences of non-lead data protection authorities and has given them greater ability to pursue Big Tech companies which are not headquartered in their territory,[427] which also questions the one-stop-shop mechanism that was once believed to be one of the major advancements the GDPR would bring to organizations.[428]

[422] Mihalis Kritikos: Artificial Intelligence ante portas: legal and ethical reflections, EPRS briefing, p. 4, available at https://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-artificial-intelligence-ante-portas.pdf. Retrieved October 24, 2021.

[423] These topics were covered in the recently held conference "AI, Law, and Agency in the Age of Machine Learning" which took place in Tel Aviv. Background information is available at https://en-ethics.tau.ac.il/AI_Law_And_Agency_in_the_Age_of_Machine_Learning/. Retrieved October 24, 2021.

[424] Lars Lensdorf, Robert Henrici, Moritz Hüsch, Nicholas Shepherd: A New Day for GDPR Damages Claims in Germany? Article published February 25 2021, available at https://www.insideprivacy.com/data-privacy/a-new-day-for-gdpr-damages-claims-in-germany/. Retrieved October 24, 2021.

[425] To quote Politico: Have a GDPR complaint? Skip the regulator and take it to court, source: https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/. Retrieved October 24, 2021.

[426] Debbie Heywood: The EC draft Data Governance Act – an altruistic approach to data. Article for Taylor Wessing published January 29 2021, available at https://www.taylorwessing.com/en/insights-and-events/insights/2021/01/the-ec-draft-data-governance-act---an-altruistic-approach-to-data#:~:text=The%20DGA%20applies%20to%20a%20very%20broad%20range,the%20form%20of%20sound%2C%20visual%20or%20audiovisual%20recording%22. Retrieved October 24, 2021.

[427] Scott Ikeda: Big Tech Companies May Face Blizzard of New Probes in EU as CJEU Ruling Clears Path for Data Protection Authorities. Article for the CPO Magazine published June 28 2021, available at https://www.cpomagazine.com/data-protection/big-tech-companies-may-face-blizzard-of-new-probes-in-eu-as-cjeu-ruling-clears-path-for-data-protection-authorities/#:~:text=The%20new%20CJEU%20ruling%20gives%20the%20data%20protection,protection%20authorities%20will%20need%20to%20meet%20certain%20conditions. Retrieved October 24, 2021.

[428] Heidi Waem, Simon Verschaeve: What's left of the GDPR's one-stop-shop? CJEU clarifies the competences of non-lead data protection authorities. Article published July 5 2021, available at https://blogs.dlapiper.com/privacymatters/eu-whats-left-of-the-gdprs-one-stop-shop-cjeu-clarifies-the-competences-of-non-lead-data-protection-authorities/?utm_source=mailpoet&utm_medium=email&utm_campaign=privacy-matters-newsletter. Retrieved October 24, 2021.

14. Security

Security is always an important component[429] whenever data processing is in question, and since Big Data and AI are about complex operations, security is a priority in an increasingly digital and data-driven economy and society.[430] If security issues are not taken seriously, this may lead to unauthorized (increased) accessibility, disclosure of (sensitive) information and unintended (undesired) inferences[431] as well as reputational damage for both, the company using AI techniques and the affected individuals. GDPR, to name just one example of legislation dealing with security,[432] correspondingly covers various such aspects[433] and Recitals 75 and 76 clearly show that the Regulation pursues a risk-based approach[434] as it distinguishes between processing activities with a high and a low likelihood and severity to the rights and freedoms of natural persons.[435] Consequently, mitigation measures have to be taken into consideration, and these have to be adjusted to the type of information processed, the devices in question as well as access to location of, and retention and preservation of data.[436] In addition, the operational environment as well as governance, resources and project management, potential conflicts of interest and issues of ownership, company values and ethics[437] play an important role to minimize risk – however, all this is based on the traditional view GDPR takes regarding companies as controllers: the true security danger we are facing with AI is that, even though AI can be used for security purposes like intrusion detection,[438] new systemic risks arise since more and more critical infrastructures[439] depend on centralized systems with operations that are based on algorithmic

[429] See for example GDPR Article 32.

[430] Background information on this issue is offered by the 2019 OECD Digital Economy Papers that deal with digital security risk management. The paper is available at https://doi.org/10.1787/20716826. Retrieved October 24, 2021.

[431] Andrew Burt: Privacy and cyber-security are converging. Here's why that matters for people and for companies. Article published January 3 2019, available at https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies. Retrieved October 24, 2021.

[432] In 2019, the German Federal Industries Association developed a tool to illustrate the current state of play regarding country-specific regulations on cyber security, critical infrastructure protection, incident notification and the protection of Intellectual Property from cyber risks, available at https://english.bdi.eu/topics/global-issues/cyber-landscapes/. Retrieved October 24, 2021.

[433] Article 32, security of processing; Article 25: data protection by design and by default; Articles 35 and 36: data protection impact assessments; Articles 33 and 34: breach notifications.

[434] Nico Härting: Datenschutzgrundverordnung, Dr. Otto Schmidt publishing, Cologne 2016, p. 34.

[435] A summary of risk-relevant provisions can be found in: Thomas Kranig, Andreas Sachs, Markus Gierschmann: Datenschutz-Compliance nach der DSGVO – Handlungshilfe für Verantwortliche inclusive Prüffragen für Aufsichtsbehörden, Bundesanzeiger Ltd. publishing Cologne, 2017, p. 87.

[436] Mike Dutch: A Data Protection Taxonomy, paper for the Storage Networking Industry Association (SNIA), published June 2010, available at https://www.snia.org/sites/default/files/A_Data_Protection_Taxonomy_V51.pdf. Retrieved October 24, 2021.

[437] Government of Canada: Guide to risk taxonomies, last modified March 29 2016, available at https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/taxonomies.html#toc2. Retrieved October 24, 2021.

[438] Bruno Capone: Intrusion Detection based on Deep Learning. Article published October 16 2020, available at https://www.aitech.vision/en/2020/10/16/intrusion-detection-based-on-deep-learning/. Retrieved October 24, 2021.

[439] Deven Desai, Christos Makridis: We should have known SolarWinds would be a target. Article published January 6 2021, available at https://www.cfr.org/blog/we-should-have-known-solarwinds-would-be-target. Retrieved October 24, 2021.

(automated) decisions. Another factor to consider is that from both, an individual's and societal perspective, this technology can "*empower malicious actors ranging from cybercriminals to totalitarian states in their desire to control populations*"[440] and this way, may pose a threat to security.

15. Malicious use of AI

The mere fact that a technology is new does not mean that it will automatically worsen the situation in terms of security. On the contrary, the majority of successful cyberattacks start with a person intentionally or unintentionally fooled into clicking somewhere they shouldn't; hackers target people because the real weakest link is often the least obvious.[441] However, fact is also that much more attention has been paid to beneficial applications of AI than the ways in which Artificial Intelligence could be used maliciously, and some predict that the growing use of AI systems will change the landscape of threats, because adequate defenses to potential security threats from malicious uses of AI are not yet developed.[442] A recent report surveyed potential security threats in the context of Artificial Intelligence and came to the following conclusions:[443] the use of Artificial Intelligence will expand existing threats and change the typical character of threats, because AI may simply lower the costs of attacks since AI is scalable and can complete tasks that would ordinarily require human labor, intelligence and expertise; the use of AI for malicious purposes could be especially effective, because it could be finely targeted, difficult to attribute, and thus likely to exploit vulnerabilities (e.g. by using speech synthesis for impersonation), and complete tasks that would be otherwise be impractical for humans (e.g. labor intensive attacks). AI can moreover be used in novel ways, for example by "*exploiting human vulnerabilities (e.g. through the use of speech synthesis for impersonation), by exploiting existing software vulnerabilities (e.g. through automated hacking) – or the vulnerabilities of AI systems (e.g. through data poisoning or by introducing training data that causes a learning system to make mistakes or by inputs designed to be misclassified by machine learning systems.*"[444] The latter is a particularly interesting aspect insofar as AI itself may be vulnerable as well: if AI systems can

[440] Catelijne Muller: The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law, report for the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI), published June 24 2020, available at https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da. Retrieved October 24, 2021.

[441] Stu Sjouwerman: Seven Reasons For Cybercrime's Meteoric Growth. Article published December 23 2019, available at https://www.forbes.com/sites/forbestechcouncil/2019/12/23/seven-reasons-for-cybercrimes-meteoric-growth/#:~:text=Cybercrime%20has%20been%20on%20the%20rise%20for%20years.,more%20criminals%20are%20leveraging%20the%20internet%20to%20steal. Retrieved October 24, 2021.

[442] Valerie Thomas on behalf of the Regulatory Institute: Report on Artificial Intelligence part I: the existing regulatory landscape. Article published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/. Retrieved October 24, 2021.

[443] Miles Brundage et al: The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Article published February 2018, available at https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217. Retrieved October 24, 2021.

[444] Miles Brundage et al: The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Article published February 2018, available at https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217. Retrieved October 24, 2021.

exceed human performance, but they may also fail in ways that a human never would. Finally, Artificial Intelligence could also be used in a political context, for example for creating targeted propaganda or to manipulate videos with the help of deepfakes,[445] or threaten physical security by subverting systems or through the use of drones.[446] In consequence, a new quality of malicious actors may emerge, and AI can thus be considered a dual-use technology.[447] It is therefore necessary to address these dual-use concerns correspondingly and collaborate closely with the relevant stakeholders, researchers and experts to investigate, prevent and mitigate potential malicious uses of AI:[448] AI's dual-use character, its efficiency and scalability, its anonymity and psychological distance together with the fact that Artificial Intelligence may exceed human capabilities and that it implies novel unresolved vulnerabilities may lead to serious threats that could affect our security, for example, by criminals training machines to hack or socially engineer victims at scales beyond what humans are doing now or by privacy-eliminating surveillance and profiling, or through automated and targeted disinformation campaigns or by non-state actors weaponizing drones or robots.[449] However, even much more harmless use cases nevertheless show the potential for risk: the e-commerce sector is a good example for the use of so-called dark patterns,[450] i.e. methods to misinform or inappropriately influence users' behavior and manipulate consumer actions, ranging from annoying-but-innocent to unlawful (e.g. checkbox, scroll-down) design, and this way, violating existing laws such as Section 5 of the FTC Act, or consumer[451] and data privacy laws.[452] Obfuscatory checkboxes are probably the most common examples of dark patterns,[453] and dark patterns are not just a side-effect of AI uses, they

[445] Kanan Purkayastha: Challenges from malicious use of AI. Article published May 18 2020, available at https://www.observerbd.com/news.php?id=257035. Retrieved October 24, 2021.

[446] Saheli Choudhury: Malicious use of A.I. could turn self-driving cars and drones into weapons, top researchers warn. Article published February 21 2018, available at https://www.cnbc.com/2018/02/21/malicious-use-of-ai-by-hackers-could-pose-security-risks-threats.html.

[447] Jayshree Pandya: The dual-use dilemma of Artificial Intelligence. Article published January 7 2019, available at https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/. Retrieved October 24, 2021.

[448] Miles Brundage et al: The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Article published February 2018, available at https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217. Retrieved October 24, 2021.

[449] Valerie Thomas on behalf of the Regulatory Institute: Report on Artificial Intelligence part I: the existing regulatory landscape, article published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/. Retrieved October 24, 2021.

[450] Harry Brignull coined the term already in the year 2010, source: https://www.darkpatterns.org/about-us - a website that has been established to raise public awareness of deceptive digital practices. Retrieved October 24, 2021.

[451] Laura Kim, John Graubert: Dark Patterns: What They Are and What You Should Know About Them. Article published July 9, 2019, available at https://www.insideprivacy.com/consumer-protection/dark-patterns-what-they-are-and-what-you-should-know-about-them/. Retrieved October 24, 2021.

[452] For example, the California Privacy Rights Act (CPRA), the first legislation explicitly regulating dark patterns in the United States: background information on the CPRA is provided by Jennifer King and Adriana Stephan in their 2021 paper "Regulating Privacy Dark Patterns in Practice – Drawing Inspiration from California Privacy Rights Act, which was published September 2021 in Georgetown Law Technology Review 2021, vol. 5 pp. 251-276, and is available at https://georgetownlawtechreview.org/regulating-privacy-dark-patterns-in-practice-drawing-inspiration-from-california-privacy-rights-act/GLTR-09-2021/. Retrieved October 24, 2021.

[453] Ben Davis: 13 examples of dark patterns in ecommerce checkouts. Article published on April 6 2017, available at https://econsultancy.com/13-examples-of-dark-patterns-in-ecommerce-checkouts/. Retrieved October 24, 2021.

have become a massive problem as a report by the Princeton research group on popular shopping websites shows:[454] the report claims to have found dark patterns in 11% of those websites, and it also identified dozens of third-party entities that offer turnkey solutions enabling sellers to build dark patterns into websites.[455]

16. Concentration of power

Some say that data is the oil of the 21st century, but that is incorrect because the volume of (machine, sensor, personal, etc.) data keeps growing exponentially[456] whereas the occurrences of oil are finite. Like every other industrial revolution, "*Industry 4.*0" has its own challenges and risks – and concentrations of power: we live in a world where a small number of companies has the power to control much of what we do – "*Alphabet controls our search and much of our mobile experience, Apple controls the remainder of our mobile and much of our content experience, Amazon controls a large portion of our content experience and much of the Internet of Things, and Microsoft essentially sweeps up everything else*,"[457] and the issue is that, without corresponding future regulation, data may be processed rather in accordance with corporate terms and conditions, and perhaps less with applicable privacy laws. The concentration of data leads to a concentration of power for those who control the data to an extent that this circumstance is relevant under antitrust law.[458] So far, the focus of regulation was on personal data and privacy self-management; legislation dealt with specific industries and specific types of data and specific uses cases (processing activities) that may result in risk or may lead to negative consequences for the individual behind the data but not with regulating machine-generated data.[459] The problem with taking market power into consideration in the framework of regulating AI starts with the fact that the existing legal landscape was not mapped,[460] and that even seemingly simple things like terminology issues are far from being harmonized but this

[454] Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites Draft. Report published June 25 2019, available at https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns.pdf. Retrieved October 24, 2021.

[455] By Laura Kim, John Graubert: Dark Patterns: What They Are and What You Should Know About Them. Article published July 9 2019, available at https://www.insideprivacy.com/consumer-protection/dark-patterns-what-they-are-and-what-you-should-know-about-them/. Retrieved October 24, 2021.

[456] The McKinsey Global Institute estimates that the global volume of data doubles every three years: https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world. Retrieved October 24, 2021.

[457] Julia Black, Andrew Murray: Regulating AI and Machine Learning: Setting the regulatory agenda. European Journal of Law and Technology, vol. 10, issue 3, 2019. The article is available at https://ejlt.org/index.php/ejlt/article/view/722/980. Retrieved October 24, 2021.

[458] The recent German Facebook case showed that antitrust issues may be a factor to consider, however, the antitrust authority's ruling that social-media giant abused its dominance was reversed: Article by Sara Germano, published August 26 2019, available at https://www.wsj.com/articles/facebook-wins-appeal-against-german-data-collection-ban-11566835967. Retrieved October 24, 2021.

[459] Jan Christian Sahl: Brauchen wir ein Datenschutzrecht für Maschinendaten? The article was published in the framework of the "Berliner Datenschutzrunde", and is available at https://www.berliner-datenschutzrunde.de/node/162. Retrieved October 24, 2021.

[460] AccessNow: Europe's approach to artificial intelligence: How AI strategy is evolving. Report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf. Retrieved October 24, 2021.

would truly be needed for a consistent approach. Recent initiatives like the DGA, DSA and DMA to regulate huge platforms and information gatekeepers are important steps, but there is more work ahead given the multitude of implications arising from AI as a technology and market dominance as a phenomenon.

E. Relevant sources of law

I. International level

1. United Nations Universal Declaration of Human Rights

In response to World War II, the United Nations (UN) adopted and proclaimed the Universal Declaration of Human Rights in 1948.[461] The Universal Declaration of Human Rights (UDHR) sets out, for the first time, fundamental human rights to be universally protected, and this includes privacy since UDHR Article 12 sets forth that "*no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks*".

2. European Convention on Human Rights

In Europe, there are two systems which ensure the protection of fundamental human rights in Europe, the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (Charter): The European Convention on Human Rights[462] was adopted in 1950. ECHR Article 8 states that "*everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*."

3. Charter of Fundamental Rights of the European Union

[461] Source: http://www.un.org/en/universal-declaration-human-rights/index.html. Retrieved September 26, 2021.
[462] The text is available at https://www.echr.coe.int/Documents/Convention_ENG.pdf. Retrieved September 26, 2021.

The Charter of Fundamental Rights of the European Union[463] was enacted in 2000 and is a legally binding[464] human rights instrument, and it also deals with the right to respect for his or her private and family life, home and communications (Article 7), but what is special is that it specifically addresses the protection of personal data: Article 8 of the Charter of Fundamental Rights of the European Union postulates that "*everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority*".[465] Although the Convention and the Charter contain provisions on human rights, they operate within separate legal frameworks:[466] The Charter of Fundamental Rights of the European Union was drafted by the European Union and is interpreted by the Court of Justice of the European Union. The European Convention on Human Rights was drafted by the Council of Europe[467] and is interpreted by the European Court of Human Rights. The Charter constitutes the legal framework for human rights in the European Union, of which the European Convention on Human Rights forms an important part.[468] Unlike the Charter of the Fundamental Rights of the European Union, the Convention does not contain a specific provision on data protection, but this does not mean that rights of data subjects are not guaranteed within this framework, as steadily growing case law confirms that corresponding control mechanisms are in place.[469]

[463] Source: http://www.europarl.europa.eu/charter/pdf/text_en.pdf. Retrieved September 26, 2021.

[464] The European Union competent to pass legislation on data protection matters based on Article 16 of the Treaty on the Functioning of the European Union and used this competence to include Article 8 on the right to data protection in the Charter.

[465] The question of the relationship between Article 7 and 8 of the Charter is controversially discussed. Some authors consider that Article 8 is lex specialis: Sebastian Bretthauer in: Louisa Specht/Reto Manz: Handbuch europäisches und deutsches Datenschutzrecht 2019, p. 29.

[466] Background information on the relationship between the Charter and the Convention is provided by UK's Equality and Human Rights Commission, a national human rights institution, and is available at https://www.equalityhumanrights.com/en/what-are-human-rights/how-are-your-rights-protected/what-charter-fundamental-rights-european-union. Retrieved September 26, 2021.

[467] Background information on various institutions is available at at https://www.coe.int/en/web/about-us/do-not-get-confused?desktop=true: "The Council of Europe is an international organization in Strasbourg which comprises 47 countries of Europe. It was set up to promote democracy and protect human rights and the rule of law in Europe. The European Council is an institution of the European Union, consisting of the heads of state or government from the member states together with the President of the European Commission, for the purpose of planning Union policy". Retrieved October 2, 2021.

[468] Nomi Byström: The data subject and the European Convention on Human Rights: access to own data. Article published December 31 2014, available at https://www.edilex.fi/viestintaoikeuden-vuosikirja/181000010. (Retrieved October 2, 2021). Some authors distinguish these two models of human rights protection as follows: the European Convention on Human Rights is considered to be a "court-centred model" of protection, whereas the Charter of Fundamental Rights may be considered a "legislative centred model" – see Simon Bronitt: A Tale of Two European Charters of Rights – Comparing the European Convention on Human Rights and the EU Charter of Fundamental Rights, article available o at http://www.academia.edu/6410839/A_Tale_of_Two_European_Charters_of_Rights_Comparing_the_European_Convention_on_Human_Rights_and_the_EU_Charter_of_Fundamental_Rights. Retrieved October 2, 2021.

[469] Nomi Byström: The data subject and the European Convention on Human Rights: Article published December 31 2014, available at https://www.edilex.fi/viestintaoikeuden-vuosikirja/181000010. Retrieved October 2, 2021.

4. Council of Europe Data Protection Convention 108+

The Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data[470] dates back to 1980 and addresses challenges for privacy resulting from the use of new information and communication technologies. While keeping the convention's philosophy, the convention has recently been modernized ("*108+*").[471] This convention lays down a number of principles which states must transpose into national law to ensure that personal data are processed only for specific purposes, that data are not retained longer than is necessary for the underlying purpose(s), and that the collection and processing of data is not excessive in relation to the purposes.[472] Article 5 lit. b of Convention 108+ also introduces the notion of incompatibility, and Article 5 lit. c of Convention 108+ addresses the principle of data minimization.[473] This convention was the first legally binding international instrument in data protection,[474] and that is why some believe that the Council of Europe has played a pioneering role the existing data protection legislation.[475] This view is underlined by the fact that the Council of Europe issued two Resolutions which formulated what later became fundamental principles of data protection law.[476] Considering the constantly increasing number of ratifications of Convention 108,[477] this convention has thus the potential to become a global standard.[478]

5. OECD Privacy Guidelines

The Organization for Economic Co-operation and Development (OECD) issued guidelines on the "*Protection of Privacy and Transborder Data Flows of Personal Data*" which were passed in September 1980[479] and updated in 2013.[480] These guidelines focus on the practical implementation of

[470] Source: https://rm.coe.int/16808ade9d. Retrieved October 2, 2021.
[471] See "The modernised Convention 108: novelties in a nutshell", available at https://rm.coe.int/16808accf8.
[472] Details can be found at https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet. Retrieved October 2, 2021.
[473] Nikolaus Forgo et al.: The principle of purpose limitation in big data, p. 24.
[474] David Wright, Paul de Hert, Serge Gutwirth: Are the OECD guidelines at 30 showing their age? Communications of the ACM, vol. 54, issue 2, February 2011, pp. 119-127, available at https://dl.acm.org/citation.cfm?id=1897848. Retrieved October 2, 2021.
[475] The German consultancy Datenschutz Nord reported on this issue in their online blog on March, 19 2019, which is available at https://www.datenschutz-notizen.de/die-konvention-nr-108-die-kleine-schwester-der-dsgvo-0222164/. Retrieved October 2, 2021.
[476] E.g., the principle of purpose limitation: Forgo et al.: The principle of purpose limitation in big data, p. 23.
[477] The latest signatories are Mexico and Cabo Verde in 2018, Tunisia in 2017 and Mauritius and Senegal in 2016; the chart of signatures and ratifications is available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures. Retrieved October 2, 2021.
[478] Source: https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet (Retrieved October 2, 2021). However, this convention only applies to personal data which are processed automatically.
[479] Original 1980 version available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#guidelines. Retrieved October 2, 2021.
[480] Source: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (Retrieved October 2, 2021). The expert group which dealt with the update also identified a number of topics which were raised but not fully

privacy protection through an approach which is based on risk management. Consequently, the revised 2013 version also deals with privacy management programs including operational (and data breach) mechanisms.[481] Just like Convention 108, these guidelines also incorporate the principle of purpose specification and the notion of incompatibility.[482] Apart from these guidelines, the OECD also issued recommendations on cross-border co-operation in the enforcement of laws protecting privacy in 2007.[483] Even though OECD's guidelines are non-binding, they can nevertheless be considered a milestone initiative, also because their material content and underlying principles are congruent with the Council of Europe Data Protection convention.[484]

6. Further Conventions, Resolutions and Guidelines[485]

Privacy is furthermore mentioned in various other legal instruments at international level,[486] for example Article 14 of the United Nations Convention on Migrant Workers,[487] Article 16 of the United Nations Convention on rights of the Child,[488] as well as Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[489] The United Nations 2015 Guidelines on Consumer Protection[490] define the protection of consumer privacy as a general principle and specify that "*businesses should protect consumers' privacy through a combination of appropriate control, security, transparency and consent mechanisms relating to the collection and use of their personal data*" as part of "principles for good business practices". In 2016, the United Nations moreover issued a resolution on the right to

addressed as part of the review process and which could be considered as candidates for possible future study: https://www.oecd-ilibrary.org/docserver/5k3xz5zmj2mx-en.pdf?expires=1549789641&id=id&accname=guest&checksum=C6CB4D94745FBAC6759C9EA424F70745. Retrieved October 2, 2021.

[481] Background information is available at http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm. Retrieved October 2, 2021.

[482] Nikolaus Forgo et al.: The principle of purpose limitation in big data, p. 25.

[483] Source: https://edps.europa.eu/sites/edp/files/publication/2013-09-09_oecd_guidelines_en.pdf. Retrieved October 2, 2021.

[484] A difference is that the OECD Guidelines, unlike the Council of Europe Data Protection Convention, do not mention the need to establish national data protection authorities, a typical (important) element in European data protection rules.

[485] The difference between these instruments is that some are legally binding, and some are not. Corresponding background information can be found at: http://www.unesco.org/new/en/social-and-human-sciences/themes/advancement/networks/larno/legal-instruments/nature-and-status/. Retrieved October 2, 2021.

[486] The Electronic Frontier Foundation provides background information on further international privacy standards on their website, available at https://www.eff.org/de/issues/international-privacy-standards. Retrieved October 2, 2021.

[487] 1990 International Convention on the Protection of the Rights of all Migrant Workers and Members of Their Families, UN Doc. A/RES/45/158, available at http://www.un.org/documents/ga/res/45/a45r158.htm. Retrieved October 2, 2021.

[488] 1989 Convention on the Rights of the Child, UN Doc. A/RES/44/25, available at http://www.un.org/documents/ga/res/44/a44r025.htm. Retrieved October 2, 2021.

[489] 1966 International Covenant on Civil and Political Rights, UN Doc. A/6316, available at https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf. Retrieved October 2, 2021.

[490] Available at https://unctad.org/en/PublicationsLibrary/ditccplpmisc2016d1_en.pdf. Retrieved October 2, 2021.

privacy in the digital age[491] in which the UN actively call upon states and upon business enterprises and in which they reaffirm the right to privacy, "*according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, as set out in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights*".

II. Global Trade Agreements

When it comes to privacy and data protection at an international level, many think of United Nations Universal Declaration of Human Rights, Convention 108+ or the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. But the collection, processing and transfer of data including personal information are not only governed by data protection laws (and other areas of law, depending on the specific case in question): there seems to be little awareness that global trade and investment agreements in fact do address the issue of handling (i.e. transfer) of data: rules on trans-border data flows are incorporated in a variety of global agreements, for example the World Trade Organization's General Agreement on Trade and Services (GATS)[492], the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)[493] or the Comprehensive Economic and Trade Agreement (CETA) between Canada and the European Union.[494] These agreements are legally binding and have in common that they set forth (minimum) standards and core norms of non-discrimination, including protections against unjustified data localization requirements: the Trans-Pacific-Partnership Agreement, for example, prohibits members from requiring companies located in a TPP country to build data centers in the market countries in which they serve.[495] Consequently, any future legislation which foresees data localization may be challenged owing to the existing overarching trade law framework.[496]

[491] Source: https://digitallibrary.un.org/record/848969/files/A_C-3_71_L-39_Rev-1-EN.pdf. Retrieved October 2, 2021.

[492] The text of the General Agreement on Trade in Services (GATS) is available at WTO's homepage: https://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm. Retrieved October 2, 2021.

[493] The text of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) as well as associated documents are available at https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents/Pages/official-documents. Retrieved October 2, 2021.

[494] The text of the Comprehensive Economic and Trade Agreement (CETA) between Canada and the EU is available at https://trade.ec.europa.eu/doclib/docs/2014/september/tradoc_152806.pdf. Retrieved October 2, 2021.

[495] Mark Mao et al: Data Privacy – the Current Legal Landscape. Article published February 2016, available at https://iapp.org/media/pdf/resource_center/TS_CurrentLegalLandscape_February_2016.pdf. Retrieved October 2, 2021.

[496] An overview over global trade agreements is provided by Sean Stephenson, Paul Lalonde in their 2019 article: The Limits of Data Localization Laws. The article was published August 9, 2019, and is available at http://www.dentonsdata.com/the-limits-of-data-localization-laws-trade-investment-and-data/. Retrieved October 2, 2021.

III. EU level

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

The General Data Protection Regulation[497] replaces[498] the 1995 Data Protection Directive which was adopted at a time when the internet was in its infancy, at a time when Meta and so many other things so many people nowadays consider indispensable did not exist. GDPR was introduced as the directive failed to achieve the desired harmonization[499] throughout the European Union due to different implementation and application of its provisions within various member states. GDPR aims at reducing fragmentation and harmonizing legislation and legislative practice, but these goals are somewhat questionable due to the rather huge number of so-called opening clauses[500] in important areas of practice like employment data protection. The regulation nevertheless marks the biggest single shift in data protection laws ever due to its expanded scope and owing to the introduction of a new framework for data protection with increased obligations for organizations including serious penalties for non- compliance.[501]

2. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

The directive on privacy and electronic communications[502] provides data protection rules for telecommunications networks and internet services and is due to be repealed.[503] The so-called ePrivacy Directive[504] (PECD) covers topics such as treatment of traffic data, spam and cookies as well as

[497] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679. Retrieved October 2, 2021.

[498] Further details including a GDPR timeline can be found at https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Retrieved October 2, 2021.

[499] David Bender: GDPR harmonization: Reality or myth? Article published on June 7 2018, available at https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/. Retrieved October 2, 2021.

[500] The GDPR contains dozens of opening clauses allowing EU member states to put national data protection laws in place to supplement the GDPR. A summary on this topic is provided by Baker McKenzie in their 2018 GDPR National Legislation Survey, available at https://www.bakermckenzie.com/-/media/minisites/tmt/files/gdpr_national_legislation_survey.pdf?la=en. Retrieved October 2, 2021.

[501] Global Legal Group: The International Comparative Legal Guide to data protection, 5th edition 2018, available at https://iapp.org/media/pdf/resource_center/Legal_Guide_To_Data_Protection_2018.pdf. Retrieved October 2, 2021.

[502] Source: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058. Retrieved October 2, 2021.

[503] In the meantime, the ePrivacy Directive was amended in 2009 by Directive 2009/136/EC, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0136. Retrieved October 2, 2021.

[504] The term / spelling of “ePrivacy” is taken from the EUR lex (Access to European Union Law) website: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52017PC0010. Retrieved October 2, 2021.

confidentiality of information.[505] This directive is highly relevant for businesses, especially in the area of (online) marketing activities, and that is why its interpretation, application and further development is followed with great interest: already in 2017, the European Commission adopted a proposal[506] for a corresponding regulation which faced controversial discussion, not only between the European Parliament and the Council of the European Union, but also between various other stakeholders.[507] Views vary depending on the respective interests, but what is clear is that this new regulation will be of great importance for businesses, because many techniques (e.g. tracking, fingerprinting, etc.) would be directly affected[508] by potential new rules on the need for consent or the use of content and metadata.[509] The hopes around the ePrivacy Directive were about the protection of online privacy by enabling users to better control how their data is handled, for example by not allowing certain types of cookies without consent. Some years ago, the EU Parliament had spoken out in favor of the establishment of a Do-Not-Track-standard,[510] but latest developments indicate many concessions to the data-processing industry by allowing companies and authorities to use (meta-)data under certain conditions, including interventions in terminal equipment like browsers to read user information and other associated data stored on a device; in addition, data retention shall remain permissible, although the European Court of Justice set high hurdles and repeatedly overturned contradicting national laws.[511] The current version seems to miss a provision previous EU Commission and Parliament drafts included regarding consent management via browser settings to enable privacy protections by default.[512]

[505] Details on the ePrivacy Directive can be found at https://www.epic.org/international/eu_privacy_and_electronic_comm.html. Retrieved October 2, 2021.

[506] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010. Retrieved October 2, 2021.

[507] The position of the EDPS on ePrivacy can be found at https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en.LIBE's assessment of the Commission's proposal on Privacy and Electronic Communications is available at http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU%282017%29583152_EN.pdf. Retrieved October 2, 2021.

[508] In 2018, the law firm of Brinkhof Advokaten prepared a paper for the Centre for Information Policy Leadership which provides background information on the relationship of "EPR vis-à-vis GDPR: A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation", available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-brinkhof_epr_study.pdf. Retrieved October 2, 2021.

[509] The law firm of Linklaters provides an overview on the status of the ePrivacy Regulation. It is available at https://www.linklaters.com/de-de/insights/publications/tmt-news/tmt-news---june-2017/eu---status-of-the-proposed-eprivacy-regulation-tighter-cookie-rules-and-more. Retrieved October 2, 2021.

[510] Christiane Schulzki-Haddouti: Scharfe E-Privacy-Verordnung verabschiedet: Mehr Datenschutz, klares Nein zu Hintertüre. Article published October 26 2017, available at https://www.heise.de/newsticker/meldung/Scharfe-E-Privacy-Verordnung-verabschiedet-Mehr-Datenschutz-klares-Nein-zu-Hintertueren-3874221.html. Retrieved October 2, 2021.

[511] Stefan Krempl: E-Privacy-Verordnung: EU-Rat für Vorratsdatenspeicherung und Cookie-Walls, Article published February 11 2021, available at https://www.heise.de/news/E-Privacy-Verordnung-EU-Rat-fuer-Vorratsdatenspeicherung-und-Cookie-Walls-5051963.html. Retrieved October 2, 2021.

[512] Alexander Fanta: E-Privacy-Verordnung: EU-Staaten verwässern digitales Briefgeheimnis. Article published February 10 2021, available at https://netzpolitik.org/2021/eprivacy-verordnung-eu-staaten-verwaessern-digitales-briefgeheimnis/.

3. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure

The European Data Protection Supervisor (EDPS) stresses[513] the relevance of personal data to the concept of trade secrets, for good reasons: Due to the fact that personal data may form part of a trade secret and given that the holder of a trade secret holder in many cases will also be a data controller if information relating to identified or identifiable individuals is processed, this directive[514] is of importance to Big Data applications. The protection of know-how is not only a standard topic in non-disclosure agreements; this new directive will have a direct impact on organizational culture including the dealing with service providers (processors).[515] Another aspect is that is traditionally recognized that, if an information is a secret, it has a commercial value,[516] and correspondingly, the same is discussed for personal data.[517] Know-how protection therefore is another important factor in the introduction of Big Data.

4. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

The European Commission proposed the EU Network and Information Security Directive[518] as part of EU's cyber-security strategy which aims at strengthening resilience for providers of critical infrastructure services and applies to sectors such as health and energy, transport, banking, water, as well as digital service providers.[519] This directive (also known as the Cyber-security Directive, in

[513] Source: https://edps.europa.eu/sites/edp/files/publication/14-03-12_trade_secrets_en.pdf. Retrieved October 2, 2021.

[514] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943. Retrieved October 2, 2021.

[515] Thomas Hoeren and Reiner Münker: Die EU-Richtlinie für den Schutz von Geschäftsgeheimnissen und ihre Umsetzung unter besonderer Berücksichtigung der Produzentenhaftung, Wettbewerb in Recht und Praxis, vol. 2, 2018 pp. 150-155, available at https://www.itm.nrw/wp-content/uploads/Die-EU-Richtlinie.pdf. Retrieved October 2, 2021.

[516] Source: https://deutschland.taylorwessing.com/de/der-lange-weg-zum-geheimnisschutzgesetz-ein-update. Retrieved October 2, 2021.

[517] Marc van Lieshout: The Value of Personal Data. In: Jan Camenisch, Simone Fischer-Hubner, Marit Hansen (eds). Privacy and Identity Management for the Future Internet in the Age of Globalisation; pp. 26-38; London: Springer Verlag 2015.

[518] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG. Retrieved October 2, 2021.

[519] Digital service providers (online marketplaces, online search engines and cloud computing services) are subject to slightly different rules: Lawrence Kalman: The GDPR and NIS Directive – a new age of accountability, security and trust?, presentation held during the 2017 OWASP summit, available at https://www.owasp.org/images/b/b9/Olswang_slides_-_GDPR_and_NIS_Directive_-_accountability_security_and_trust_-_25_Jan_2017.pdf. Retrieved October 2, 2021.

brief: NISD) is the first piece of EU-wide cyber-security legislation,[520] and even though it does not apply to all companies, it may serve as an orientation in terms of security standards, because all businesses have to take care of the security of processing.[521] Moreover, it has significant intersections with GDPR in terms of accountability, one of GDPR key elements,[522] and it also includes a wide range of organizational requirements (e.g. risk management, incident reporting).[523] NISD and GDPR, however, are not exactly the same as, for example, NISD breach notification requirements extend beyond those of GDPR.[524] The European Commission announced to review the NIS Directive by the end of 2020.[525]

5. Regulation of the European Parliament and of the Council on ENISA, the "EU Cyber-security Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cyber-Security Certification

This regulation,[526] also called Cyber-security Act, aims to achieve a high level of cyber-security and cyber resilience, and to reinforce the role of the European Union Agency for Cyber-security as the European Union's center of cyber-security expertise in the framework of a permanent mandate. Among other things, ENISA will be responsible for a cyber-security certification framework. This is remarkable insofar as this initiative is the first internal market law that creates that takes up the challenge of enhancing the security of IoT devices and connected products. This way, a one-stop shop for cyber-security certification will be created that could lead to the removal of potential market-entry barriers and significant cost saving for enterprises, since they would otherwise need to apply for several certificates in several EU countries.[527] Businesses could use such certifications to have their security features independently verified and strengthen users' trust in their products and services.

[520] Source: European Agency for Network and Information Security, https://www.enisa.europa.eu/topics/nis-directive. Retrieved October 2, 2021.

[521] GDPR Article 32.

[522] GDPR Article 5 (2) "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')".

[523] Background information is available at https://www.twobirds.com/en/news/articles/2016/global/new-security-and-reporting-requirements-for-infrastructure-providers-and-certain-digital-businesses. Retrieved October 2, 2021.

[524] Source: International Association of Privacy Professionals (IAPP): NIS + GDPR = A New Breach Regime in the EU, available at https://iapp.org/news/a/nis-gdpr-a-new-breach-regime-in-the-eu/. Retrieved October 2, 2021.

[525] After a period of public consultation the European Commission started in June 2020, see https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive. Retrieved October 2, 2021.

[526] Source: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0151+0+DOC+PDF+V0//EN. Retrieved October 2, 2021.

[527] The European Commission offers detailed information on the Cyber-security Act and ENISA's role and tasks including advantages for businesses on their website, which is available at https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en. Retrieved October 2, 2021.

6. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union

The above regulation[528] is, unlike the ePrivacy Regulation, already in force[529] and is part of the EU's digital single market strategy.[530] It aims at promoting data economy and the development of new technologies by removing existing data localization requirements and at enabling storage of data[531] in multiple locations across the European Union. New technologies include artificial intelligence,[532] and that makes this regulation particularly interesting to Big Data applications. As for practical implications, it is foreseeable that problems will arise from the demarcation between personal (identifiable) and non-personal data such as aggregate and anonymized data. The fundamental underlying problem is that anonymization is hard to achieve:[533] an investigation of as little as four spatiotemporal points (credit card metadata) was enough to uniquely re-identify 90 % of individuals behind the data.[534] This example of reverse engineering shows that it is necessary to rethink and question currently implemented (technical) privacy standards.[535] Given the growing relevance of machine-generated, non-personal data in the Industry 4.0, some authors stress the necessity of regulations for this type of data as so far, the focus of regulation is with personal data.[536]

7. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

[528] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.303.01.0059.01.ENG. Retrieved October 2, 2021.

[529] It will be applicable in all European Union member states as of May 2019.

[530] Source: https://www.consilium.europa.eu/en/policies/digital-single-market/. Retrieved October 2, 2021.

[531] With exceptions where data localization restrictions are justified on grounds of public security: http://www.mondaq.com/x/762982/data+protection/New+Regulation+Favors+Free+Flow+Of+NonPersonal+Data+In+The+EU. Retrieved October 2, 2021.

[532] See corresponding press release 603/18 from November 9, 2018, available at https://www.consilium.europa.eu/en/press/press-releases/2018/11/09/free-flow-of-data-eu-adopts-new-rules/. Retrieved October 2, 2021.

[533] In their 2014 opinion (05/2014) on anonymization techniques, the Article 29 Working Party explains how difficult it is to anonymize personal data. Opinion 05/2014 is available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Retrieved October 2, 2021.

[534] Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh and Alex Pentland: Unique in the shopping mall: On the reidentifiability of credit card metadata, Science 2015, vol. 347, issue 6221, pp. 536-539, available at http://science.sciencemag.org/content/347/6221/536/tab-pdf. Retrieved October 2, 2021.

[535] Sector-specific reactions occurred, e.g. the Payment Services Directive (PSD2) for the banking industry which introduces “regulatory technical standards enabling consumers to benefit from safer and more innovative electronic payments”, source: European Commission 2017 fact sheet on PSD2, available at http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm. Retrieved October 2, 2021.

[536] Jan Christian Sahl: Brauchen wir ein Datenschutzrecht für Maschinendaten? Newspaper interview on May 7 2018, available at https://www.marktundmittelstand.de/recht-steuern/die-dsgvo-gilt-auch-fuer-personenbezogene-maschinendaten-1271211/ Retrieved October 2, 2021.

This regulation[537] concerns the processing of personal data by European Union institutions, bodies, offices and agencies. It abolished Regulation (EC) No 45/2001[538] which also dealt with the protection of individuals with regard to the processing of personal data by community institutions, and which established the European Data Protection Supervisor to be the independent data protection authority which is tasked to ensure that the right to privacy is respected by European institutions and bodies.[539] It is noteworthy that both, the predecessor and the current version of the regulation contain provisions on compatible processing of personal data, which is important for the interpretation of purpose limitation and thus of relevance to Big Data and AI uses.

8. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Like the GDPR, the Law Enforcement Directive[540] also entered into force in May 2018. The directive is a little-known, much overlooked part of the EU data protection reform package.[541] This directive applies when a competent authority processes personal data for law enforcement purposes, i.e. for preventing, investigating, detecting and prosecuting crimes. In practice, so-called predictive policing relies on AI, for example for the calculation of geographic threat scores.[542] However, the Law Enforcement Directive also applies to processing that is conducted by private bodies, as long as the processing purpose is law enforcement, meaning that, for example, public transportation may rely on this directive in relation to ticket offences. The applicability of this directive is therefore not limited to the public sector and needs to be evaluated on a case-by-case basis, which can be challenging in the context of public–private partnerships.[543]

[537] Source: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018R1725. Retrieved October 2, 2021.

[538] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001R0045. Retrieved October 2, 2021.

[539] Source: https://edps.europa.eu/data-protection/our-work/subjects/regulation-452001_en. Retrieved October 2, 2021.

[540] The text of the Law Enforcement Directive is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG. Retrieved October 2, 2021.

[541] Paul de Hert, Vagelis Papakonstantinou: The new police and criminal justice data protection directive: A first analysis, New journal of European criminal law 2016, vol. 7, issue 1, pp. 7-19, available at https://research.tilburguniversity.edu/en/publications/the-new-police-and-criminal-justice-data-protection-directive-a-f#:~:text=Allegedly%20the%20Police%20and%20Criminal%20Justice%20Data%20Protection,EU%20legislative%20agenda%20towards%20the%20end%20of%202015. Retrieved October 2, 2021.

[542] Detailed examples and use cases are summarized by Privacy International on their website, available at https://www.privacyinternational.org/examples/predictive-policing. Retrieved October 2, 2021.

[543] Nadezhda Purtova: Between the GDPR and the Police Directive: navigating through the maze of information sharing in public–private partnerships, International Data Privacy Law, vol. 8, issue 1, 2018, pp. 52–68, available version at https://doi.org/10.1093/idpl/ipx021. Retrieved October 2, 2021.

9. Directive 96/9/EC of the European Parliament and of the Council on the legal protection of databases

The Database directive[544] was enacted as the need for database protection has increased in the digital age, because copying of data at large scale is easy. Although most of the content of social networks was created by the users and not by operators, harvesting of information and personal data on such platforms may infringe the rights of the platform operator.[545] The directive aims at preventing competitors from skimming off investments by providing a specific (sui generis) property right for analogue and digital databases that is unrelated to other forms of protection such as copyright. The Directive protects databases by copyright if they are original; non-original databases such as compilations of legal cases and laws, listings of advertisements or databases of scientific publications can also be protected, if the investment in obtaining, verifying and presenting the data was substantial.[546]

10. Directive 2000/43/EC on equal treatment and against discrimination and Directive 2004/113/EC on equality in the access to and supply of goods and services

When implementing and applying Big Data analytics and AI applications for eligibility decisions, for example in the context of housing, lending or healthcare, companies should also consider further directives which are primarily concerned with preventing (gender-based) bias and promoting fairness, for example the Directive against discrimination on grounds of race and ethnic origin (Directive 2000/43/EC)[547] and Directive 2004/113/EC[548] on equality in the access to and supply of goods and services. It can thus be said that discrimination and equal treatment are addressed at EU level, however, these directives have not been discussed in the context of Big Data or Artificial Intelligence.

11. Directive 2000/78/EC against discrimination at work on grounds of religion or belief, disability, age or sexual orientation; see also Directive 2006/54/EC equal treatment for men and women in matters of employment and occupation

[544] Source: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31996L0009. Retrieved October 2, 2021.

[545] Thomas Hoeren: Big Data und Recht, p. 129, C.H. Beck publishing Munich 2014.

[546] Background information is available at https://ec.europa.eu/digital-single-market/en/protection-databases. Retrieved October 2, 2021.

[547] The text of the Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin is available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0043:en:HTML. Retrieved October 2, 2021.

[548] Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32004L0113. Retrieved October 2, 2021.

Ditto for other directives at EU-level that are concerned with equal treatment at work, for example Directive 2000/78/EC[549] against discrimination at work on grounds of religion or belief, disability, age or sexual orientation; see also Directive 2006/54/EC[550] equal treatment for men and women in matters of employment and occupation. Owing to the fact that the hiring process nowadays often starts with background checks and resume screenings, workplace decisions are very often being (partially) automated, and therefore, Artificial Intelligence plays a role in the employment context.

12. Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

Difficulties may also arise from the fact that the existing Product Liability Directive[551] has not been amended to reflect specific implications Big Data and AI applications may involve: The European Commission has determined that the directive for defective products, which has been in place for over 30 years, requires further work, but is still fit for purpose.[552] But AI-driven products should be examined in the light of product liability to properly address the risk of accidents[553] and damage resulting from interaction with humans. The same applies to the General Product Safety Directive[554] which imposes general safety requirements on any product put on the market for consumers: it should be reviewed against modern safety and security threats as well as present cyber-security standards[555]

[549] The text of the Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0078. Retrieved October 2, 2021.

[550] Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0054. Retrieved October 2, 2021.

[551] The text of the Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374. Retrieved October 2, 2021.

[552] Report on on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) issued on May 7, 2018, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1525769201372&uri=COM:2018:246:FIN. Retrieved October 2, 2021.

[553] For example, self-driving car fatalities: ‘Wired’ reported about the latest Tesla car crash on May 16, 2019: https://www.wired.com/story/teslas-latest-autopilot-death-looks-like-prior-crash/. Retrieved October 2, 2021.

[554] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety can be found at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0095. Retrieved October 2, 2021.

[555] See also rules on internet-connected devices. Background information on the IoT regulatory framework for Europe is provided by Vodafone in their 2019, and is available at https://www.vodafone.com/content/dam/vodcom/files/public-policy/iot-whitepaper/IoT_whitepaper_.pdf. Retrieved October 2, 2021.

13. Directive (EU) 2019/770 on digital content

The Directive on digital content[556] is not related to Big Data or Artificial Intelligence, but it is related to the use of personal data: business models in which consumers provide data in exchange for a digital content or service – a phenomenon that has been under discussion for many years within the privacy community. The Digital Content Directive aims to harmonize the legal relationship between consumers and traders for the supply of digital contents and it "*gives consumers the right to a remedy when digital content or a digital service is faulty, regardless of whether they paid for it or only provided personal data.*"[557] But the proposal has sparked some controversy for possibly introducing an instrument that acknowledges contracts in which personal data is being treated as contractual "*counter-performance*"[558] – in times where NGOs like "None Of Your Business" (NYOB) file hundreds of complaints against cookie banners[559] and paywalls which requires users to "*buy back their own data*".[560]

14. Further Directives to consider

Depending on the intended use of Artificial Intelligence, further Directives may be relevant, and their importance may not be apparent at first sight: owing to the fact that Artificial Intelligence is part of autonomous weapons, the Directive on defence-related products[561] comes into play – or even the BioTech Directive:[562] many say that Big Data and AI will become instrumental in Life Sciences,[563] and few people may be *aware of the fact that research has pushed so far as to store information and data in DNA: "DNA molecules can store up to 215 petabytes, or 215 million gigabytes, of data in a*

[556] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0770. Retrieved October 2, 2021.

[557] Source: European Commission website, news on Digital contract rules, available at https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/digital-contract-rules_en. Retrieved October 2, 2021.

[558] Weizenbaum Institut: Statement on the Proposed Digital Content Directive. The statement was published July 4 2018, and is available at https://www.weizenbaum-institut.de/index.php?id=107&tx_news_pi1%5Baction%5D=&tx_news_pi1%5Bcontroller%5D=&tx_news_pi1%5Bnews%5D=36&L=5&cHash=416e3183f5ac501a1777c33e947ff6ae. Retrieved October 2, 2021.

[559] Source: NYOB's website. Blog entry published August 10 2021, available at https://noyb.eu/en/noyb-files-422-formal-gdpr-complaints-nerve-wrecking-cookie-banners. Retrieved October 2, 2021.

[560] Source: NYOB's website. Blog entry published August 13 2021, available at https://noyb.eu/en/news-sites-readers-need-buy-back-their-own-data-exorbitant-price. Retrieved October 2, 2021.

[561] Directive 2009/43/EC on intra-EU transfers of defence-related products is available at https://ec.europa.eu/growth/sectors/defence/transfers-products_en#:~:text=The%20transfer%20directive%20Directive%202009%2F43%2FEC%20on%20intra-EU%20transfers,for%20transfers%20of%20defence-related%20products%20within%20the%20EU. Retrieved October 2, 2021.

[562] Directive 98/44/EC on the legal protection of biotechnological inventions is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31998L0044. Retrieved October 2, 2021.

[563] Arlindo Oliveira: Biotechnology, Big Data and Artificial Intelligence. Biotechnology Journal 2019, vol. 14, issue 8. The article is available at https://doi.org/10.1002/biot.201800613. Retrieved October 2, 2021.

single doubled stranded molecule, making it one of the highest storage density mediums in the world (... which is much more) than we can currently create, so there has been a lot of focus in trying to harness the power and data storage capabilities of DNA for our (...)data storage systems."[564]

15. Rules (Directives) which are no longer in force

The following Directives are no longer in force, but they are useful to understand the developments, discussions and the overall context:

a) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

In 1995, the European Data Protection Directive[565] was created. It regulated the processing (including the collection, use, storage, disclosure, and destruction) of personal data within[566] the European Union. The Directive was the first framework for data protection regulation at European Union level and an important component of the European Union's data protection rights for more than two decades. The Directive intended to harmonize data protection law across Europe.[567] Due to the fact that member states must transpose directives into national law, this directive served as basis for numerous national data protection laws throughout the European Union. Differences in terms of content and timing of implementation of the requirements lead to somewhat differing levels of privacy protection even within the European. This also resulted in cases of conflict between European and national law, especially when there were overlaps with other areas of law, for example competition laws, since data protection laws are not the only issue to address for marketing activities. As regards the processing of personal data, Article 6 (1) b of the Data Protection Directive stipulated that member states shall provide that personal data must be "(…) *collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that member states provide appropriate safeguards*". Rules on compatible processing of personal data including exceptions for statistical or scientific purposes are important for Big Data applications.

[564] Liam Critchey: Storing Information and Data with DNA. Article published August 11 2020, available at https://www.electropages.com/blog/2020/08/storing-information-and-data-dna. Retrieved October 2, 2021.

[565] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046. Retrieved October 2, 2021.

[566] Details on the scope (applicability) of the directive can be found in article 4 of the directive, see https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. Retrieved October 2, 2021.

[567] Jürgen Kühling: Die Europäisierung des Datenschutzrechts – Gefährdung deutscher Grundrechtsstandards? C.H. Beck publishing Munich 2014, p. 12.

b) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

The Data retention directive[568] obliged electronic communication service providers to retain traffic and location data for a certain period. The directive was invalidated in 2014 in a cutting-edge decision: Even though it was recognized that the purpose of the directive genuinely satisfies an objective of general interest, the CJEU[569] concluded that the directive was incompatible with Article 7 and 8 of the Charter. The reason for this was that, if traffic and location data are taken as a whole, this provides for a detailed picture of individuals' private lives, and therefore constitutes a serious interference with fundamental rights to respect for private life and to the protection of personal data. In another case,[570] the CJEU found that the generalized retention of traffic and location data may affect the use of electronic communication and how users' exercise their freedom of expression guaranteed in Article 11 of the Charter. Even though this directive is no longer in force, it cannot be disregarded as the CJEU's decision may well serve as an indicator when it comes to judging storage periods.[571] Moreover, the battle for the retention (use) of traffic and location data of telecommunications is not over: several member states are putting pressure on the European Council to adopt rules that allow for the retention of metadata of communications; their ideas are far-reaching and could change existing data protection rules.[572] Some member states made it to advocate for the introduction of provision allowing for data retention measures in the Council version of the ePrivacy Regulation.[573] In this regard, it is important to note that various national constitutional courts[574] as well as the European Court of Justice continue with decisions that limit data retention measures.[575]

[568] Source: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

[569] CJEU press release from April 8, 2014, available at https://edps.europa.eu/press-publications/press-news/press-releases/2014/press-statement-cjeu-rules-data-retention_en. Retrieved October 2, 2021.

[570] Tele2 Sverige, source: https://www.ebu.ch/files/live/sites/ebu/files/News/2017/02/Legal%20Case%20note%20Tele2%20Sverige%20and%20Tom%20Watson%20a.o.pdf. Retrieved October 3, 2021.

[571] Those that are not governed by explicit requirements, e.g., tax matters.

[572] Alexander Fanta: France, Spain push for new EU data retention law. Article published March 5, 2021, available at https://netzpolitik.org/2021/urgently-needed-france-spain-push-for-new-eu-data-retention-law/. Retrieved October 3, 2021.

[573] The Council version of the ePrivacy Regulation is available at https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf. Retrieved October 3, 2021.

[574] Marek Zubik, Jan Podkowik, Robert Rybski: European Constitutional Courts towards Data Retention Laws, Law, Governance and Technology Series, Springer Nature Switzerland AG 2021.

[575] For example, in K. v. Prokuratuu (Case C-746/18H): The European Court of Justice found that crime has to be serious in order to allow for access to traffic and location data, this way limiting data retention measures. The corresponding press release No. 29/21 is available at https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-03/cp210029en.pdf. Retrieved October 3, 2021.

IV. GDPR novelties, goals and gaps

GDPR sets forth important principles like accountability, lawfulness, fairness and transparency, purpose and storage limitation, data minimization, accuracy as well as integrity and confidentiality[576] and introduced novelties. However, GDPR also poses challenges, be it because of its extra-territorial scope and new sanctions, or because of new requirements, enhanced data subject rights and indeterminate legal terms.

1. New scope

a) Territorial scope

The Data Protection Directive's territorial scope comprised member states and non-EU members which are a part of the European Economic Area.[577] In comparison to the Data Protection Directive, the scope of the GDPR was expanded materially and territorially, for good reason: Personal data is collected and shared globally, and therefore, inconsistent (national) data protection laws are neither appropriate nor timely.[578] GDPR captures much more overseas organizations, because it not only applies to organizations which are established within the European Union, but also to organizations that are not established in the EU: according to GDPR Article 3 (1), the "*Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*". Recital 22 says that an "*establishment implies the effective and real exercise of activity through stable arrangements*" and clarifies that "*the legal form of such arrangements (...) is not the determining factor*". This leads to the result that there is a wide spectrum of what might be caught by GDPR; depending on the circumstances, perhaps even single individual sales representatives may fall under the Regulation. At present, there are two relevant decisions with regard to the question of whether or not European data protection law is applicable. In 2014, the CJEU ruled that that Google Inc. with EU based sales and advertising operations in Spain was established within the EU.[579] The court delivered another landmark ruling in 2015 in the so-called Weltimmo-case. The court considered the meaning of establishment and concluded that, because Weltimmo pursued real and effective activity in Hungary, it had an establishment in Hungary and is therefore subject to Hungarian data protection laws, even if

[576] See GDPR Art. 5.

[577] Iceland, Liechtenstein and Norway; Switzerland is a member of EFTA but does not take part in the EEA: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Aem0024. However, the adequate protection of personal data in Switzerland was acknowledged by the Commission: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0518. Retrieved October 24, 2021.

[578] Christopher Kuner, Fred Cate, Christopher Millard and Dan Svantesson: The Challenge of Big Data for Data Protection, International Data Privacy Law 2012, vol. 2, no. 2, p. 48.

[579] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=DE.

Weltimmo is a Slovakian property website.[580] Weltimmo was thus subject to both, Hungarian and Slovakian data protection laws, i.e., the data protection of its home country. This decision dates back to 2015 when GDPR was not valid yet, and it is interesting insofar as the Regulation envisages that companies will only have to deal with one single DPA,[581] typically the supervisory authority in the member state in which the company has its EU headquarters. But what is more important, GDPR may also be applicable when the company has no establishment within the European Union. An organization is still caught by the Regulation if it processes personal data of data subjects who are in the Union and where the processing activities are related to "*the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behavior as far as their behavior takes place within the Union*".[582] Internet use profiling (Recital 24) is expressly referred to as an example of monitoring. Recital 24 underlines that the latter example refers to processors not established in the Union "*if data subjects within the Union are profiled*". The Regulation thus shifts its focus to the country of destination, and especially Recital 24 shows that, even though there is no single specific article on marketing, GDPR indeed targets the advertising industry if profiling and online tracking techniques are used. This approach is consistent and consequent as it means that companies who want to benefit from the European market will have to stick to EU rules. Finally, in order to allow for supervisory authorities to communicate with companies established outside the EU, the Regulation stipulates that a representative must be appointed.[583] Companies may not be able to escape or avoid GDPR's extra-territorial approach, but It remains to be seen whether or not companies will be able to forum shop by assigning their representative in a country where the supervisory authority is known to be rather tolerant as GDPR Article 27 (3) allows that the "*representative is established in one of the member states where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behavior is monitored, are.*"

b) Material scope

The Directive focused on those who determined purposes and means of the processing, and this way, it primarily addressed controllers. Under the Directive, processors were subject to obligations which were imposed on them through contractual relationships with data controllers. This became particularly evident in the case of "processing chains" when the general contractor had to ensure that all other suppliers who act as data processors observe the contractual regulations laid down by the controller. In contrast, GDPR imposes direct obligations on data processors, i.e., entities and suppliers

[580] Source: http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN. Retrieved October 24, 2021.

[581] See article 60 GDPR, the "*cooperation between the lead supervisory authority and the other supervisory authorities concerned*", also called "*one-stop-shop*"-mechanism.

[582] GDPR Article 3 (2a, b).

[583] GDPR Article 2.

which are engaged by a controller to process personal data on their behalf. GDPR are directly required to obey numerous specific obligations, for example the maintenance of records of processing activities,[584] the implementation of appropriate security standards,[585] the appointment of a Data Protection Officer if need be,[586] and the obligation to cooperate with supervisory authorities.[587] Just like controllers, processors are liable to sanctions if they fail to meet these requirements and they may also face claims for compensation.

2. New sanctions

a) Administrative fines

An important change under the Regulation is that businesses, in the event that they fail to comply with GDPR requirements, may be liable to pay fines of up to four percent of the annual worldwide turnover or 20 million Euros, whichever is higher.[588] In comparison to the previous legal setting under the Directive and national legislations,[589] this is a substantial increase in the maximum possible fine, especially given the fact that such fines are not calculated on the basis of a local entities' turnover:[590] The term undertaking is defined in GDPR Article 4 (19), and Recital 150 says that undertaking shall be understood "*to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes"*. Even though the TFEU does not define the term undertaking and despite of the fact that, like in every legal field, extensive case law must be considered, it may be assumed that a group of companies shall be regarded as part of the same undertaking; the concept of an undertaking encompasses every entity that engages in economic activities regardless of its legal status or how the entity is financed. Fines will therefore not be imposed by reference to the individual controller or processor, but by revenue of an undertaking, and GDPR this way follows the broad definition of undertaking in anti-trust and anti-bribery laws. This conceptual change represents a high impact for businesses and may thus lead to data protection being taken seriously in terms of compliance risk. This is especially true for multinational businesses as group revenues will be taken into consideration when calculating fines. This is underlined by the fact that national data protection supervisory bodies will be coordinating their work across EU member states, which will likely lead to a more pronounced enforcement, especially in an international context as the so-called "one-stop-shop" principle[591] shows:

[584] GDPR Article 30 (2).
[585] GDPR Article 32.
[586] GDPR Article 37.
[587] GDPR Article 31.
[588] GDPR Article 83.
[589] For example, the maximum fine in Germany prior to GDPR was 300000 EUR (§ 43 BDSG).
[590] Carlo Piltz: How German Data Protection Authorities interpret the GDPR. Article published July 5 2017, available at https://www.delegedata.de/2017/07/how-german-data-protection-authorities-interpret-the-gdpr/. Retrieved October 24, 2021.
[591] GDPR Article 60.

Even though this principle only applies to cross-border cases where the supervisory authority (SA) of the main establishment of the controller or processor will be competent to act as the lead SA and serve as a “one-stop-shop” to supervise all processing activities of that business, this mechanism is a perfect example of a cooperation procedure between several supervisory authorities and will thus ensure the desired consistency in law enforcement in the area of data protection. It is difficult to say how various national SAs will interpret the demand that administrative sanctions are effective, proportionate and dissuasive,[592] which of course depends on the case in question. However, recently, there has been a trend towards more drastic fines, and European data protection supervisory authorities announced the following penalties for GDPR violations: Vodafone: € 12 million,[593] Marriott: £ 18 million,[594] Google: € 50 million,[595] WhatsApp: € 225 million,[596] and Amazon holds the record for the highest penalty ever imposed to date with € 746 million.[597] However, sanctions and fines under GDPR, member-state data privacy and administrative as well as business criminal law are not the same: certain member states do not foresee for fines[598], other laws foresee that there must be a link to linked to a concrete, reproachable act of a natural person, which is not the same as the (group of) undertaking.[599] In addition, several cases have shown that regulator fines under GDPR may be contested[600], for a variety

[592] GDPR Article 83 (1).

[593] The EDPB reports about the case in their November 19 2020 news blog entry: Aggressive telemarketing practices: Vodafone fined over 12 million Euro by Italian DPA, available at https://edpb.europa.eu/news/national-news/2020/aggressive-telemarketing-practices-vodafone-fined-over-12-million-euro_en. Retrieved October 24, 2021.

[594] ICO fined Marriott International Inc on October 30 2020 for failing to keep customers’ personal data secure: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/. Retrieved October 24, 2021.

[595] The fine against Google was imposed by CNIL on January 21 2019. The regulator provides background on their decision on their website, which is available at https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc. Retrieved October 24, 2021.

[596] This fine was imposed by the Irish Data Protection Commission on September 2 2021. Background information on the case is provided on the regulator’s website: https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry. Retrieved October 24, 2021.

[597] Grand-Duchy of Luxemburg’s National Commission for Data Protection: Decision regarding Amazon Europe Core S.à r.l.: Press release published online on the SA’s homepage on August 6 2021, available at https://cnpd.public.lu/en/actualites/international/2021/08/decision-amazon-2.html. Retrieved October 24, 2021.

[598] Recital 151: Administrative Fines in Denmark and Estonia.

[599] Max Adamek, Julian Räder: DSGVO-Verstöße und das OWiG. Article published August 20 2021, available at https://haerting.de/wissen/dsgvo-verstoesse-und-das-owig/#:~:text=Gem.%20%C2%A7%2030%20Abs.%201%20Nr.%205%20OWiG,handelt%20und%20eine%20Straftat%20oder%20Ordnungswidrigkeit%20begangen%20hat. Retrieved January 22, 2022.

[600] The consultancy Datenschutz Lübbecke reports on a case in Berlin where a 14 million Euro fine was not successful because the fine imposed by the state data protection authority contained significant deficiencies. The article has been published on February 24 2021 on their company website: Peinlicher Vorfall: Deutsche Wohnen entkommt DSGVO-Bußgeld in Millionenhöhe. The article is available at https://datenschutz-luebbecke.de/blog/peinlicher-vorfall-deutsche-wohnen-entkommt-dsgvo-bussgeld-in-millionenhoehe/#:~:text=Blamage%20f%C3%BCr%20die%20Datenschutzbeh%C3%B6rde%20in%20Berlin%3A%20Allem%20Anschein,Beschluss%20vom%2018.%20Februar%202021%20eingestellt%20worden%20ist. Retrieved January 22 2022.

of reasons,[601] meaning that it is perhaps not as easy as envisaged to successfully issue penalties for GDPR violations.

b) Enforcement powers

Apart from administrative fines, supervisory authorities are provided with wide-ranging powers[602] to enforce compliance with the Regulation, for example the right to issue warnings, to perform audits, the power to compel a controller or processor to provide any information which is relevant to the performance of supervisory authority's duties as well as the possibility to impose a ban on processing.[603] Given the large number of conceivable infringements, which must always be assessed individually, it is difficult to tell how different supervisory authorities will implement their enforcement powers. Even though the GDPR has not been in force for long, the "multitude of regulators" that govern the use of personal information, the processing with the help of AI, including further bodies like the FTC or supervisory authorities in charge of competition law or consumer protection – set aside legal proceedings for claims for damages – shows that overlapping responsibilities could be problematic.

c) Representation of data subjects

On top of GDPR's administrative sanctions, the Regulation also allows for non-for-profit bodies, organizations or associations which are active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data and which disposes of statutory objectives that are in the public interest to lodge a complaint on behalf of the data subject and to exercise data subjects' rights including the right to receive compensation.[604] It is moreover necessary that such an association has been properly constituted in accordance with the law of a member state, meaning that not each and every NGO has the right to represent data subjects. Although this is not exactly the same as a US style class action, this genuine novelty increases the risk of group privacy claims, and this type of actions leads to further pressure to observe the new rules as business typically fear potential negative consequences for public opinion. Another fact to consider is emerging legal tech: the number of providers who are offering assistance for individuals to exercise their data subject rights is growing, and this poses further challenges, for example in the area of identification and valid representation of the individuals behind those claims.

[601] Alexander Fanta: Millionenstrafe gegen Österreichische Post AG aufgehoben. Article published December 2 2020, available at https://netzpolitik.org/2020/dsgvo-millionenstrafe-gegen-oesterreichische-post-ag-aufgehoben/.

[602] GDPR Article 58 (1 a).

[603] GDPR Article 58 (1 f). This shall be considered during the introduction of new tools, especially when there is a need to exchange with the works council for corresponding agreements.

[604] GDPR Article 80.

d) Claims by individuals

Claims under competition law by competitors and contractual claims by business partners are not at all a new phenomenon; these risks are part of business life, but what is new is that GDPR makes it considerably easier for individuals to bring private claims against data controllers or processors: GDPR Article 81 (1) states that "*any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered*". The inclusion of non-material damage means that claims of individuals are not limited to financial loss; even distress may justify a claim under GDPR Article 81. Recent developments show that there seems to be a trend to use data subject rights under GDPR to enforce other claims, namely in the context of severance claims in termination actions under labor law, which some consequently name as the "*golden handshake*".[605]

3. New goals

a) Broad applicability

GDPR's broad applicability is not only due to the broader material and territorial scope, but it also based on the fact that the Regulation has a broader definition of personal data. Personally identifiable information such as online identifiers is explicitly included, and it is important to note that Recital 26 not only sets a low bar for the prerequisite "identifiable", but it also makes clear that personal data can be given despite the fact that the organization which holds the data cannot itself identify a natural person: the only requirement is that, if anyone can identify a natural person using all means reasonably likely to be used, the relevant data may be considered personal data.[606] Businesses are often not aware that, even though they might not be able to read a set of data, the same set of data is subject to data protection law. The effect of broader applicability also applies to special categories of data whose definition was also broadened in GDPR Article 9 as genetic and biometric data were expressly included. While a few decades ago, for example iris-scans were only used in movies, today, every modern smartphone can be unlocked by using a fingerprint. The increase in technical applications with security features which process biometric data has led to a proportional increase in the applicability of

[605] Niko Härting: Mit der DSGVO zum "*Golden Handshake*" – von der Sprengkraft des "*Rechts auf Kopie*". Article published March 29 2019, available at https://www.cr-online.de/blog/2019/03/29/mit-der-dsgvo-zum-golden-handshake-von-der-sprengkraft-des-rechts-auf-kopie/. Retrieved October 24, 2021.

[606] GDPR Recital 26, sentence 3 and 4: "*To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*".

data protection law – with all data protection, security law and sector-specific consequences. Another point to consider is that the volume of data that is being produced rises at an incredible rate, because people dispose of more devices that generate more data, which again leads to a broader applicability of data protection laws.[607]

b) Uniform applicability

GDPR's broad applicability must be distinguished from the intended uniform applicability of the Regulation: GDPR clearly aims at ensuring a consistent and high level of protection of the rights and freedoms of natural persons with regards to the processing of their data,[608] and that can only be achieved if that level is equivalent in all member states. Even though a consistent and homogenous application of data protection laws is desired throughout the European Union, GDPR Article 23 clearly says that member state law may restrict "*by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard national security, defense, (…)".* This is just one example out of dozens of exceptions[609] for the regulatory scope of national legislators. It can therefore be said that the intended harmonization is relative insofar as many important issues and areas of law continue to be governed by national laws. Moreover, chapter IX of GDPR sets out various processing operations which include additional derogations and exemptions[610] such as processing and freedom of expression and information, processing and public access to official documents, processing of national identification numbers and processing in the context of employment.

c) Focus on accountability

Many of the principles laid down in GDPR Article 5 were also incorporated in the previous Directive, for example the principle of purpose limitation or the principle of data minimization: Article 6 of the Directive stipulated that "*personal data must be: (a) processed fairly and lawfully; (b) collected for*

[607] GDPR itself explains the development in Recital 6: "*Rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life.*"

[608] GDPR Recital 10.

[609] Lukas Feiler provides an overview over the topic in his presentation: Die 69 Öffnungsklauseln der DSGVO, presentation held on behalf of the law firm of Baker & McKenzie/Diwok Hermann Petsche Rechtsanwälte LLP & Co KG in Vienna during the meeting of JusIT on June 1, 2017, available at http://www.lukasfeiler.com/presentations/Feiler_Die_69_Oeffnungsklauseln_der%20DS-GVO.pdf. Retrieved October 24, 2021.

[610] GDPR Articles 85, 86, 87 and 88.

specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. (...) (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (...)" and concluded with the statement in paragraph 2 that "*it shall be for the controller to ensure that paragraph 1 is complied with*". In contrast, Article 5 (2) of the Regulation requires that the controller is responsible for and must be able to demonstrate compliance with all data protection principles. The difference is that, even though most of the standards existed before, the focus on accountability requires that the lawfulness of processing activities is established, meaning that the controller (and processor) has the burden of proof that business operations are compliant with the Regulation. And the relief some expected owing to the fact that, consent for example does not have to be given in writing, is not really given as consent must be verifiable, meaning that the controller also has to obey indirect documentation requirements. The accountability principle has become a core element of data protection in many other jurisdictions, for example Australia, Canada or Singapore.[611] Accountability leads to greater efforts with regards to the documentation of processes, the performance of controls, the conclusion of (outsourcing) contracts, and the overall legality of decisions including providing proof of legal grounds for processing which allow controllers to be able to demonstrate compliance. The accountability principle primarily manifests itself in documentation obligations, namely records of processing activities[612] and the performance of data protection impact assessments.[613] While the latter only applies to high risk processing, records of processing activities have to be present for every single data processing activity the controller carries out.[614] Provided that Big Data and AI applications may pose high risks to the rights and freedoms of individuals, it is likely that many such processing activities will result in the creation of impact assessments, particularly when profiling is in question, when sensitive personal data are processed or when publicly accessible areas are systematically monitored on a large scale.[615] Other mandatory requirements include the implementation of privacy by design and privacy by default,[616] the establishment of mechanisms for data breaches[617] and responses to data subject requests. The designation of a data protection officer is necessary, either when certain conditions are met or when

[611] In their March 5, 2019 blog entry, the law firm of Hunton Andrews Kurth refers to the results of the 2018 intelligence gathering operation on organizations' data privacy accountability practices which was carried out by GPEN, a global network of more than 60 DPAs around the world. This message is available at their privacy and information security law blog: https://www.huntonprivacyblog.com/2019/03/11/gpen-and-national-dpas-publish-sweep-results-on-privacy-accountability/. Retrieved October 24, 2021.

[612] GDPR Article 30.

[613] GDPR Article 35.

[614] The issue was solved inconsistently in previous data protection laws within the EU; in some jurisdictions (for example in Austria), there was a requirement to notify the national data protection authority of data processing operations. In others, e.g., in Germany, this requirement was not applied as a general rule as the controller was obliged to maintain the relevant documentation and to provide it to the DPO for checking purposes (see § 4 e, g of the pre-GDPR-BDSG). Under GDPR, there is a general necessity to keep extensive internal records of data protection activities.

[615] Recital 91 provides further background information and examples for data protection impact assessments.

[616] GDPR Article 25.

[617] GDPR Articles 33 and 34.

Union or Member State requires that a DPO is appointed.[618] This is yet another example of how the situation will continue to vary from one Member State to another, even with mandatory requirements. Data controllers may, on a voluntary basis, also opt for certification mechanisms to demonstrate compliance, but at present, standards for certification schemes are not available.[619]

d) Enhanced transparency

Transparency is a central principle in the GDPR because it promotes the objective of strengthening individuals' rights and underlines the importance of the lawfulness of processing personal information. Processing is only lawful if it is fair and transparent, and that is why any communication towards data subjects must be concise, transparent, intelligible and easily accessible, and use clear and plain language.[620] In connection with transparency requirements, one is immediately tempted to think about one specific use case: privacy notices on website that must be provided at the time data is collected.[621] But much of the content that is displayed as mandatory information on websites in fact is not solely based on data protection law. For example, neither the imprint nor terms and conditions or payment information is a genuine data protection issue; this is rather about consumer protection and provider identification, in some cases extended with information on the competent regulatory authority.[622] However, a positive development could be that GDPR's requirements might have already changed users' perceptions since information obligations apply to various (more) use cases.[623] But at the same time, a negative consequence is that this may lead to users being overwhelmed with information which in turn leads to information fatigue.[624] More importantly, transparency requirements are not only limited but in certain cases almost impossible to implement. First, explaining the underlying logic when automated decision-making including profiling is in question is restricted because controllers are not required to provide all kinds of information, not to mention protected business information (secrets). Second, in many cases, it is not feasible to explain all decisions made by a multitude of algorithms that work together, and that makes it very questionable how meaningful information about the underlying logic including the significance and the envisaged consequences of such processing for the data subject can be made available.[625] Even though GDPR made a genuine effort to better inform individuals, there seem to be restrictions that are hard to overcome.

[618] GDPR Article 37 (4).

[619] ICO: GDPR guidance – contracts and liabilities between controllers and processors, available at https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf. Retrieved October 24, 2021.

[620] GDPR Article 12 (1).

[621] GDPR Articles 13 and 14.

[622] This is mandatory for certain professions and subject to national legislation.

[623] For example: on websites, in apps, during the application process, and in many more scenarios.

[624] Müge Fazlioglu: Transparency and the GDPR: Practical guidance and interpretive assistance from the Article 29 Working Party. Article published December 14 2017, available at https://iapp.org/news/a/transparency-and-the-gdpr-practical-guidance-and-interpretive-assistance-from-the-article-29-working-party/.

[625] As required by Article 14 (2) lit. g

Lastly, transparency requirements not only concern data subjects, but also supervisory authorities. Online (website, etc.) information is available to the public and is thus suitable for investigations by supervisory authorities, which explains why several regulators took advantage of this rather simple way to examine compliance with privacy policy requirements or related issues such as technical measures.[626] In the event that companies are obliged to provide information, for example when the supervisory authority must be consulted in the framework of impact assessments,[627] this could perhaps also be considered a transparency requirement. At the same time however, the Regulation removed the need to register with supervisory authorities and notify them for certain endeavors, and this shows that GDPR is predominantly concerned with transparency towards affected individuals. As a consequence, it is left to the individual to intervene as opposed to the supervisory authority being in charge for the review of certain operations.[628]

e) Strengthening of data subject rights

Data subject rights have been rights have been considerably extended: the right to information and the right to access existed before, but the right to data portability and the explicit right to be forgotten are genuine novelties. Subject access rights must be answered during a certain period in time,[629] and given that the maximum period is three months, it cannot be said that businesses face time pressure with regard to this requirement. A practical problem arises out of the right to request information or a copy of personal data by electronic means:[630] first, the controller has to make sure that he is answering to the correct person, i.e. the data subject whose data are in question; second, answering by electronic means cannot and must not mean that simple e-mail is used as this way of communication is, unless encryption is used, not safe. This would necessarily lead to a violation of GDPR Article 32, security of processing. That means that something as simple as a demand by email necessarily leads to additional processes, primarily the identification of the individual.[631] This is the mandatory first step businesses need to think about, and depending on their business model (B2B or B2C) and the number of

[626] Already in 2017, the Bavarian State Office for Data Protection Supervision who is in charge of the private sector in Bavaria carried out an inspection on the encryption of websites in the framework of its cyber-security-initiative for the protection of personal data. The corresponding press release is available at https://www.lda.bayern.de/media/pm2017_08.pdf. Retrieved October 24, 2021.

[627] GDPR Article 36 (1).

[628] For instance, in Austria, where § 16 of the Federal Austrian Data Protection Law (DSG 2000) required companies to do so. Background information can be found at the official (archived) website: https://web.archive.org/web/20161220005959/https://www.dsb.gv.at/rechtsgrundlagen-und-beschreibung. Retrieved October 24, 2021.

[629] As a basic rule, such requests have to be answered within one month; this period may be extended by two further months where necessary, for example in the event that the request is of complex nature: GDPR Article 12 (3).

[630] GDPR Article 12 (3).

[631] The State Commissioner for Data Protection and Data Security in the German state of Baden-Württemberg dealt with this neglected topic. Their findings are available in the corresponding press release from February 6, 2019 which is available on their homepage at https://www.baden-wuerttemberg.datenschutz.de/identitaetspruefung-bei-elektronischen-auskunftsersuchen-nach-art-15-ds-gvo/. Retrieved October 24, 2021.

incoming requests, it is conceivable that data subject rights are resolved e.g. by the implementation (further customization) of a customer portal[632] including relevant log-in data in order to verify and ensure that the right person requests the right information. Such a self-service would also be valuable for other data subject rights, for example the right to copy of their data. At present, the relationship between the right to information about personal data and the right to a copy of personal data is unclear; there is little or insufficient guidance at authority level as most SAs mention that such a right exists rather than explaining the scope and relationship between those rights.[633] Some seem to suggest that a copy could be considered the format of the right for information or equal to the right to access,[634] others quote Recital 63 and argue that the scope of the right to a copy is limited by trade secrets or intellectual property rights and/or rights and freedoms of others.[635] Others think about the possibility that data subjects shall be provided with an "overview" over their data as a simplified first step of information rather than enabling them to access all data the controller holds about them.[636] On the one hand, the right to access should be interpreted broadly as the opposite would lead to a limitation of data subject rights, especially as information is the basis for many other initiatives data subjects might want to take. On the other hand, Recital 63 says that, if the "*controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specifies the information or processing activities to which the request relates*". Moreover, the European Court of Justice ruled[637] that the right to access/information shall not be interpreted in a manner that allows data subjects to request full duplicates of datasets, but that it is sufficient to provide the information in the form of an overview of the stored data. Even though the decision dates back to 2014 and thus refers to the Directive, it may still be considered applicable as the rationale the ECJ quoted remained the same in the Regulation, i.e. to enable the data subject to obtain knowledge of their data and to verify that it is accurate and processed in accordance with applicable laws with the goal to put the data subject in a position to examine further rights if need be.

[632] Recital 63 also deals with the issue of providing data subjects with remote access to their data.

[633] For instanc, the German DSK short-paper no. 6 which was published 2017: Auskunftsrecht der betroffenen Person nach Art. 15 DSGVO, available at https://www.lda.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf. Retrieved October 24, 2021.

[634] For example, the short-paper of the Bavarian supervisory authority which is in charge of the private sector: EU-Datenschutz-Grundverordnung - Das BayLDA auf dem Weg zur Umsetzung der Verordnung. Paper published 2017, available at https://www.lda.bayern.de/media/baylda_ds-gvo_16_right_of_access.pdf. Retrieved October 24, 2021.

[635] GDPR Article 15 (4).

[636] Intersoft Consulting Services: Die Kopie von personenbezogenen Daten im Auskunftsanspruch. Article published on their company website on March 8 2019, available at https://www.datenschutzbeauftragter-info.de/die-kopie-von-personenbezogenen-daten-im-auskunftsanspruch/. Retrieved October 24, 2021.

[637] Source: http://curia.europa.eu/juris/document/document.jsf;jsessionid=DD36E0EFF4D8F25CEA8CC48A373DDE4C?text=&docid=155114&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3639809. Retrieved October 24, 2021.

Not all companies dispose of possibilities to provide information to customers and clients per remote, and particularly businesses who traditionally deal with a lesser number of requests may opt for a manual process, and that may result in data being stored on a mobile storage device and sent to a postal address at which a person is officially registered as this is the address a controller can legally rely upon. The outcome of such processes is de facto ironic as the legislator intended to enhance data subject rights and to facilitate a smooth and easy way of communication and exchange. Not only does this problem not fit in the digital age; the solutions that have so far been presented for identification purposes[638] (and for avoidance of mistakes, i.e., data breaches) all have in common that they are in potential conflict with the principle of data minimization, because they all require even more information. Most potential solutions suggest that applicants provide further information and/or a copy of their ID card or that they undergo a postal or video identification process.[639] Apart from the fact that it is not possible to connect ID card information to an e-mail address, which may vary, which may be replaced in the course of time, any such proposals lead to additional problems, for example duration and safety of storage of ID documents. This way, average companies might face further challenges like the avoidance of identity theft as one simple access request might lead to a full set of personal including ID-data being stored in systems which are not tailored to meet the needs of handling such sensitive data (technical security measures, authorization concept, retention periods, etc.). If the data subject by mistake contacted the wrong controller, then his request is the initial ignition for a full set of data including sensitive information like national identification numbers (which might be subject to national legislation according to GDPR Article 87) being collected and stored. If one is seriously thinking of postal or video-identification-processes for identification purposes, this means that data subjects would have to put up with a great deal of effort, only because they want to exercise their rights. In addition, video-identification-processes involve biometric data (voice, iris), and that leads to further problems as special categories of data enjoy special protection in accordance with GDPR Article 9 (1), and as a basic rule, must not be processed – unless, for example, the data subject explicitly and voluntarily consented. As a result, even more data is collected (time, date, signature) and documentation (evidence) is produced. As a matter of fact, this procedure can only represent one solution, because if the data subject does not consent, then an alternative must be provided as the proper execution of data subject rights is mandatory. It furthermore cannot be assumed that the video-identification-processes is a secure solution, because it has already been repeatedly misused in the framework of fictitious job offers.[640]

[638] This text only uses the term identification, although to identification and authentication are meant.

[639] The State Commissioner for Data Protection and Data Security in Baden-Württemberg summarized possible solutions and evaluated them their February 6, 2019 press release which is available at https://www.baden-wuerttemberg.datenschutz.de/identitaetspruefung-bei-elektronischen-auskunftsersuchen-nach-art-15-ds-gvo/. Retrieved October 24, 2021.

[640] Victims are typically urged to install the app of a bank, and if the victim does not realize that he or she is going through a video procedure to open an account via the app which has nothing to do with their supposed application, they this way help backers to set up a money laundering account in their name. Further background

In summary, it can already at this stage be said that the overall effort and implications of data subject requests shall not be underestimated, particularly because data subjects enjoy additional rights on top of the right to access information, for example the right to restrict processing of their personal data in defined circumstances[641] where the accuracy of the data is contested or where the processing is believed to be unlawful. Individuals may also require that their data is rectified[642] if it is inaccurate or incomplete, or that their data is deleted, the so-called right to be forgotten,[643] which now has its own article in the Regulation. The forerunner of this right was CJEU's decision in which the court ruled that Google had to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.[644] However, the right to be forgotten as any other right has limitations, typically the rights of others, and that applies especially to the field of media as the right to be forgotten must not lead to censorship as freedom of expression must be respected.[645] In in everyday business life, requests for deletion may quite often fail as controllers have to obey statutory retention periods, meaning that they have legitimate grounds to continue to process/store the data. As a result, the right to be forgotten only applies in rather a narrow set of circumstances, notably where the controller has no legal ground for processing the information.

The right to data portability is new and has no equivalent in the previous Directive. It is based on the idea that data subjects should be able to obtain their data in a structured, commonly used and machine-readable format,[646] including the right to transmit those data to another controller without hindrance.[647] Recital 68 clarifies that the data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. This clarification is important as there was a fear that this new right would result in businesses tailoring their (CRM, HR, etc.) systems to fulfill such requests in an automated (ad hoc) manner. In fact, the Regulation clearly says that such investments are not needed. Depending on the underlying business model it is however likely that certain providers will agree upon certain standards between each other, for example email and cloud service providers and social networks. A request for data portability does not mean that data the (first) controller holds shall (also) be deleted, nor does it mean that the right only exists when a customer or client finishes the (business)

information can be found at https://www.morgenpost.de/web-wissen/web-technik/article214921573/So-wird-das-Video-Ident-Verfahren-missbraucht.html. Retrieved October 24, 2021.

[641] GDPR Article 18 provides further details.

[642] GDPR Article 16.

[643] In accordance with GDPR Article 17.

[644] Source: http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=152065&occ=first&dir=&cid=667631. Retrieved October 24, 2021.

[645] GDPR Article 17 (3).

[646] This does not mean that data subjects can insist on a specific format as the Regulation only requires that data are provided in a structured and commonly used format that is machine-readable.

[647] GDPR Article 20 (1).

relationship; data subjects are free to request data portability at any time – but only if certain conditions are met: this right can only be exercised when the (automated) processing of personal data is justified on the basis of consent, or where processing is necessary for the performance of a contract. Recital 68 makes it clear that the right to data portability is not given when the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or when the processing was carried out in public interest. Since there is hardly one dataset in real life to which exactly the same legal grounds apply for each and every entry, in most of the cases where a data subject requests their data to be transmitted to either themselves or another recipient, the data set will have mixed legal grounds. For example, an application for a credit loan requires certain basic data such as full name and date of birth for identification purposes and (retrospective) salary information for credit rating purposes. This is the data the subject provides directly and voluntarily. Because the bank is obliged to perform a background check with regards to liquidity and the matching against sanction lists, further data are collected from other sources such as credit agencies. Then there is yet other data the bank must collect from all applicants like the tax and/or identification number. Depending on whether the credit applied for is received through a website, further data will be collected, and this is usually the moment when Big Data comes into play as user and device information are collected and evaluated. This data together represents the dataset for the credit application, and includes various legal bases, for example data needed for the performance of a contract, data needed to fulfill a legal (compliance) obligation and data which can be used for legitimate purposes. Apart from the fact that one could already argue which pieces of information fall under the category of data needed for the performance of a contract, it is even more questionable whether consent is the right legal basis for certain (extended) background checks or if legitimate interests of the controller may apply, especially in the field of predictive analytics. As data portability only applies to those data which the data subjects provide themselves and which are based either on consent or if the processing was necessary for the performance of a contract to which the data subject is party, it seems problematic to customize the right set of information. One solution could be to downsize accordingly, another solution could be over-fulfillment in the sense of providing more information than needed. Companies may like to tend to provide more than necessary by law to avoid conflicts, however, the dataset must always be checked against collateral data and/or information which may be considered business secrets. In any event, data portability is a perfect example of how important it is to carefully select suitable legal grounds for processing as the right to portability is the "price for consent"; the right does not apply when data are processed on the basis of legitimate interests.[648] As a result, consent is not always the best and easiest solution to place data processing on a legal basis,[649] especially because any processing based on consent alone needs to be stopped

[648] But the "*price*" here is balancing of interests.

[649] Nico Härting described this phenomenon as the "*consent fetishism*" as many businesses fail to recognize that consent is neither the only nor always the best legal grounds for data processing. He provided thoughts on this

immediately once consent is withdrawn,[650] and that can happen any time without providing any reasons.[651]

f) Setting the bar for lawful processing

The fact that businesses fail to recognize that consent is neither the only nor the best legal grounds for the processing of personal data is just one problem, the other is that the Regulation sets a higher bar for lawful processing for both, legitimate interest and consent. GDPR Article 6 provides for six lawful bases for processing[652] which are equivalent[653] as there is no priority between the legal bases; choosing the right legal grounds depends on the overall context, the underlying purposes of the processing and the existing relationship with the data subject.[654] This structure and approach was already present in the Directive, but the Regulation places more emphasis on being accountable for and transparent about the relevant lawful basis for processing. For example, if a procedure is based on the controller's legitimate interests, the prerequisite for that is that any such legitimate interests are documented internally[655] and communicated externally.[656] Given the complex matter, transparency needs in the framework of Big Data and AI applications and automated individual decision-making represent a high barrier for data processing as the controller has to ensure that data subjects are furnished with all relevant information in conjunction with GDPR Articles 6, 7 and 12 to 22 in order to put them in the position to realize how such a processing may (and will) affect him.[657] Despite the fact that the catalogue of data processing principles in GDPR Article 5 (1) is clear and comprehensible, it is often overlooked that every legal basis for processing of personal data involves the evaluation of whether or not such processing is necessary.[658] Necessity must not be confused with the method chosen to operate

problem during his 2012 presentation in the framework of the DSRI Herbstakademie (annual DSRI academy summit), available at https://rsw.beck.de/cms/?toc=ZD.60&docid=338853. Retrieved October 24, 2021.

[650] GDPR Article 7 (3): The withdrawal does not affect the lawfulness of processing before its withdrawal.

[651] The difference between GDPR Article 7 (3) and GDPR Article 21 (1) is that freely given consent can be withdrawn at any time, for any reason - unlike the need to specify or explain "*grounds relating to his or her particular situation*" when processing is based on legitimate interests or is performed for a task carried out in the public interest. GDPR Article 21 (1) in conjunction with GDPR Articles 6 (1) lit. e, f.

[652] Apart from specialties like article 88 GDPR, processing in the context of employment.

[653] ICO: Guide to the General Data Protection Regulation, p. 49. Guide published 2018, available at https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Retrieved October 24, 2021.

[654] This can lead to advantages, e.g. in the area of direct marketing.

[655] GDPR Article 6 lit f says that processing is only lawful if legitimate interests of a controller are not "*overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data* (…)". This means that a balancing of interests has to take place and given that controllers are accountable to demonstrate compliance with the principles relating to the processing of personal data in accordance with GDPR Article 5 (2), they have to document that they obeyed the principle of lawfulness, fairness and transparency in accordance with GDPR Article 5 (1 a).

[656] Transparency needs in accordance with GDPR Articles 13 and 14.

[657] Laurens Nauds: The Right not to be Subject to Automated Decision-Making: The role of explicit consent. Article published in 2016 available at https://www.law.kuleuven.be/citip/blog/the-right-not-to-be-subject-to-automated-decision-making-the-role-of-explicit-consent/. Retrieved October 24, 2021.

[658] GDPR Article 6 (1) lit. b, c, d, e and f explicitly mention that processing has to be necessary; GDPR Article 6 (1 a) – processing on the basis of the individual's consent – does not mention this term. However, GDPR Article

a business in a particular way;[659] necessity is "*a fundamental principle when assessing the restriction of fundamental rights, such as the right to the protection of personal data*".[660] Therefore, even if the principle of data minimization is only mentioned once in the text of the Regulation explicitly,[661] Recital 39 further clarifies the principles of data processing and specifies that the processing of personal data should be limited to what is necessary for the purposes for which they are processed. The same idea is expressed in the principle of purpose limitation,[662] and both principles are core issues in the framework of Big Data and AI applications as these applications typically depend on large (growing) datasets and quite often also on changing (dynamic) purposes.[663]

The changed bar for lawful processing has several further manifestations. A simple example is that consent cannot be based on mere inactivity or acquiescence of the data subject because consent can only be provided by a statement or by a clear affirmative act.[664] Even though there is no requirement to provide consent in a written format, Recital 42 says that the controller must be able to demonstrate that the data subject has given consent, and that leads to a burden of proof for the controller. However, if consent is to be given in the context of a written declaration which involves other matters, the request for consent must be presented in such a way that it makes it "*clearly distinguishable from all other matters, in an intelligible and easily accessible form, using clear and plain language*".[665] The latter shall not be underestimated as some companies are facing trouble due to mishandling of user information due to fragmentation of information and the length of their terms.[666] This indeed is a problem as consent must be informed and specific[667] and, among other things,[668] freely given, a prerequisite which leads to further questions when consent is to be bundled with other matters and/or is made conditional. In this regard, European supervisory authorities commented on the issue of cookies used on websites. The problem with the practice of using cookies is that users are either not really asked for consent as some providers tend to rely on the idea that pop-up windows are sufficient in order to create transparency about the manner in which cookies are used, or that consent is

7 (4) stipulates that, when "*assessing whether consent is freely given, utmost account shall be taken of whether,* inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*".

[659] ICO: Guide to the General Data Protection Regulation, p. 53, available at https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Retrieved October 24, 2021.

[660] EDPS on the principles of necessity and proportionality, available at https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en. Retrieved October 24, 2021.

[661] GDPR Article 5 (1 c).

[662] GDPR Article 5 (1 b).

[663] GDPR Article 6 (4) sets forth the conditions of such processing.

[664] Consequently, Recital 32 explicitly mentions that inactivity cannot constitute consent.

[665] GDPR Article 7 (2).

[666] The press agency Bloomberg reported that PayPal's terms and conditions are almost 50,000 words spread across 21 separate web pages, the corresponding news entry from April 20, 2018 is available on their website at https://www.bloomberg.com/news/articles/2018-04-20/uber-paypal-face-reckoning-over-opaque-terms-and-conditions. Retrieved October 24, 2021.

[667] GDPR Article 6 (1 a).

[668] See article 4 (11): consent must always be a freely given and an unambiguous indication of the data subject's wishes.

mandatory in order to proceed with accessing the content and using the services of the website.[669] In March 2019, the Dutch SA published their opinion[670] on so-called cookie-walls on websites. A cookie-wall has the effect that access to the website is only granted when consent to the placing of tracking cookies[671] and similar technologies is given. The Dutch authority said that the (required) consent obtained in this way is not freely given, because individuals have no genuine and free choice as withholding consent has adverse consequences. Such a use of a cookie-walls results in a take-it-or-leave-it-approach, and this practice is not compliant with the GDPR. Consequently, the regulator recommend that websites shall offer a real choice for users to either accept or reject cookies, meaning that the website must remain accessible if tracking cookies are refused.[672]

The guidance of the Dutch supervisory authority is a remarkable decision after a much-disputed decision[673] Austrian case[674] in late 2018 in which a complaint about consent that was obtained through a cookie-wall was not freely given was rejected. Instead, it validated (paid) subscription models as a viable alternative to (ad) tracking. On the one hand, it is true that the freedom to contract principle applies to private parties, and therefore, it could be assumed that providers are not obliged to make their content available free of charge and they have the right to set certain conditions for allowing access to their website or other services. On the other hand, it seems difficult to recognize a free choice when the choice is reduced to personal data or money in return. Such an interpretation is open to challenge, because as a result, it reinforces business models on the basis service against data. However, regulators issued further decisions in the meantime, which are not only relevant for cookies, but also meaningful for international data transfers since they underline the inadmissibility of such transfers to the U.S.:[675] in late 2021, the Austrian regulator held that that the use of Google Analytics by a local website provider led to transfers of personal data such as identifiers, IP address and browser parameters to Google LLC in the U.S., and that this is in violation of Chapter V of the GDPR, because "*the SCCs concluded between the respondents do not offer an adequate level of protection, because*

[669] For the purposes of this example, it is assumed that consent is necessary, regardless of whether GDPR or PECR are the appropriate legal framework.

[670] The statement of the Dutch supervisory authority from March 7, 2019 is available at https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies. Retrieved October 24, 2021.

[671] Consent is not required for placing functional cookies and non-privacy sensitive analytical cookies.

[672] Sibylle Gierschmann: Was bringt deutschen Unternehmen die DSGVO – mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD 2016, p. 54.

[673] Background information on the case is provided by the law firm of Hogan Lovells in their January 21, 2019 blog entry on their website, available at http://hoganlovells-blog.de/2019/01/21/oesterreichische-datenschutzbehoerde-zur-reichweite-des-kopplungsverbots/#. The original decision is available at https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00.html. Retrieved October 24, 2021.

[674] Unlike in Germany, there was no explicit provision in Austria under their pre-GDPR Data Protection Act. Before GDPR came into force, § 28 (3b) BDSG stipulated that "*the conclusion of a contract may not be made dependent on consent (...) if another access to equivalent contractual services is not possible or not reasonably possible without such consent.*" (Free translation from German).

[675] For example, the Dutch regulator: file:///C:/Users/kvarn/AppData/Local/Temp/handleiding_privacyvriendelijk_instellen_google_analytics.pdf.

Google LLC qualifies as "electronic communication service provider" under 50 U.S. Code § 1881(b)(4) and is subject to surveillance by US intelligence services and because any additional safeguards which have been put into place in addition to where insufficient as they could not prevent US intelligence services from accessing the data subject's personal data".[676] But there are not only remarkable decisions, but there are also remarkable penalties: the French regulator CNIL issued high fines for Google and Meta, because following investigations, the CNIL found that the websites facebook.com, google.fr and youtube.com do not make refusing cookies as easy as to accept them and thus fined Meta 60 million Euro and Google 150 million Euro and ordered them to comply within three months.[677]

In Germany, the former BDSG[678] took a clear position by saying that the conclusion of a contract must not be made dependent on the data subject's consent if access to equivalent contractual services is not (reasonably) possible without such consent.[679] The law intended to stress that services must not be made dependent on consent for data which are not required for the execution of the specific service. But it is important to note that the prohibition of tying only applies if the person concerned cannot reasonably be expected / is unable to switch to another supplier – such a thought is foreign to the General Data Protection Regulation as there is no such criterion in GDPR Article 7 (4); the norm merely states that "*when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*". This means that any such circumstance must be taken into account, but it does not mean that any such circumstance would automatically lead to invalid consent. Several courts in Germany held that consent must be obtained for necessary cookies.[680] Germany introduced a new Telecommunications Telemedia Data Protection Act (TTDSG) which is applicable as of December 2021 and which combines data protection provisions from the existing Telemedia Act (TMG) and the Telecommunications Act (TKG).[681] According to the new TTDSG which came with a twelve year delay, consent would not be required in certain instances, and the law also allows for consent

[676] Max Schrems' NGO „NOYB" represented the data subject. Background information on the case, including this quote, is available on NOYB's website at https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2021-0.586.257_(D155.027)&fbclid=IwAR2j5-utq3BCBMr-CFl4afREQjdY5kcnqI4dEE6J-wGSHO9jGT_gWOR7qIU. Retrieved January 22, 2022.

[677] Source: CNIL's website news entry from January 6 2022, available at https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance#:~:text=Cookies%3A%20the%20CNIL%20fines%20GOOGLE%20a%20total%20of,refusing%20cookies%20as%20easy%20as%20to%20accept%20them.

[678] BDSG § 28 3b.

[679] A very similar provision is included in § 95 (5) of the German Telecommunications Act.

[680] For example, the county court in Frankfurt am Main (Az.: 3-06 O 24/21) in a decision that was issued October 19, 2021 which is available at https://openjur.de/u/2378854.html.

[681] Andy Splittgerber: German Cookie Law enters into force on Dec. 1, 2021. Article available at https://viewpoints.reedsmith.com/post/102gyp8/german-cookie-law-enters-into-force-on-dec-1-2021. Retrieved January 22, 2022.

management services so that users to indicate whether, where and under which conditions they consent or refuse to the setting of cookies.

Regarding freely given consent, the problem is that even within the Regulation, the relevant Article and the corresponding Recital are not congruent: Recital 43 says that "*consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance*." GDPR Article 7 (4) and Recital 43 are therefore led to different results.[682] Given that GDPR-Articles have priority over Recitals, some authors claim that the effectiveness of coupling has to be assessed on case-by-case.[683] Others claim that consent is always freely given when the data subject is free to choose between providers.[684] The upcoming ePrivacy Regulation will hopefully help answer the question whether making access to website content without direct monetary payment conditional to the consent of the end-user will (not?) be considered disproportionate: it seems that cookie-walls will not be prohibited as long as users are given an "equivalent offer" and that consent will be feasible through browser settings – and that users who consented to the use of cookies will have to be periodically reminded of their choices.[685] The trouble with obtaining valid consent might to lead to a shift of legal basis: provided that the desired processing of personal data can be justified with legitimate interest, consent could become a phase-out model.[686] Some authors therefore believe that the economy will have to start to base processing of personal data on legitimate interests, because consent as a legal instrument appears to be severely weakened.[687] This argument is reinforced by the fact that Recital 43 mentions another criterion as it stresses that consent is not valid if there is a clear imbalance between the data subject and the controller. This is very important in practice, and it even applies to all of our workplaces, because a typical example of imbalances is the relationship between employer and employee.[688]

[682] Niko Härting: Kopplungsverbot nach der DSGVO – erste Sichtung der Literatur, itrb-Rechtsberater 2019, Sonderheft zur DSGVO, p. 5.

[683] Eike Michael Frenzel in Paal/Pauly: Kommentar zur Datenschutzgrundverordnung, Bundesdatenschutzgesetz, second edition 2018, C.H. Beck publishing Munich 2018, note 18 on GDPR Article 7. KÜRZEN, Quelle als solche korrekt, stammt aus Härting, sonderheft S. 5.

[684] Kai-Uwe Plath: Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen des TMG und TKG, second edition 2016, Otto Schmidt publishing Cologne, note 14 on GDPR Article 7. KÜRZEN, Quelle als solche korrekt, stammt aus Härting, sonderheft S. 5.

[685] Jetty Tielemanns, Müzge Fazlioglu: ePrivacy Regulation — Q&A on select topics. Article published May 25 2021, available at https://iapp.org/news/a/eprivacy-regulation-qa-on-select-topics/. Retrieved October 24, 2021.

[686] Winfried Veil: Die Datenschutzgrundverordnung: Des Kaisers neue Kleider, NVwZ 2018, p. 695.

[687] Niko Härting: Kopplungsverbot nach der DSGVO – erste Sichtung der Literatur, itrb-Rechtsberater 2019, Sonderheft zur DSGVO, p. 6.

[688] However, the individual case has to be examined as it is conceivable that employees consent to data processing, for example in the framework of an internal corporate videos, see also the Article 29 Working Party Guidelines on consent under Regulation 2016/679 (2018 version), available at https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf. Retrieved October 24, 2021.

The imbalance between processor and data subject was also criticized by the German Federal Cartel Office: in a recent decision, the Cartel Office prohibited Meta from merging user data from various sources. The Cartel Office said that the data processing conditions for the use of Meta violate data protection law as set forth by the GDPR and that they constitute an abuse of Meta's dominant position in the market for social networks for private users.[689] The result is that, as far as Germany is concerned, WhatsApp and Instagram may continue to collect data. However, in the future, data may only be assigned to a Meta user account with the user's consent. If such consent is not given, the data must remain with the other services and may not be processed in combination with Meta data. The same applies to the collection and assignment of data from third-party websites to the Meta user account, which will also only be possible in the future if the user voluntarily consents to the assignment to his or her Meta user account. While data protection practitioners may welcome this opinion as it is in favor of data subjects, the decision caused astonishment, because the German Federal Cartel Office felt competent[690] to comment on a data protection matter. The Cartel Office moreover does not seem to see a conflict between the application of antitrust law and data protection law,[691] since it attempted to establish its competence by examining data protection law within the framework of antitrust law. But this view seems contestable given that GDPR aims at a uniform application of the Regulation, and that is why cooperation between supervisory authorities is foreseen.[692] It is therefore time for the European Data Protection Board to provide clarity[693] on the admissibility of cookie walls, especially owing to the (surprising) fact that, in the Austrian case, a referral to the ECJ was rejected, because it was considered that the case has been clarified – despite the fact that differing opinions within literature showed that the legal position on this issue is not clear, was quoted in the decision.[694] The opinions on the relationship between (freely given) consent and other legal bases also do not show a uniform picture: despite the fact that GDPR Article 6 (1) says that processing is lawful "*if and to the extent that at least one of the following applies (...)",* therefore clearly saying that more than just one legal basis may be applicable for the case in question, it is disputed whether or not data processing may be based on several legal bases mentioned in GDPR Article 6. Some believe that consent may be used as a precautionary measure in the event that there is

[689] The decision of the German Federal Cartel Office was published on February 2, 2019: Bundeskartellamt untersagt Facebook die Zusammenführung von Nutzerdaten aus verschiedenen Quellen. It is available at https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2019/07_02_2019_Facebook.html. Retrieved October 24, 2021.

[690] GDPR Article 51 (1) and Article 55: a Cartel Office is not a data protection supervisory authority.

[691] Carlo Piltz: Bundeskartellamt erlasst Untersagungsverfügung gegen Facebook – Warum das Vorgehen der Behörde datenschutzrechtlich kritisch betrachtet werden muss. Article published February 7 2019, available at https://www.delegedata.de/2019/02/bundeskartellamt-erlasst-untersagungsverfuegung-gegen-facebook-warum-das-vorgehen-der-behoerde-datenschutzrechtlich-kritisch-betrachtet-werden-muss/. Retrieved October 24, 2021.

[692] GDPR Article 60.

[693] Per consistency mechanism: GDPR Article 63.

[694] Carlo Piltz: Oberster Gerichtshof in Österreich zur Kopplung der Einwilligung nach der DSGVO – grundsätzlich unzulässig? Article published November 13 2018, available at https://www.delegedata.de/2018/11/oberster-gerichtshof-in-oesterreich-zur-kopplung-der-einwilligung-nach-der-dsgvo-grundsaetzlich-unzulaessig/. Retrieved October 24, 2021.

doubt which other legal bases may be applicable.[695] This interpretation seems comprehensible, since a literal interpretation of GDPR Article 6 (1) does not suggest that a particular legal basis is favored or preferred, but that all the possibilities mentioned are equivalent.[696] Consequently, some authors suggest that several legal grounds may be used as a legal basis for processing, while other authors believe that recourse on other legal grounds such as legitimate interests is not possible whenever consent was provided, especially if consent was revoked.[697] The reason for this is that, if consent is obtained, this serves as an indicator that the data subject is in full control of the data processing, and that the use of any other legal basis shall be considered contradictory and therefore inadmissible.[698] In this context, some also speak of the blocking effect which unfolds when consent is given.[699] This argument is rejected by others, because this way, consent would have a more important position than other legal provisions.[700]

At present, the relationship between various legal bases which are provided by GDPR Article 6 (1) does not seem to be clear. This circumstance is worsened by the fact that many businesses continue to "misuse" consent as an easy means of obtaining legal grounds, either not knowing or ignoring that consent is not needed and therefore not the appropriate legal basis: a typical example is that companies ask for consent even though the data processing for the service in question is covered by GDPR Article 6 (1) lit. b, the performance of a contract, which is regularly the case for many services which are rendered for customers.[701] However, if companies base (part of) their data processing operations on the performance of a contract, such legal grounds must not be overused either: the EDPB adopted guidelines on the scope and application of GDPR Article 6 (1b) in the context of information society services.[702] The EDPB restricts the possibility for companies to base the processing of users' data on

[695] The Hessian supervisory authority issued FAQs on GDPR issues, and the SA says that (free translation from German: "*It can often be difficult to determine the right legal basis for data processing or to clearly identify its limits. In such cases, it is not harmful for both responsible bodies and data subjects to obtain consent as a precautionary measure, particularly for reasons of security and transparency*." The FAQs were published on the SA's website and are available at https://datenschutz.hessen.de/infothek/h%C3%A4ufig-gestellte-fragen-hgf#Einwilligung. Retrieved October 24, 2021.

[696] Benedikt Buchner, Jürgen Kühling: Kommentar zur DSGVO, C.H. Beck publishing Munich 2016, note 16 on GDPR Article 7.

[697] Sebastian Schulz in Gola: Kommentar zur DSGVO, C.H. Beck publishing Munich 2018, note 11 on GDPR Article 6.

[698] Benedikt Buchner, Thomas Petri in Kühling/Buchner: Kommentar zur DSGVO, C.H. Beck publishing Munich 2016, note 23 on GDPR Article 6.

[699] Maria Cristina Caldarola, Joachim Schrey: Big Data und Recht, C.H. Beck publishing Munich 2019, pp. 54 and 55.

[700] Niko Härting: Berechtigte Interessen nach der DSGVO, itrb-Rechtsberater, Sonderheft zur DSGVO 2019, p. 3.

[701] In this regard, it is interesting to read the examples provided by the Commission on their website: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en. Retrieved October 24, 2021.

[702] Background information is provided in EDPB's Guidelines 2/2019 on the processing of personal data under Article 6 (1) lit. b GDPR in the context of the provision of online services to data subjects (version for public consultation) adopted on April 9, 2019, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf. It is important to note that "*all documents adopted during the EDPB*

the legal basis fulfillment of contract. This view was welcomed, because it is argued that, if GDPR sets strict conditions for the permissibility of consent, it shall not be acceptable to bypass this requirement simply by including certain data processing operations in contracts (terms and conditions) that actually do not have much to do with the provision of their (online) services.[703] Apart from these general rules for consent, special conditions apply to vulnerable groups[704] like the consent of children,[705] and special requirements also apply if consent is given in relation to sensitive personal data.[706]

g) Contract and vendor management

Much of the literature on GDPR is concerned with new requirements including controller and processor duties, which of course makes sense as companies have to comply with (partially) new rules – especially because, under the Regulation, practically everything is sanctioned as GDPR uses the general term "infringements of the provisions" and then specifies which type of infringement leads to which (maximum) fine.[707] This was not the case under the previous regime with the Directive and national laws across the EU as penalties and sanctions were not harmonized and varied significantly in different member states. The result was that, for example in Germany, for years, there were only sporadic sanctions according to § 44 of the pre-GDPR Federal Data Protection Act.[708] Another difference is that enforcement is likely to change as national data protection supervisory authorities will be coordinating their enforcement powers across member states. It is important to note that the maximum fine of up to 20 million Euros[709] may be imposed for infringements in the framework of transfers of personal data to recipients in a third country or an international organization pursuant to GDPR Articles 44 to 49.[710] Considering that data transfers outside the own organization and inside an undertaking is very common and that interconnectedness and globalization are growing, there is a definite necessity to review the existing (contractual) framework with suppliers, subsidiaries and

Plenary are subject to the necessary legal, linguistic and formatting checks and will be made available on the EDPB website once these have been completed", source: https://edpb.europa.eu/news/news/2019/ninth-plenary-session-guidelines-processing-personal-data-context-information-society_de. Retrieved October 24, 2021.

[703] Ulrich Kelber, German Federal Commissioner for Data Protection and Freedom of Information (BfDI), comments on the guidelines in a news entry published April 10 2019, available at https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/15_EDSA_Art.6_1_b.html. Retrieved October 24, 2021.

[704] This is a newly introduced concept which did not exist in the Directive.

[705] GDPR Article 8 GDPR and Recital 38.

[706] GDPR Article 9 (2 a).

[707] GDPR Article 83.

[708] Christiane Schulzki-Haddouti: Datenschutz-Verstöße werden sehr selten sanktioniert. Article published April 4 2016, available at https://www.datenschutzbeauftragter-online.de/datenschutz-verstoesse-werden-sehr-selten-sanktioniert/9536/. Retrieved October 24, 2021.

[709] Or, in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: GDPR Article 83 (5).

[710] GDPR Article 83 (5 c).

parent companies.[711] This is particularly true when an international context is given, because different rules may apply as simple data processing agreements might not be sufficient. It is likely that nowadays, most companies are aware of the need for a (contractual) data protection framework when data transfers are in question, but it is also questionable whether they are prepared for a proper contract and vendor management including background screenings, since there are differences between the Directive and the Regulation: GDPR establishes a cumulative liability regime for controllers and processors[712] and thus foresees a joint and several liability. Controllers still carry primary responsibility for compliance, but processors have become subject to several obligations and are directly liable towards data subjects in case of non-compliance.[713] Second, eventual fines will also depend on factors which are influenced by the processor's behavior and prehistory: mainly the degree of responsibility of the processor;[714] any relevant previous infringements the processor committed;[715] any previous measures referred to in GDPR Article 58 (2) which have previously been ordered;[716] the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement.[717] The framework for outsourcing of services which implies the processing of personal data did not change substantially, however, businesses must take note of the fact that outsourcing standards were altered as regards format and content. The latter depends on the jurisdiction,[718] industry sector[719] or profession in question.[720] The GDPR provides that processing by a processor shall be governed by a contract or other legal act under Union or member state law, binding the processor to the controller.[721] In the framework of a parliamentary question session in August 2018,[722] the European Commission clarified that a legal act may be "*an ordinance or other type of administrative decision whereby controllers vested in public authority may stipulate the conditions for processing personal data on their behalf*".

[711] For the sake of simplicity, this paragraph does not cover issues of joint controllership.
[712] Brendan Van Alsenoy: Liability under EU Data Protection Law - from Directive 95/46 to the General Data Protection Regulation, Jipitec 2016, p. 282.
[713] GDPR Article 82 (2).
[714] GDPR Article 83 (2 d).
[715] GDPR Article 83 (2 e).
[716] GDPR Article 83 (2 i).
[717] GDPR Article 83 (2 h).
[718] The Bavarian State Commissioner for Data Protection issued guidance in which the following opinion was expressed (free translation) "*Provided that the treaties complied with the previous legal requirements, the need for adaptation to the GDPR should be manageable*". Der Bayerische Landesbeauftragtefür den Datenschutz: Orientierungshilfe Auftragsdatenverarbeitung, p. 10. Paper published 2018, available at https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf. Retrieved October 24, 2021.
[719] For example, specific rules apply in the banking sector as risk management has to apply to the outsourcing and other external procurement of IT services. Details on this issue are summarized by Ulf Morgenstern: 5. MaRisk-Novelle in Kraft getreten – deutliche Herausforderungen für Kreditinstitute. Article published December 20 2017, available at https://bankinghub.de/banking/steuerung/5-marisk-novelle-kraft-getreten. Retrieved October 24, 2021.
[720] For instance, because of professional secrecy that applies to solicitors, notaries or physicians: these professional groups have always had to take special care to ensure that data about their clients and patients are securely processed and stored.
[721] GDPR Article 28 (3).
[722] Question reference: E-003163/2018 available at http://www.europarl.europa.eu/doceo/document/E-8-2018-003163-ASW_EN.html.

The Commission also addressed the question of the appropriate format of such an agreement as GDPR Article 28 (9) states that the contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including the electronic format. It said that "*the rules for entering into contracts or other legal acts, including in electronic form, are not set forth in the GDPR but in other EU and/or national legislation. The e-commerce Directive*[723] *provides for the removal of legal obstacles to the use of electronic contracts. It does not harmonize the form electronic contracts can take. In principle, automated contract processes are lawful. It is not necessary to append an electronic signature to contracts for them to have legal effects. E-signatures are one of several means to prove their conclusion and terms*". One the one hand, GDPR allows for more flexibility when data processing agreements are in question. On the other hand, real life will show whether businesses will make use of the above possibilities. If important contracts may be concluded in such an easy manner, this carries the risk that unauthorized staff may engage in contractual agreements. The same idea applies to amendments: if a simple email will suffice to change or amend a contractual arrangement, this may lead to undesired results. It is therefore probable that many companies will stick to the written format in favor of legal certainty. Exceptions seem likely for business models in which the controller offers an online platform for their suppliers in which they can easily access business relevant documents such as terms and conditions and conclude relevant contracts including data processing agreements. This type of process automation depends on the underlying cooperation in question and especially on whether the parties intend or desire to conclude standard contracts rather than negotiating agreements individually. Speaking of negotiating agreements individually – this is an extremely important topic when it comes to damages and liability as the Regulation provides that controllers and processors will be jointly and severally liable where they are both responsible for damage caused by their processing.[724] According to GDPR Article 82 (2) and (3), a processor "*shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller*". If a company acts as a processor, it shall be exempt from liability if it is able to provide proof that it is not in any way responsible for the event giving rise to the damage. In the event that one party pays all of the compensation for the damage, it is entitled to claim back relevant amounts from the other party.[725] Since GDPR significantly increases possible fines, vendors may well try to shift present liability limits to their own favor. As a result, not only is there a need to review existing data processing agreements to check whether they match all new requirements; vendor management will become a key issue in the framework of business compliance. The invalidation of the Privacy Shield and subsequent regulator recommendations on supplementary measures such as transfer impact

[723] Source: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031. Retrieved October 24, 2021.

[724] ICO: GDPR guidance – contracts and liabilities between controllers and processors. Guidance published 2018, available at https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf. Retrieved October 24, 2021.

[725] GDPR Article 82 (5).

assessments is a good example of how important the profound selection and evaluation of appropriate service providers including underlying contractual agreements is.[726] Controllers shall moreover examine their insurance policies to make sure that they have the needed coverage. The problem being that even data protection authorities will need some time to determine a reasonable and market standard approach to the appropriate allocation of risk and financial responsibility for such fines as between customers and third-party processors.[727]

h) Emphasis on governance and response mechanisms

Information and notification requirements which occur in the framework of data breaches[728] are a perfect example of the fact that response mechanisms are needed to address the requirements of the Regulation. The same applies to data subject requests as processes must be in place to check and fulfill individual requests for information, deletion or data portability. Depending on the business model, this will either be resolved case-by-case or lead to the implementation of corresponding (self-service) tools.[729] The difference being that the timeline for answering data subject request is totally different[730] from the deadline for reporting data breaches: in the event of a personal data breach, the controller has to notify the competent supervisory authority without undue delay, where feasible, no later than 72 hours after having become aware of the data breach.[731] But it is questionable whether it will be feasible to provide all necessary information[732] on such short notice. It seems likely that, in many cases, it will not be feasible to find all necessary details on the nature and consequences of the data breach, especially when service suppliers are involved, meaning that the controller is dependent on their approach to the incident. In addition, reporting on such short notice can only focus on ad-hoc-measures, but not on long-term security (preventive) technical and organizational measures, and that is why some believe that data breach notifications under GDPR are an unrealistic default and shall be

[726] On June 21 2021 the EDPB adopted a Recommendations on supplementary measures, which is available at https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en. Retrieved October 24, 2021.

[727] ICO: GDPR guidance – contracts and liabilities between controllers and processors. Guidance published 2018, available at https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf. Retrieved October 24, 2021.

[728] GDPR Articles 33, 34.

[729] Michele Nati, Cert Ahlin: Data Portability 2.0 is yet to come. Article published September 17 2018, available at https://medium.com/mydata/data-portability-2-0-is-yet-to-come-1c438c2a96c1. The authors summarize the current stage of the right to data portability and report that major social platforms are offering data portability functions. Retrieved October 24, 2021.

[730] Depending on case and circumstances, the controller may take up to three months: GDPR Article 12 (3), first and second sentence: "*The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests*".

[731] GDPR Article 33 (1).

[732] GDPR Article 33 (3) specifies which details have to be provided in the framework of a breach notification.

corrected.[733] Given the breach and response mechanisms, (expert) manpower will be needed, and this is underlined by a wide of range of tasks needs to be fulfilled: from the implementation of relevant (information, data subject, design, reporting) processes, various documentation and (risk) assessment needs over data minimization, quality, security and retention issues up to the management of breaches and third parties – all this together with the need to make sure that the lawfulness of the processing of all personal data the organization holds is given (including proof of legal grounds/origin of data/ rules for special data) can only be achieved if a corresponding governance structure is present. GDPR Article 5 (2) stipulates that the controller is responsible and "*must able to demonstrate compliance with paragraph 1*", i.e. the basic principles relating to processing of personal data such as accuracy, integrity and confidentiality, lawfulness, fairness and transparency as well as purpose and storage limitation. This means that, regardless of the question of whether or not a data protection officer has to be appointed,[734] organizations must make sure that there are individuals accountable for data protection. The above requirements show that, rather to sticking to certain conditions which must be met for certain data, the Regulation requires the overall modeling of various processes and procedures based on relevant documentation for evidentiary purposes. If, for example, a certain data processing is based on legitimate interests or if the underlying purposes for a certain data processing operation is to be changed or amended, the corresponding assessment and reasoning has to be demonstrated even years later. At the same time, governance needs lead to an ongoing assessment, which is also of relevance for Big Data and AI applications, since businesses will have to review their level of compliance with GDPR requirements for every newly introduced set of data and for every newly introduced (purpose for) data processing.

4. New gaps

a) Heterogeneous and indeterminate terms

Despite the fact that quite a large number of terms have been defined in the Regulation, there are, apart from Recital 47 which deals with direct marketing in the framework of legitimate interests, no definitions or specific articles on marketing. Any further clarification would have been helpful for various (online) business activities for which Big Data and AI applications are frequently used. The

[733] On April 3 2019, the German state of Lower Saxony proposed amendments to data protection provisions to the Germany Federal Council, and one of the motions was to review the current deadline for data breach notifications as set forth in GDPR Article 33 (1) for adequacy, source: https://www.datenschutzticker.de/2019/04/niedersachesen-schlaegt-aenderung-datenschutzrechtlicher-bestimmungen-im-bundesrat-vor/. Retrieved October 24, 2021.

[734] The requirement to appoint a DPO varies between Member States, see GDPR Article 37 (4). Depending on certain circumstances like industry and business model, organizations may have to appoint more than data protection officers, for instance, compliance officers (e.g., banking sector) or authorized recipients (e.g., in the framework of the German Network Enforcement Act). Another example is the mandatory contact person as foreseen in the e-evidence proposal.

trouble is that the interpretation of this specific Recital would affirm the admissibility of direct e-mail-marketing, but for example from a German perspective, the national law against unfair competition (Gesetz gegen den unlauteren Wettbewerb, UWG) requires consent for such an activity. The UWG is based on Directive 2002/58, the so-called ePrivacy Directive (PECD), and some believe that it would have been more suitable to enshrine this regulation in data protection law and not competition law to better serve the purposes of Union law.[735] At the moment, the relationship between the PECD and the GDPR is not clear: Even though Recital 173 says that "*this Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons*", the second sentence of the Recital shows that there is indeed a need for further clarification: "*In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation*."

As regards data subject rights, the Regulation uses the term interests[736] without providing further background information like is the case with other terms (articles). This term comprises economic, financial and other, intangible interests,[737] but the question is how such broad concepts shall be balanced against each other as both, data subjects and controllers have economic, financial as well as tangible and intangible interests. Furthermore, a recent case in Germany shows how important the correct interpretation of legal terms indeed is: the article reported about the explosive power of right to copy[738] in the framework of the case of an employee who sued his employer. The plaintiff has worked for the company since 2007, and since performance and behavioral data are vague terms, the company may have to search for files, emails, minutes and logs containing personal information throughout all his years of service. The problem is that the wording of GDPR Article 15 (3) can be understood in a manner that allows for an interpretation which leads to the result that the person concerned must be provided with a copy of each and every e-mail, document and note he has ever written or received. The seemingly simple right to copy is a good example of how important it is to further discuss limitations of data subject rights, based either on legal interpretation or on right of others since any correspondence this particular plaintiff wrote not only concerns him, but others as well.

[735] Helmut Köhler: Die Umsetzung der Richtlinie über unlautere Geschäftspraktiken in Deutschland – eine kritische Analyse, Gewerblicher Rechtsschutz und Urheberrecht 2012, pp. 1073 and 1079.

[736] For example, GDPR Articles 6 (1) lit. f and Article 9 (2) lit. b or Article 49 (1) lit. c.

[737] Datenschutzkonferenz: Risiko für die Rechte und Freiheiten natürlicher, Working Paper No. 18, p. 3. The document is available at https://www.lda.bayern.de/media/dsk_kpnr_18_risiko.pdf. Retrieved October 24, 2021.

[738] Niko Härting: Mit der DSGVO zum "*Golden Handshake*" – von der Sprengkraft des "*Rechts auf Kopie*". Article published March 29 2019, available at https://www.cr-online.de/blog/author/haerting/. Retrieved October 24, 2021.

In the framework of data subject rights, the Regulation naturally also uses the terms fundamental rights and freedoms, but deviations in the interpretation of the Regulation could result from the fact that GDPR Articles 22 (2) b and 35 (7) c which relate to profiling and impact assessments use the term "rights and freedoms", whereas GDPR Articles 4 (24) or 6 (1) lit. f and 23 (1) which relate to legitimate interests and restrictions of obligations and rights provided for in GDPR Articles 12 to 22 and Article 34, use the term fundamental rights and freedoms. Fundamental rights and freedoms are governed by the Charter of Fundamental Rights and the European Convention on Human Rights, and the starting point for the interpretation of this term is the fundamental right to the protection of personal data pursuant to Article 8 of the Charter,[739] since these terms must be interpreted within the context of European law and not according to a purely national understanding[740]. But the problem is that, prior to GDPR, national interpretation of data protection regulations dominated the application and transposition of data protection law into national law within the EU for decades.[741] Another challenge is that other sources of law which are part of the (global) data protection framework use a different terminology; the situation gets complicated if one takes a look beyond GDPR – which is necessary because the Regulation is embedded in higher-ranking laws and must not be interpreted from a national perspective, only. While the Charter of Fundamental Rights and the draft of the ePrivacy-Regulation are concerned with "*data protection*", the European Convention on Human Rights deals with the "*respect for private life*", the Council of Europe Convention 108 as well as the corresponding OECD Guidelines talk about "*privacy*", Data Protection Directive and the General Data Protection Regulation speak about "*(fundamental) rights and freedoms*" of natural persons, while the Charter of Fundamental Rights or the draft ePrivacy Regulation also deal with the protection of "*communications*".[742] This paper already explained that the notion of privacy is not exactly the same like data protection. The core issue in this context is that the applicability of data protection rules depends on these terms.

b) Unclear protective goals

The above exceptions to the harmonization of the legal framework as well as the discussion on relevant, consistent and future-proof legal terms inevitably also leads to the question of the purposes of

[739] This basically covers all fundamental rights which are at least indirectly protected by data protection law: Datenschutzkonferenz: Risiko für die Rechte und Freiheiten natürlicher, Working Paper No. 18, p. 1, published 2018, available at https://www.lda.bayern.de/media/dsk_kpnr_18_risiko.pdf. Retrieved October 24, 2021.

[740] Datenschutzkonferenz: Risiko für die Rechte und Freiheiten natürlicher, Working Paper No. 18, p. 1, published 2018, available at https://www.lda.bayern.de/media/dsk_kpnr_18_risiko.pdf. Retrieved October 24, 2021.

[741] Coherence mechanisms were usually only important for BCRs or the like; businesses typically faced the problem of multiple interpretation of the law in multiple jurisdictions, especially as there are typical overlaps with other areas of law such as labor or competition or IT-security laws.

[742] Winfried Veil: Die Schutzgutmisere des Datenschutzrechts (Teil II). Article published February 6 2019, available at https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/. Retrieved October 24, 2021.

data protection in the sense of: what exactly is to be protected? What is so valuable that no deviations are accepted? As for the latter, GDPR Article 9 (2) a makes a clear statement on the relationship of sensitive data and individuals' consent: the processing of sensitive data such as health, biometric or genetic data or personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership is not permitted unless certain exceptions which are listed in GDPR Article 9 (2) lit. a to lit. j apply. One exception is that the data subject has given explicit consent to the processing of those personal data for one or more specified purposes – but Union or member state law may provide that the prohibition may not be lifted by the data subject. This is an important aspect as it shows that individual's rights and freedoms may have limitations, but these restrictions are for their own good, in favor of data subjects, not the processors. Whenever the sense behind data protection regulation is questioned, there is a tendency to summarize data protection legislation by saying that data protection is not about the protection of data, but about the protection of the individuals behind the data. This may well be the case, but it is truly not the only aspect as many years of case law for example in Germany show: many courts believe that data protection requirements may, depending on the case,[743] also be relevant to competition law.[744] In the US, the Federal Trade Commission states that data protection is about consumer protection,[745] and this this view is understandable as the example preset (default) checkboxes in the framework of online bookings and the like shows: this is a good example of inadmissible practices which are not tolerated, neither from a data or consumer protection nor from a competition law perspective. This example shows that various areas of law can go hand in hand, and as regards the Regulation, GDPR itself says that individuals' (fundamental) "*rights and freedoms*" shall be protected. That much is undisputed, but at the same time, the scope and concrete content of this statement is unclear. The challenge is that this is an important prerequisite as none of the many interpretation issues of the GDPR can be answered in a reasonable and satisfying manner as long as the protected good(s) remain unclear: the problem is that, without an identification of the protective goals and the protected goods, there is no benchmark for numerous considerations controllers have to undertake in the framework of various necessity, proportionality, compatibility and risk tests.[746] If we set aside complex legal discussions and have a

[743] Some authors believe that it is likely that infringements of transparency needs may lead to the issuance of warnings, whereas other violations shall not automatically serve as a justification for competitors to initiate actions, see Marlene Schreiber: Drohen wettbewerbsrechtliche Abmahnungen wegen Verstößen gegen die DSGVO? Article published July 4 2018, available at https://www.haerting.de/neuigkeit/drohen-wettbewerbsrechtliche-abmahnungen-wegen-verstoessen-gegen-die. Retrieved October 24, 2021.

[744] Niko Härting provides an overview over the relevant case law in Germany: Sind Datenschutzverstöße abmahnfähig? Ein Rechtsprechungsüberblick. Article published July 24 2013, and is available at https://www.cr-online.de/blog/2013/07/24/sind-datenschutzverstose-abmahnfahig-ein-rechtsprechungsuberblick/. Retrieved October 24, 2021.

[745] However, there are discussions of whether or not an additional federal authority shall be introduced in the US to cover Internet privacy and data security as this could enhance consumer protection. News entry published March 7 2019, available at https://www.gao.gov/products/GAO-19-427T. Retrieved October 24, 2021.

[746] Winfried Veil: Die Schutzgutmisere des Datenschutzrechts (Teil I). Article published February 6 2019, available at https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/. Retrieved October 24, 2021.

look at what the underlying intensions of data subjects' rights are, the following examples can show what shall be protected: the right to be forgotten is about the right to make a fresh start,[747] and Google Spain is a perfect example for that. The right not to be subject to automated decision-making is rather about enabling due process and preventing discrimination[748] than about objecting sophisticated data processing, and the principles of fairness and storage limitation reflect these ideas.

Apart from individuals' rights and freedoms, already the title of the Directive and the Regulation indicate that the free flow of personal data shall be protected (enabled). And given that processing is regularly possible when public interests are in question, this shows that processing of personal data which takes place in public interest is privileged.[749] Further literal interpretation of the Regulation allows for the assumption that there are good arguments that privacy self-management is anchored in the Regulation. Irrespective of the obvious fact that consent is equivalent to the exercise of control, several Recitals operate with the term "*control*" when talking about rights and freedoms of natural persons: Recital 7 says that natural persons shall have control over their own data, and Recital 75 deals with risks to rights and freedoms of data subjects and explains that risks may occur when data subjects are prevented from exercising control over their personal data. Finally, Recital 85 specifies that a "*personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data*". Altogether, these text passages reinforce the importance of exercising control in the framework of data subject rights, but the comprehensive protective purpose of the Regulation which is expressed in the detailed catalogue of examples for potential risks and harms Recital 75 presents, is viewed critically by some authors who say that "*no life risk of this world remains unmentioned in Recital 75*",[750] and who warn that the Regulation may degenerate into an end in itself, finishing with the question where data protection actually ends. In this regard, other authors underline that data protection law, unlike other areas of law, does not dispose of limiting, restrictive criteria and is thus about to change the nature of the data protection regime to a fully prehensive cover.[751] Other authors raise similar concerns by saying that, owing to the fact that more and more data may be considered as personal data, literally

[747] Raphael Gellert: Understanding data protection as risk regulation, Journal of Internet Law 2015, p. 6.
[748] In his article, Raphael Gellert stresses that, in his view, the biggest issues stemming from automated data processing are not violations of privacy, but social sorting practices which are discriminating and also infringe upon the right to due process.
[749] GDPR Article 6 (1) lit. e allows for the processing of personal data when public interest is in question, even for sensitive data (GDPR Article 9 (2) lit. g, even for data transfers to third countries (GDPR Article 49 (1) lit. d.
[750] Niko Härting: Wann ist eine Datenverarbeitung eigentlich erforderlich? Article published February 1 2019, available at https://www.cr-online.de/blog/2019/02/01/wann-ist-eine-datenverarbeitung-eigentlich-erforderlich/. Retrieved October 24, 2021.
[751] In this regard, the author quotes the euivalence theory and adequacy theory which is used in other areas of law: Winfried Veil, Die Schutzgutmisere des Datenschutzrechts (Teil I). Article published February 6 2019, available at https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/. Retrieved October 24, 2021.

any handling of data will be subject to data protection laws,[752] which could lead to undesired incentives for companies to abandon de-identification and therefore increase rather than alleviate privacy risks. It is undisputed that the question of whether information may be viewed as personally identifiable is a fundamental normative question, but the way in which data protection laws (and corresponding sanctions) shall be interpreted and applied very much depends on the question on what exactly is to be protected. Contrary to common acceptations of data protection as data privacy, some authors suggest that data protection shall be interpreted as a legal framework for the regulation and risks to fundamental rights.[753] They claim that mechanisms and tools of data and risk regulation are similar as both rely on methods which involve proportionality (balancing) testing, and they also stress that data protection was a technology-specific legislation at the time of its emergence.[754] The simple reason for this was that data protection laws were a reaction to technical developments. Record keeping as such existed for centuries, but the difference is that new technologies pose new risks.[755] This argument is underlined by the fact that, for example the 1980 OECD Guidelines apply to "*personal data, which, because of the manner in which they are processed, (...) pose a danger to privacy and individual liberties*". There is good reason why the Regulation chose a risk-based approach and why specific rules for certain (high-risk) processing of personal data exist which arise from modern data processing technologies.

c) Significance of accountability

The issue of indeterminate legal terms has not only been raised in the framework of basic definitions, the interpretation of terms is also relevant for the meaning and scope of the accountability principle:[756] The term accountability itself only appears in GDPR Article 5 (2) and GDPR Article 24 (1). According to GDPR Article 5 (2), the "*controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*." GDPR Article 24 (1) says that the "*controller shall implement appropriate (...) measures to (...) be able to demonstrate that processing is performed in accordance with this regulation*". On the one hand, it is clear that the accountability principle leads to a catalogue of tasks businesses have to perform in order to demonstrate that they are compliant with the Regulation, for example by preparing corresponding documentation to serve as evidence.[757] On the

[752] Omer Tene, Jules Polonetsky: Privacy in the age of big data – a time for big decisions, Stanford Law Review 2012, vol. 64:63, p. 66.

[753] Raphael Gellert: Understanding data protection as risk regulation, Journal of Internet Law 2015, pp. 3-15.

[754] Viktor Mayer-Schönberger: Generational Development of Data Protection in Europe, in: Philip E. Agre – Marc Rotenberg (eds.): Technology and Privacy: The New Landscape, Massachusetts Institute of Technology Press 1998, Cambridge and London, pp. 224.

[755] Raphael Gellert: Understanding data protection as risk regulation, Journal of Internet Law 2015, p. 4.

[756] For instancr, Winfried Veil: Accountability – Wie weit reicht die Rechenschaftspflicht der DSGVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, Zeitschrift für Datenschutz 2018, Vol. 1, pp. 9-16.

[757] E.g., records of processing activities, templates for contract or consent, impact assessments, policies, etc.

other hand, the Regulation pursues a risk-based approach[758] as Recitals 75 and 76 clearly show that GDPR distinguishes between processing activities with a high and a low likelihood and severity of the risk to the rights and freedoms of data subjects. Various articles of the General Data Protection Regulation stress this approach, for example GDPR Articles 35 and 36: data protection impact assessment, GDPR Articles 33 and 34: data breach notification, GDPR Article 25: data protection by design and by default and GDPR Article 32: security of processing.[759] As a result, low-risk processing activities face a reduced compliance burden, but it is questionable what shall be considered (minimum) standard and therefore subject to fines if there is a proven lack of compliance. In this regard, there is controversy within literature as to whether businesses may claim for themselves the principle of proportionality in the sense of a limitation of the level of requirements to what is commensurate and reasonable.[760] The scope of documentation obligations is only one question; the other issue is that relationship between the controller's obligation to provide evidence has to be balanced against the supervisory authority's duty to investigate an incident: even if the SA has good reason to approach a controller or processor, businesses may well have the duty of cooperation, but there is no duty of self-accusation,[761] because it is up to the SA to solve the case meaning that it is up to the authority to ensure enlightenment.[762] The investigation principle is a basic principle of administrative procedural law,[763] which is accompanied by the right not to incriminate themselves. An (absurd) comparative example would be that, any driver would have to demonstrate that he or she obeyed all traffic rules at all times.[764] Another problem is that further regulations such as the draft AI Regulation introduced further roles and responsibilities. On the hand, this shall be welcomed as this may help establish a liability regime and capture all parties involved in the AI value chain; on the other hand, this further complicates the situation, especially for complex processing operations within joint controllership scenarios, meaning that one and the same party may hold several roles.

[758] Nico Härting: Datenschutzgrundverordnung, Dr. Otto Schmidt publishing, Cologne 2016, p. 34.

[759] A summary of risk-relevant provisions can be found in: Thomas Kranig, Andreas Sachs, Markus Gierschmann: Datenschutz-Compliance nach der DSGVO – Handlungshilfe für Verantwortliche inclusive Prüffragen für Aufsichtsbehörden, Bundesanzeiger Ltd. publishing Cologne, 2017, p. 87.

[760] Winfried Veil summarizes the discussion in his 2018 article: Accountability – Wie weit reicht die Rechenschaftspflicht der DSGVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, Zeitschrift für Datenschutz 2018, vol. 1, pp. 9-16.

[761] Thomas Petri in: Spiros Simitis: comment 46 on article 5 GDPR in: Bundesdatenschutzgesetz 2014 edition, Nomos Verlag publishing Baden Baden.

[762] Nico Härting: Post von der Datenschutzbehörde – Risiken des Wohlverhaltens: Was ist zu beachten, wenn eine Datenschutzbehörde Auskünfte verlangt? Article published November 8 2018, available at https://www.cr-online.de/blog/2018/11/08/post-von-der-datenschutzbehoerde-risiken-des-wohlverhaltens/. Retrieved October 24, 2021.

[763] Background information can be found on the German Federal Administrative Court's Website: https://www.bverwg.de/en/rechtsprechung/verwaltungsgerichtsbarkeit/grundsaetze-des-verwaltungsprozesses. Retrieved October 24, 2021.

[764] Gabriele Buchholtz, Rainer Stentzel in: Gierschmann, Schlender, Stentzel, Veil: Kommentar zur Datenschutzgrundverordnung, Bundesanzeiger Verlag publishing, Cologne 2017, note 46 on GDPR Article 5 .

d) Fragmentation

Another problem is that enforcement rules are harmonized, but data protection rules are not: GDPR aimed at providing a single framework for data protection to serve as a response to the fact that member states had a different level of implementation in times of the Directive. The result was that European data protection laws in many cases were substantially different. GDPR's goal to harmonize data protection law is actually questionable given the large number of opening clauses,[765] which result in a number of areas in which businesses may have to cope with different national requirements in each member state, for example employment law.[766] The same applies in the context of freedom of expression including processing of data for journalistic, academic and artistic purposes or literary expression,[767] or when personal data are processed for reasons of national security.[768] Other out-of-scope areas include the processing of national ID numbers[769] and personal data contained in official documents.[770] Member states may moreover create their own rules in relation to controllers or processors which are subject to obligations of professional secrecy.[771] The result is that some issues like sanctions are no longer governed by national law,[772] while many other data processing scenarios continue to be governed by national law.[773] The Regulation therefore preserves the right for member states to uphold or introduce different laws in many areas.

e) Shifting of the protection of fundamental rights to the private sector

If the processing of personal data becomes more difficult, because valid consent is – for a variety of reasons – difficult to obtain, and the processing cannot be justified with the fulfillment of a contract as set forth in GDPR Article 6 (1) lit. b, then the only way to defend the data processing is to use legitimate interests as a legal justification. Consequently, some authors claim that GDPR Article 6 (1) lit. f, that is: legitimate interests, will play a central role in the future of data processing including Big Data and AI applications. The challenge with this development is that, if companies decide about data subject rights in the framework of balancing their fundamental rights and freedoms against their own economic interests, this leads to a shift of the data protection regime: all of a sudden, the private sector becomes the responsible body for the individuals' data protection. Some authors are very critical about

[765] An overview of opening clauses is provided by the law firm of Baker McKenzie in their 2018 GDPR National Legislation Survey, available at https://www.bakermckenzie.com/-/media/minisites/tmt/files/gdpr_national_legislation_survey.pdf?la=en. Retrieved October 24, 2021.
[766] See article 88 GDPR.
[767] See article 85 GDPR.
[768] See article 2 (2 d) GDPR.
[769] GDPR Article 87.
[770] GDPR Article 86.
[771] GDPR Articles 9 (2 I and 3), 14 (5 d), 54 (2) and 90 as well as Recitals 50, 53, 75, 85, 164.
[772] Or have been abandoned, e.g. the registration requirement with the local supervisory authority.
[773] This includes the processing personal data in the context of churches and religious establishments (GDPR Article 91, Recital 165). However, this provision is unlikely to be of practical significance for the vast majority of organizations.

this, and they call this the “*outsourcing of fundamental rights protection*” to controllers. If legitimate interests become the central aspect of the new data protection law, this, in effect, leads to a self-regulatory regime which many criticize as AI ethics washing[774] that can be compared to green washing used in marketing. If internal project managers of companies decide upon the design and implementation of Big Data and AI applications, the problem is that such staff is not qualified in data protection and potentially prejudiced: it may well be assumed that diverging interests between data subjects and organizations are given, and it may also be assumed that the latter could prevail: given the complexity of the data protection regime, employees could simply be overwhelmed by privacy issues and due to the fact that they are personally dependent on their employer as the data controller, they will likely follow employer interests and instructions.

f) Viability of traditional concepts

The General Data Protection Regulation is the first piece of legislation that was created in times when Big Tech and social media companies like Google or Meta already existed. Many authors reflected on the issue of future-proof definitions and the Regulation’s future-viability[775] as much of its concept is based on principles which date back to an era in which technology was by far not as sophisticated as it is now: not only did technology change, but the whole setting in which personal data is being processed changed. It can no longer be assumed that processing is performed by one single controller and that data are held in one central database. Processing of personal data is nowadays characterized by the interaction and networking of many actors, very often crossing many national borders and sometimes, very often with no or little possibility to localize the storage location.[776] Moreover, protection was primarily directed against the state and its institutions, not against private companies. Another significant change is that previously, data used to be a by-product of the purpose for which the data was collected; it is typically not possible to render a certain service without certain data, for example, a delivery address must be used for shipment purposes on top general of customer master data such as name and billing address. Today, the exact opposite is the case: data is no longer a simple by-product – data are collected first in order to deliver the service.[777] Traditional data protection

[774] Jean-Etienne Goubet: AI Ethics – beware of AI ethics washing. Article published September 24 2019, available at https://www.genesys.com/blog/post/ai-ethics-beware-of-ai-ethics-washing. Retrieved October 24, 2021.

[775] Winfried Veil: 21 Thesen zum Irrweg der DSGVO. Article published May 23 2018 in, available at https://www.cr-online.de/blog/2018/05/23/21-thesen-zum-irrweg-der-ds-gvo/#anker4. Retrieved October 24, 2021.

[776] Winfried Veil: 21 Thesen zum Irrweg der DSGVO. Article published May 23 2018, available at https://www.cr-online.de/blog/2018/05/23/21-thesen-zum-irrweg-der-ds-gvo/#anker4. Retrieved October 24, 2021.

[777] Lokke Moerel and Corien Prins: On the death of purpose limitation. Article published June 2 2015, available at https://iapp.org/news/a/on-the-death-of-purpose-limitation/. Retrieved October 24, 2021.

principles like notice and choice[778] or data minimization[779] are appropriate examples of the conflict we are facing: data minimization is difficult to achieve when large amounts of data rely on a large data set and informed consent is difficult to imagine when the vast majority of average users de facto have no idea what exactly can be done with their data and what legal basis for the processing exists, in particular because many operations can be justified by legitimate interests and 'compatible' processing in accordance with GDPR Article 6 (1) lit. f and 6 (4). Far too often the consent requirement has degenerated into a mere click mechanism, and therefore, privacy self-management does not seem to be viable anymore.

V. Rules at national level

1. National data protection laws

One of GDPR’s main goals was to harmonize data protection rules throughout Europe. However, owing to various mandatory and optional opening clauses,[780] member states shall and may carve out exceptions within the Articles of the Regulation. It was therefore necessary for member states to pass GDPR implementation laws.[781] As a result, businesses will have to comply with both, the legal framework of the GDPR and (potentially deviating) national legal frameworks of the specific countries where they operate.[782] In addition, due to GDPR’s wider scope, even companies who do not have their seat within the European Union are also required to comply with GDPR. US businesses face further challenges, because they have to comply with the so-called Fair Information Practice Principles and moreover, California issued a new privacy act:[783] just like GDPR, the California Consumer Privacy Act may also apply to companies located outside California,[784] but even though both laws

[778] Daniel Solove: Introduction – Privacy Self-Management and the Consent Dilemma, Harvard Law Review 2013, vol. 126:1880, p.1903.

[779] Ira Rubinstein discusses this issue in his 2013 article: Big Data: The End of Privacy or a New Beginning? International Data Privacy Law 2013, Vol. 3, No. 2, p. 74.

[780] Lukas Feiler: Die 69 Öffnungsklauseln der DSGVO - Regelungsspielräume der nationalen Gesetzgeber. Presentation held on June 1 2017, available at http://www.lukasfeiler.com/presentations/Feiler_Die_69_Oeffnungsklauseln_der%20DS-GVO.pdf. Retrieved October 3, 2021.

[781] An overview over GDPR implementation laws and drafts can be found at IAPP’s website: https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/. Retrieved October 3, 2021.

[782] Jan Dhont and Lauren Cuyvers: National Variations Further Fragment GDPR, The National Law Journal June 2018 edition. Article published June 26 2018, available at https://www.alstonprivacy.com/gdpr-fragmentation-may-appear-more-significant-than-intended/.

[783] Source: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. Retrieved October 3, 2021.

[784] Lydia de la Torre: GDPR matchup – The California Consumer Privacy Act. Article published July 31 2018, available at https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/. Retrieved October 3, 2021.

share some general features, their actual provisions are quite different.[785] As a result, companies that are subject to multiple jurisdictions will have to make a significant effort to achieve compliance with all relevant regulations, particularly when sector-specific (e.g. banking, health, etc.) rules have to be obeyed as well. It can therefore generally be said that the problem of (undesired) fragmentation of laws remains significant. Depending on the organization in question, legal uncertainty may worsen and legal complexity may increase:

2. Emerging US data protection laws

Safe Harbor and the Privacy Shield were common examples of a privacy framework, and even though the United States do not have a uniform federal data protection law comparable to the GDPR, it is certainly wrong to assume that there is no privacy legislation: prominent examples of US privacy laws include (sector-specific) laws like the Health Insurance Portability and Accountability Act (HIPAA)[786] and the Children's Online Privacy Protection Act (COPPA).[787] Many states either already have or are about to introduce laws to establish data privacy (and security) requirements for the protection of financial account numbers, social security numbers as well as health records and medical or other sensitive information, for example New York, Maine, Connecticut, Illinois, Maryland, Nebraska, North Dakota, Texas, Nevada, Washington, Florida or Virgnia.[788] In this context, California was a pioneer: the 2018 California Consumer Privacy Act (CCPA) and the California Online Privacy Protection Act (CalOPPA)[789] positioned California at the top of the list for the toughest data rules in the country. While the emergence of privacy laws in the US as such shall be welcomed, some describe recent developments as a disparate landscape in need of consolidation.[790] The US privacy landscape became so dynamic that some specialized law firms provide weekly status information about the status of proposed CCPA-like state privacy legislation.[791]

[785] Kristen Mathews and Courtney Bowman: The California Consumer Privacy Act of 2018. Article published July 13 2018, available at https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/. Retrieved October 3, 2021.

[786] HIPAA text available at: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf. Retrieved October 3, 2021.

[787] COPPA text available at: https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim. Retrieved October 3, 2021.

[788] Brian Hengesbaugh explains the emerging US privacy landscape in BakerMcKenzie's blog on US state laws which is available at https://www.connectontech.com/tag/us-state-laws/.

[789] California Online Privacy Protection Act text available at: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC. Retrieved October 3, 2021.

[790] Jacob Nix, Pascal Bizarro: US Data Privacy Law: A Disparate Landscape in Need of Consolidation. Article published September 9 2020, available at https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/us-data-privacy-law-a-disparate-landscape-in-need-of-consolidation. Retrieved October 3, 2021.

[791] David Stauss for Husch Blackwell: Status of Proposed CCPA-Like State Privacy Legislation as of May 3, 2021. Article published May 2 2021, available at https://www.bytebacklaw.com/2021/05/status-of-proposed-ccpa-like-state-privacy-legislation-as-of-may-3-2021/. Retrieved October 3, 2021.

3. Consumer protection laws

Existing laws in the US show that there is overlap between privacy protection and consumer protection, for example the Gramm-Leach-Bliley Act (GLBA)[792], the Telemarketing Sales Rule (TSR)[793] as well as the Telephone Consumer Protection Act (TCPA)[794] and the CAN SPAM Act[795]. Another prominent example in this regard is the Fair Credit Reporting Act (FCRA)[796] that applies in the context of housing, insurance, employment and credit: while, for example, traditional credit scoring is based on traditional characteristics such as historical information on how individuals meet their credit obligations, modern scoring works with non-traditional characteristics such as social media usage or shopping behavior: analysis on historical information about the individual in question is replaced by predictive analytics based on a comparison of other consumers' behaviors.[797]

4. Competition law

GDPR does not contain a specific article on marketing, but Recital 47 (7) states that "*the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest*".[798] One may thus suggest that contacting individuals via electronic mail for commercial purposes is admissible. However, Article 13 of the ePrivacy Directive obliges member states to prohibit unsolicited e-mail advertising.[799] As for the relationship between the PECD and GDPR, GDPR Article 95 says that GDPR applies to all data protection issues unless special provisions with the same regulatory objective result from PECD.[800] Therefore, the prevailing opinion in Germany is

[792] Gramm-Leach-Bliley-Act text available at: https://www.sec.gov/about/laws/glba.pdf. Retrieved October 3, 2021.

[793] Telemarketing Sales Rule text available at: https://www.ecfr.gov/cgi-bin/text-idx?SID=e37d3cd088c6b4724a389338f9c3e141&mc=true&tpl=/ecfrbrowse/Title16/16cfr310_main_02.tpl. Retrieved October 3, 2021.

[794] Telephone Consumer Protection Act text available at https://www.govinfo.gov/content/pkg/FR-2012-06-11/pdf/2012-13862.pdf. Retrieved October 3, 2021.

[795] The text of the CAN SPAM Act is available at: https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf. Retrieved October 3, 2021.

[796] Fair Credit Reporting Act text available at: https://www.ecfr.gov/cgi-bin/text-idx?SID=2b1fab8de5438fc52f2a326fc6592874&mc=true&tpl=/ecfrbrowse/Title16/16CIsubchapF.tpl. Retrieved October 3, 2021.

[797] Federal Trade Commission: Big Data – a Tool for Inclusion or Exclusion? Understanding the Issues, FTC Report issued January 2016, available at https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report. Retrieved October 3, 2021.

[798] Provided that a (documented) balancing of interests took place.

[799] The German legislator has fulfilled this obligation by creating § 7 UWG (Gesetz gegen den unlauteren Wettbewerb: German Federal law against unfair competition).

[800] Recital 173 (Relationship to Directive 2002/58/EC) says that "*This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council¹, including the obligations on the controller and the rights of natural persons. ²In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. ³Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation*".

that this provision thus leads to the fact that § 7 UWG is retained with the consequence that e-mail advertising is only possible with the explicit consent of the recipient[801] - contrary to many jurisdictions with "*can-spam-acts*"[802] or "*soft opt-in*"-concepts.[803] E-mail-marketing may not be a standard use case of Big Data.[804] But the legal framework which governs the activity is a good example of how complex the situation for globally active businesses has become. Moreover, harvesting of contact details such as email-addresses from a website or proprietary online service using automated means is a method of data collection in preparation of Big Data analytics, and this is explicitly covered (forbidden) in certain jurisdictions.[805]

5. IT security laws including Cybersecurity and Internet of Things

It is hardly feasible to provide an overview over all applicable IT-, IoT and cyber-security laws.[806] However, data protection is not possible without data security, and it is therefore a must to include a brief overview over IT-security laws: against the background of increasing threats like cyber-attacks, industrial espionage and owing to the growing complexity of IT infrastructures, many European countries enacted IT-/cyber-security laws of their own.[807] Given the importance of the issue, similar laws exist in most jurisdictions, including the U.S.A., where the Internet of Things Cybersecurity Improvement Act has recently been introduced.[808] The U.S.A. also have specific data breach laws at

[801] Detailed background information is provided by Intersoft Consulting Services: E-Mail-Werbung künftig auch ohne Einwilligung möglich? Article published on their company website on March 30 2017, available at https://www.datenschutzbeauftragter-info.de/e-mail-werbung-kuenftig-auch-ohne-einwilligung-moeglich/. Retrieved October 3, 2021.

[802] In February 2019, the Federal Trade Commission voted to retain the US "Can Spam Act": https://www.lexology.com/library/detail.aspx?g=6379a9eb-e07d-495d-8118-f804647303d5. Retrieved October 3, 2021.

[803] While the basic rule in many countries is that businesses must not send marketing emails to individuals without specific/prior consent, a typical exception applies for own previous customers. UK's Information Commissioner's Office offers background information on the so-called "soft-opt-in" which is available at https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/. Retrieved October 3, 2021.

[804] Even though email marketing activities are subject to different analyses of click rates and the like.

[805] Email harvesting without authorization is prohibited under section 5 (b) of the 2003 US Can Spam Act, available at https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf. Retrieved October 3, 2021.

[806] There are not only laws, but also recommendations, for instance, European Commission recommendation on cyber-security in the energy sector which builds on recent EU legislation in this area, including the NIS Directive and EU Cyber-Security Act. The recommendation was issued on April 3, 2019 and is available at https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf. Retrieved October 3, 2021.

[807] For example, Germany with its 2015 IT-Sicherheitsgesetz (German IT Security Act). This act amends and supplements the German federal Energy Industry Act, the Tele-Media Act, the Telecommunications Act and other laws, source: German Federal Office for Security in Information Technology, available at https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_IT_SiG/neur_IT_SiG_node.html. Retrieved October 3, 2021.

[808] The text of the IoT Cybersecurity Improvement Act of 2020 is available at https://www.congress.gov/bill/116th-congress/house-bill/1668. Retrieved October 3, 2021.

both, federal[809] and state level.[810] With regards to key state data privacy and security laws, all US states have breach notification laws.[811] In addition, case law confirms and concretizes certain entrepreneurial obligations which are considered compliance-relevant, for example in the area of security of communications and IT-outsourcing, or in the context of the preservation of evidence or disaster and recovery management.[812]

6. Equal opportunity laws

The U.S.A. are a good example of a country with a multitude of laws that prohibit discrimination based on characteristics such as age, gender, disability, race, origin or marital status: e.g., a lender must not refuse to offer (certain conditions for) loans to a single person as opposed to a married person even if Big Data analytics suggest that single persons are less likely to pay back their mortgage than married individuals.[813] Other examples of equal opportunity laws are the Age Discrimination in Employment Act,[814] the Fair Housing Act,[815] and the Genetic Information Nondiscrimination Act[816] to only name a few.

[809] Federal data breach notification requirements are mostly sector-specific, for instance, the Gramm-Leach-Bliley Act for the financial sector or HIPAA and further laws which govern the health sector. A summary on this topic is provided by Al Saikali in his 2012 article: Federal Data Breach Notification Laws, available at https://www.datasecuritylawjournal.com/2012/05/06/federal-data-breach-notification-laws/. Retrieved October 3, 2021.

[810] An overview over state breach notification laws is provided by Steptoe & Johnson LLP: Comparison of US State and Federal Security Breach Notification Laws, available at https://www.steptoe.com/images/content/1/7/v2/175438/Comparison-of-Security-Breach-Notification-Laws-Updated-6-1-201.pdf. Retrieved October 3, 2021.

[811] BakerMcKenzie: Global Data Privacy & Security Handbook, last updated: 9 February 9 2020, available at https://globaltmt.bakermckenzie.com/data-privacy-security/views/jurisdiction-view?id=4b2271a7b1ef4bbd88e79183b52b3a7c&section=5cfdfd0aa92d44e6848a792f31ddcb67. Retrieved October 3, 2021.

[812] Jens Bücking: Datenschutzgrundverordnung, NIS-Richtlinie der EU und das IT-Sicherheitsgesetz – ein neues, einheitliches Datensicherheits-/Datenschutzrecht für Europa, working paper provided by SEP Software Corp., available at https://www.sep.de/fileadmin/user_upload/Compliance/SEPsesam_Compliance_de_web.pdf. Retrieved October 3, 2021.

[813] Federal Trade Commission: Big Data – a Tool for Inclusion or Exclusion? Understanding the Issues, FTC Report issued January 2016, available at https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report. Retrieved October 3, 2021.

[814] Background information on the Age Discrimination in Employment Act of 1967 can be found at the U.S. Equal Employment Opportunity Commission at https://www.eeoc.gov/statutes/age-discrimination-employment-act-1967. Retrieved October 3, 2021.

[815] Source: U.S. Department of Justice: https://www.justice.gov/crt/fair-housing-act-1#:~:text=The%20Fair%20Housing%20Act%20prohibits%20discrimination%20on%20the,substantially%20limit%20one%20or%20more%20major%20life%20activities. Retrieved October 3, 2021.

[816] A factsheet on the Genetic Information Nondiscrimination Act is available at the U.S. Equal Employment Opportunity Commission's website: https://www.eeoc.gov/laws/guidance/fact-sheet-genetic-information-nondiscrimination-act#:~:text=Title%20II%20of%20the%20Genetic%20Information%20Nondiscrimination%20Act,training%20and%20apprenticeship%20programs%2C%20and%20the%20federal%20government. Retrieved October 3, 2021.

7. Labor law and industrial constitution laws

Variations of the applicable legal framework may also arise in the area of labor law,[817] especially when company-internal rules arising from works council agreements[818] have to be considered on top of existing employment law. This can lead to restrictions in the use of data, since such agreements can stipulate that certain (performance-relevant) data must not be processed or analyzed. The employment context is generally a good example as regards admissible use of information, including applicable timings: while it may not be permissible to collect data on the fact that an applicant is pregnant, once the employment relationship is established, the same person will have to report this circumstance because the employer has a duty of care and is obliged to implement protective measures if need be (depending on the workplace). However, all such constraints are only relevant to analyses which are carried out on the basis of employee data, a much smaller use case[819] than in other areas.

VI. Specific rules for algorithm-based decisions, ADM and AI

In the context of data protection laws which have to be taken into consideration for Big Data, ADM and AI applications, sector-specific rules (e.g., banking) as well as product (e.g., health appliance), incident (e.g. data breach), infrastructure (e.g. certain types of plants) and data-specific (e.g., information relating to children) rules apply. Moreover, data residency rules may require that (a copy of) data is stored locally also must be considered.[820] Other provisions may foresee that certain information (e.g. technical data, data worthy of protection for reasons of national security) must be handled in a certain manner and / or stored locally, meaning that trade compliance may also lead to challenges with regards to export controlled data may being stored in the Cloud.[821] To name all relevant provisions would go beyond the scope of this work, so that this section of the paper only serves to point out that, depending on the type of business activity, sector-, product and further specific rules may apply which have to be obeyed as well.[822] This circumstance increases the legal

[817] A simple example is that the German Federal Data Protection Law enacted in the course of the introduction of GDPR (as a basic rule with exceptions) requires written consent from employees (see § 26 II 3 BDSG).

[818] GDPR Article 88: processing of personal data in the context of employment.

[819] Those are in many cases due to compliance requirements, for instance, background screenings, analysis of Internet usage, use of cyber-security tools for the protection of company systems.

[820] Consequently, specialized data-residency-as-a-service vendors emerged as Ryan Chiavetta reports in his 2019 article: Tech vendor looks to tackle data localization compliance. The article was published July 18 2019, and is available at https://iapp.org/news/a/tech-vendor-looks-to-tackle-data-localization-compliance/. Retrieved October 3, 2021.

[821] Background information on trade and export compliance is provided by BakerMcKenzie in their 2020 article: US – DDTC issues ITAR rule affecting technology transfers, encryption and cloud computing. Article published January 31 2020, available at https://www.internationaltradecomplianceupdate.com/2020/01/31/us-ddtc-issues-itar-rule-affecting-technology-transfers-encryption-and-cloud-computing/. Retrieved October 3, 2021.

[822] Not only in the form of a law: see the "Generally Accepted Privacy Principles" which the Canadian Institute of Chartered Accountants introduced together with the American Institute of Certified Public Accountants. The 2009 version of their GAPPs is available at https://iapp.org/media/presentations/11Summit/DeathofSASHO2.pdf. Retrieved October 3, 2021.

complexity, because sector-specific regulations exist at national (federal) and at EU level, both in the EU and in the US: compliance-rules such as anti-money-laundry provisions and the like typically exist at national level; federal data breach notification requirements for the financial and health sector are a typical example sector-specific US laws at federal level,[823] whereas the Clinical Trial Regulation[824] is an example of an industry-specific regulation at EU level. This regulation intends to harmonize the market as regards clinical trials and medicinal products and introduces rules on the protection of individuals, including informed consent and transparency requirements.[825] It thus contains specific data protection provisions including rules on the secondary use of clinical trial data outside the clinical trial protocol for scientific purposes, which may become relevant in the context of Big Data and AI applications.[826]

1. Regulations at international and sectoral level

a) Traffic: Vienna Convention on Road Traffic, UN Regulation on Automated Lane Keeping Systems

Even though some consider that the regulation of AI is in its infancy, there are indeed advanced regulations in certain industries, and that is especially true with regard to autonomous driving: the 1968 Vienna Convention on Road Traffic was amended in 2016[827] in order to allow for transferring driving tasks to autonomous vehicles (AV); AV is considered one of the most remarkable use cases and one of the most critical components in the so-called Fourth Industrial Revolution,[828] and many

[823] For example, HIPAA for the health sector or the Gramm-Leach-Bliley Act for the banking sector. Further details on US data breach notification requirements are provided by Al Saikali in his 2012 -article: Federal Data Breach Notification Laws, available at https://www.datasecuritylawjournal.com/2012/05/06/federal-data-breach-notification-laws/. Retrieved October 3, 2021.

[824] Source: https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/reg_2014_536/reg_2014_536_en.pdf. Retrieved October 3, 2021.

[825] EDPS opinion issued in January 2019 concerning the interplay between the Clinical Trials Regulation and the General Data Protection regulation: Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), p. 3, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf. Retrieved October 3, 2021.

[826] EDPS opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), p. 8. The text of EDPS' opinion 3/2019 is available at https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en. Retrieved October 3, 2021.

[827] The corresponding press release: UNECE paves the way for automated driving by updating UN international convention was published March 23, 2016 and is available at https://www.unece.org/info/media/presscurrent-press-h/transport/2016/unece-paves-the-way-for-automated-driving-by-updating-un-international-convention/doc.html. Retrieved October 3, 2021.

[828] World Economic Forum: Filling Legislative Gaps in Automated Vehicles, white paper in cooperation with Sompo Holdings Inc. Paper published April 2019, available at http://www3.weforum.org/docs/WEF_Filling_Legislative_Gaps_in_Automated_Vehicles.pdf. Retrieved October 3, 2021.

countries engage in testing of such vehicles.[829] And there is further development in the area of autonomous vehicles: while for example an autopilot system is level 2, the new rules on Automated Lane Keeping Systems (ALKS) that will come into force in 2021 are the first international binding regulation[830] on level 3; level 5 is fully automated with features that can drive the vehicle under all conditions.[831]

b) Weapons: Convention on Certain Conventional Weapons[832] and Lethal Autonomous Weapons Systems

Regulations are also in place with regards to the use of lethal autonomous weapons systems (LAWS).[833] Many countries enacted laws on autonomous weapons,[834] and many call for a regular and systematic review in this area to ensure that humans remain in control of such technologies and prevent the creation and use of harmful applications.[835]

c) Finance: MiFID II[836]

The banking sector is yet another example of an industry that already has rules for algorithms that are being used for high frequency algorithmic trading,[837] and this shows that AI regulation is perhaps not any more in its infancy.

[829] Australia, Canada, China, Germany, New Zealand, the UK and the USA have started government-level discourse around autonomous vehicles, source: May Bayern: Autonomous vehicles: How 7 countries are handling the regulatory landscape. Article published February 5 2020, available at https://www.techrepublic.com/article/autonomous-vehicles-how-7-countries-are-handling-the-regulatory-landscape/. Retrieved October 3, 2021.

[830] UNECE press release published June 25, 2020, available at https://www.unece.org/?id=54669. Retrieved October 3, 2021.

[831] UNECE overview on all levels: https://www.unece.org/fileadmin/DAM/5_Levels_of_Driving_Automation.pdf. Retrieved October 3, 2021.

[832] Background information can be found at United Nations homepage, available at https://www.unog.ch/80256EE600585943/(httpPages)/4F0DEF093B4860B4C1257180004B1B30. Retrieved October 3, 2021.

[833] Background information on the topic is provided by Kenneth Anderson Matthew Waxman: Law and Ethics for Autonomous Weapon Systems: Why a ban won't work and how the laws of war can, American University Washington College of Law Research Paper No. 2013-11, available at http://ssrn.com/abstract=2250126. Retrieved October 3, 2021.

[834] For example, China, South Korea, Israel, Russia, and the UK either use or develop LAWS with decreasing levels of human control, source: Campaign to Stop Killer Robots, Retaining human control of weapons systems. Briefing Note for the Convention on Conventional Weapons Group of Governmental Experts Meeting on Lethal Autonomous Weapons Systems, April 9-13, 2018, available at https://www.stopkillerrobots.org/wp-content/uploads/2018/03/KRC_Briefing_CCWApr2018.pdf. Retrieved October 3, 2021.

[835] Statement by the EU Group of Governmental Experts Lethal Autonomous Weapons Systems Convention on Certain Conventional Weapons, published August 27 2018, available at https://eeas.europa.eu/headquarters/headquarters-homepage/49763/convention-certain-conventional-weapons-group-governmental-experts-lethal-autonomous-weapons_en. Retrieved October 3, 2021.

[836] Markets in Financial Instruments (MiFID II) The text of Directive 2014/65/EU is available at https://ec.europa.eu/info/law/markets-financial-instruments-mifid-ii-directive-2014-65-eu_en.

[837] Danny Busch: MiFID II - Regulating High Frequency Trading, Other Forms of Algorithmic Trading and Direct Electronic Market Access, Law and Financial Markets Review 2016/2, retrieved from:

2. Rules at national and state level: AI, algorithmic and ADM specific rues

Apart from the fact that the United States seem to be moving towards a comprehensive federal privacy and data protection legislation,[838] the country engaged in numerous legal initiatives in the area of Artificial Intelligence as the following examples show: the Advancing American AI Act,[839] the Future of AI Act,[840] the National Artificial Intelligence Initiative Act,[841] the Artificial Intelligence Act[842], the Algorithmic Accountability Act,[843] the AI in Government Act,[844] the Artificial Intelligence Reporting Act,[845] the Advancing AI Research Act,[846] the Growing Artificial Intelligence Through Research Act,[847] the Mind Your Own Business Act,[848] or the Protecting Americans from Dangerous Algorithms Act.[849] The country moreover plans for the establishment of a National Security Commission on Artificial Intelligence[850] and is also very active in the area of Automated Decision Making: many states already have ADM legislation, for example California, Virginia and Colorado, and many others are discussing similar initiatives.[851] What these laws have in common is that they "*borrow some terms and ideas from the EU's General Data Protection Regulation*,"[852] for example, by foreseeing that internal duties include risk assessments and that external duties include meaningful information of individuals. The interesting development in this context is that, for example, the Colorado Privacy Act[853] says that Data Protection Assessment for high-risk profiling will be required to be made available to the Attorney General upon request. However, one issue to consider is that unlike GDPR,

https://ssrn.com/abstract=3068104 or http://dx.doi.org/10.2139/ssrn.3068104 explains how algorithmic trading to subject to supervision. Retrieved October 3, 2021.

[838] Shiva Stella: Senate Releases Principles for Comprehensive Privacy Legislation. Article published on November 18 2019, available at https://www.publicknowledge.org/press-release/senate-releases-principles-for-comprehensive-privacy-legislation/. Retrieved October 3, 2021.

[839] Source: https://www.congress.gov/bill/117th-congress/senate-bill/1353/text?q=%7B%22search%22%3A%5B%22data+OR+privacy%22%5D%7D&r=27&s=5. Retrieved October 3, 2021.

[840] Source: https://www.congress.gov/bill/115th-congress/house-bill/4625. Retrieved October 3, 2021.

[841] Source: https://www.congress.gov/bill/116th-congress/house-bill/6216. Retrieved October 3, 2021.

[842] Benjamin Muller: The Artificial Intelligence Act – a quick explainer. Article published on May 4 2021, available at https://datainnovation.org/2021/05/the-artificial-intelligence-act-a-quick-explainer/. Retrieved October 3, 2021.

[843] Source: https://www.congress.gov/bill/116th-congress/senate-bill/1108. Retrieved October 3, 2021.

[844] Source: https://www.congress.gov/bill/115th-congress/senate-bill/3502. Retrieved October 3, 2021.

[845] Source: https://www.congress.gov/bill/115th-congress/house-bill/6090/. Retrieved October 3, 2021.

[846] Source: https://www.congress.gov/bill/116th-congress/senate-bill/3891. Retrieved October 3, 2021.

[847] Source: https://www.congress.gov/bill/116th-congress/house-bill/2202. Retrieved October 3, 2021.

[848] Source: https://www.congress.gov/bill/117th-congress/senate-bill/1444/text?q=%7B%22search%22%3A%5B%22automated+decision-making%22%5D%7D&r=3&s=3. Retrieved October 3, 2021.

[849] Source: https://www.congress.gov/bill/117th-congress/house-bill/2154?q=%7B%22search%22%3A%5B%22algorithmic%22%5D%7D&s=1&r=2.

[850] Source: https://www.congress.gov/bill/115th-congress/house-bill/5356/. Retrieved October 3, 2021.

[851] Pollyanna Sanderson: Automated Decision Systems Legislation Update, presentation held on June 14 2021 during a Future of Privacy Forum meeting.

[852] Angelique Carson: Colorado Privacy Act (CPA): What is it? Article published June 11 2021, available at https://www.osano.com/articles/colorado-privacy-act-what-is-it.

[853] Source: https://leg.colorado.gov/bills/sb21-190. Retrieved October 3, 2021.

many of these laws are concerned with consumers[854] and not addressed towards individuals, which leads to the question if privacy protections do not apply to individuals which do not qualify as consumers. Obviously, such a variety of definitions and such a high degree of fragmentation will lead to challenges at implementation level.

VII. Product, purpose and data-(processing) specific rules

1. Biometric data and facial recognition

Apart from the above-mentioned rules for the finance industry as well as autonomous weapons and vehicles, there are the only few other areas of AI for which specific rules already exist. In this regard, facial recognition technology is a good example: in the US, Illinois passed the Biometric Information Privacy Act (BIPA) already in 2008,[855] and several states (for example California, Texas) and numerous cities (for example San Francisco, Seattle or Oakland) either already have or are planning to ban the use of the facial recognition;[856] ditto for further cities around the globe that are taking joint efforts to defend digital rights at municipal level.[857] The opposite is true for China: millions of cameras are used for facial (and voice) recognition that can identify people and monitor their behavior for identification[858] or surveillance purposes,[859] however, the fact that Clearview, a tool that allows to identify individuals based on a single photo, has been used by police[860] shows that the wish to use such technology is present in many jurisdictions: in the framework of its border management, the European Union decided – without great public impact – to introduce a biometrics database which includes

[854] For example, the Colorado Privacy Act, Virginia's CDPA or the New Jersey Disclosure and Accountability Transparency Act, see Pollyanna Sanderson: Automated Decision Systems Legislation Update, presentation held on June 14 2021 during a Future of Privacy Forum meeting.

[855] Michael Lore:: The Illinois Biometric Information Privacy Act. Article published January 31 2020, available at https://www.overtime-flsa.com/illinois-biometric-information-privacy-act-bipa/. Retrieved October 3, 2021.

[856] Source: AI Now Institute 2019 report available at https://ainowinstitute.org/AI_Now_2019_Report.pdf. Retrieved October 3, 2021.

[857] The "Cities Coalition for Digital Rights" is a network of cities helping each other in the greenfield of digital rights based policy-making and was launched by the cities of Amsterdam, Barcelona and New York in 2018 and now has more than 50 cities worldwide, source: https://citiesfordigitalrights.org/about. Retrieved October 3, 2021.

[858] Researcher found a database used to track a certain ethnic group, because the corresponding database was accessible on the internet for months, source: Chinese company leaves Muslim-tracking facial recognition database exposed online, blog entry published on February 14, 2019, available at https://www.zdnet.com/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/. Retrieved October 3, 2021.

[859] Bill Gertz: Social credit score: China set to roll out "Orwellian" mass surveillance tool. Article published December 9 2019, available at https://www.washingtontimes.com/news/2019/dec/9/social-credit-system-china-mass-surveillance-tool-/. Retrieved October 3, 2021.

[860] Ariel Bogle: Australian Federal Police officers trialed controversial facial recognition tool Clearview AI. Article published on April 15 2020, available at https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894. Retrieved October 3, 2021.

fingerprints and facial scans, the "*Common Identity Repository*."[861] The database was designed to allow for better tracking of immigration and criminals and will be one of the largest information systems for retrieving biometric data worldwide, putting Europe "*right behind the Chinese government and India's Aadhar system in terms of the size of people-tracking databases*". There is fear that the system may be expanded to track people that are not the subject of criminal investigations, for example tourists, and this way, millions of EU citizens might be affected, and not only criminals.[862] Some therefore consider this to be a harmful step and comment on the initiative as "a *Big Brother centralized EU database including all existing and future Justice and Home affairs databases*." [863] Against this background, the campaign "*Reclaim Your Face*" calls for a ban on mass surveillance with the help of biometric information, demanding that authorities take note of serious risks implied with the use of facial recognition and other biometric technologies in public spaces[864] - and not only in public spaces: today's technology shows that the use of static information that would have previously been considered non-sensitive data should be reconsidered, because it became fairly easy to, for example, manipulate pictures by "*morphing faces to influence voters"*[865], or by producing a "*deep fake*" to embarrass or expose someone[866] or by identifying the individuals behind those photos[867] – or by erasing them from a group picture.[868]

2. Genetic information

Florida enacted a new genetic privacy law in October 2021 which establishes four new crimes related to the unlawful use of another person's DNA, the Protecting DNA Privacy Act (HB 833).[869] Florida is only one of many examples within the U.S.A. of a state that demonstrates an increased focus on

[861] Background information is available at and was available at https://www.securityresearch-cou.eu/sites/default/files/02.Rinkens.Secure%20safe%20societies_EU%20interoperability_4-3_v1.0.pdf. Retrieved October 3, 2021.

[862] Tony Bunyan for Statewatch: The "point of no return" - Interoperability morphs into the creation of a Big Brother centralized EU state database including all existing and future Justice and Home Affairs databases. Article published June 2018, available at https://www.statewatch.org/media/documents/analyses/no-332-eu-interop-morphs-into-central-database-revised.pdf. Retrieved October 3, 2021.

[863] Tony Bunyan for Statewatch: The "point of no return" - Interoperability morphs into the creation of a Big Brother centralized EU state database including all existing and future Justice and Home Affairs databases. Article published June 2018, available at https://www.statewatch.org/media/documents/analyses/no-332-eu-interop-morphs-into-central-database-revised.pdf. Retrieved October 3, 2021.

[864] Source: https://reclaimyourface.eu/. Retrieved October 3, 2021.

[865] Adam Gorlick: Researchers say voters swayed by candidates who share their looks, Stanford University report published October 22 2008, available at https://news.stanford.edu/news/2008/october22/morph-102208.html. Retrieved October 3, 2021.

[866] Rachel Metz: Researchers can now use AI and a photo to make fake videos of anyone. Article published May 24 2019, available at https://edition.cnn.com/2019/05/24/tech/deepfake-ai-one-photo/index.html. Retrieved October 3, 2021.

[867] Will Knight: Clearview AI Has New Tools to Identify You in Photos. Article published April 10 2021, available at https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/. Retrieved October 3, 2021.

[868] Kim Lyons : Google Pixel 6 leak teases Magic Eraser feature, plus five years of Android security updates. Article published October 9 2021, available at https://www.theverge.com/2021/10/9/22718007/google-pixel-6-leak-teases-magic-eraser-camera-five-years-android-security-updates. Retrieved October 3, 2021.

[869] Source: https://flsenate.gov/Session/Bill/2021/833. Retrieved October 3, 2021.

genetic privacy protections: California, Arizona and Utah have also started developing genetic privacy laws to govern privacy practices, for example of direct-to-consumer genetic testing companies.[870]

VIII. Private sector initiatives and technical standards

In addition to hard law and soft law at international, European or national level, there are self-regulation initiatives at industry and company level as well as technical developments and standards.

1. Private sector initiatives

Telecommunication companies like Telefónica,[871] Vodafone[872] or German Telekom[873] were amongst the first ones to think about company-own standards and rules with regards to the use of AI. Other companies like Sony[874] of big tech companies like IBM[875] or China's tech giant Tencent[876] followed. Further important players like Google[877] and Microsoft[878] also issued their own AI principles; together with Meta, Amazon and IBM, Google and Microsoft launched the Partnership on AI "*to educate the public, open up dialogue about AI technologies, and identify opportunities to use it to solve problems in the world.*"[879] Google moreover announced that it plans to address specific challenges in the area of AI with the help of an Advanced Technology External Advisory Council.[880] Like many others who

[870] Libbie Canter, Rebecca Yergin: Newly Effective Florida Law Imposing Criminal Sanctions Adds to Developing Nationwide Patchwork of State Genetic Privacy Laws. Article published October 6 2021, available at https://www.insideprivacy.com/health-privacy/newly-effective-florida-law-imposing-criminal-sanctions-adds-to-developing-nationwide-patchwork-of-state-genetic-privacy-laws/. Retrieved October 3, 2021.

[871] Source: (https://www.telefonica.com/en/web/responsible-business/our-commitments/ai-principles). Retrieved October 3, 2021.

[872] Source: https://www.vodafone.com/about-vodafone/how-we-operate/public-policy/policy-positions/artificial-intelligence-framework. Retrieved October 3, 2021.

[873] Source: https://www.telekom.com/en/company/digital-responsibility/digital-ethics-deutsche-telekoms-ai-guideline. Retrieved October 3, 2021.

[874] Source: https://www.sony.net/SonyInfo/csr_report/humanrights/hkrfmg0000007rtj-att/AI_Engagement_within_Sony_Group.pdf#:~:text=The%20%E2%80%9CSony%20Group%20AI%20Ethics%20Guidelines%E2%80%9D%20%28Guidelines%29%20set,and%20services%20by%20Sony%2C%20including%20entertainment%20content%20. Retrieved October 3, 2021.

[875] Source: https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf. Retrieved October 3, 2021.

[876] Wenjun Wu, TiejunHuang, KeGong: Ethical Principles and Governance Technology Development of AI in China, Engineering vol. 6, issue 3, March 2020, pp. 302-309, available at https://doi.org/10.1016/j.eng.2019.12.015. Retrieved October 3, 2021.

[877] Source: https://blog.google/technology/ai/ai-principles/. Retrieved October 3, 2021.

[878] Source: https://www.microsoft.com/en-gb/ai/responsible-ai?activetab=pivot1%3aprimaryr6. Retrieved October 3, 2021.

[879] Tas Bindi: Amazon, Google, Facebook, IBM, and Microsoft form AI non-profit. Article published September 29 2016, available at https://www.zdnet.com/article/amazon-google-facebook-ibm-and-microsoft-form-ai-non-profit/. Retrieved October 3, 2021.

[880] Abner Li: Google names external advisory council to guide artificial intelligence usage. Article published March 26 2019, available at https://9to5google.com/guides/google-ai-principles/#:~:text=Google%20AI%20Google%20AI%20Principles.%20Back%20in%20June%2C,implemented%20to%20ensure%20that%20all%20guidelines%20are%20enforced. Retrieved October 3, 2021.

believe in the future of this technology, Microsoft is involved in research in the topic[881] and runs a project with the Massachusetts Institute of Technology's Computer Science & Artificial Intelligence Lab on Trustworthy & Robust AI Collaboration.[882] Given the fact that Microsoft's applications are used by the vast majority of organizations[883], the company is in the spotlight of the authorities more than others: recently, Microsoft was criticized for some of its AI-based Office 365 applications, for example Delve and Graph: a German regulator conducted two surveys on the use of Microsoft Office 365 in 2019 to find out how local companies use Office 365,[884] and local labor chambers also dealt with Graph, Delve and MyAnalytics since these applications are relevant for the working environment.[885] Controversial discussions around associated data protection risks of (Microsoft) Office 365 are still ongoing between regulators.[886] Moreover, the Dutch Ministry of Security and Justice commissioned a data privacy impact assessment for Microsoft Office ProPlus[887] which came to the result that the use of Microsoft's Office ProPlus Enterprise indeed involves privacy risks,[888] and in mid-2020, the European Data Protection Supervisor initiated an own investigation into EU institutions' use of Microsoft products and services.[889] Apple communicates a different approach: even though not tailored with a specific regard to AI, its consent for IDFA[890] initiative is an example of how privacy by design could be a "*game changer for online and mobile privacy and drive change in a way that legislative efforts have so far been unable*":[891] if users cannot be tracked and targeted without their

[881] Source: https://www.microsoft.com/en-us/research/research-area/artificial-intelligence/?facet%5Btax%5D%5Bmsr-research-area%5D%5B0%5D=13556&sort_by=most-recent. Retrieved October 3, 2021.

[882] Source: https://trac.csail.mit.edu/#:~:text=The%20Trustworthy%20and%20Robust%20AI%20collaboration%20%28TRAC%29%20between,which%20spans%20safety%20%26%20reliability%2C%20intelligibility%2C%20and%20accountability. Retrieved October 3, 2021.

[883] Microsoft's use rate in the public sector in Germany is as high as 96 %, source: Price Waterhouse Coopers 2019 report: Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Article published August 2019, available at https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile. Retrieved October 3, 2021.

[884] Background information on the survey can be found at https://www.datenschutz.bremen.de/sixcms/detail.php?gsid=bremen236.c.16021.de. Retrieved October 3, 2021.

[885] Source: ttps://www.arbeitnehmerkammer.de/fileadmin/user_upload/Veranstaltungen/Veranstaltungsdokumentation/Downloads/Datenschutzrecht_20180221_Hanke.pdf. Retrieved October 3, 2021.

[886] Joerg Heidrich: Datenschutzbehörden erklären den Einsatz von Microsoft 365 für rechtswidrig. Article published October 23 2020, available at https://www.heise.de/news/Datenschutzbehoerden-erklaeren-den-Einsatz-von-Microsoft-365-fuer-rechtswidrig-4931745.html. Retrieved October 3, 2021.

[887] That is, for Office 2016 MSI and Office 365 CTR.

[888] The DPIA was carried out by the "Privacy Company", source: https://www.privacycompany.eu/blogpost-en/impact-assessment-shows-privacy-risks-microsoft-office-proplus-enterprise. Retrieved October 3, 2021.

[889] The outcome is summarized in a paper the EDPB published on July 2 2020, and is available at https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html.

[890] IDFA is an abbreviation for "ID for advertisers", a unique identifier on the Apple iPhone that allows mobile advertisers to track usage of applications on the phone and websites accessed via the mobile browser to use this information for targeting purposes.

[891] Phil Lee: Why Apple's "Consent for IDFA" announcement is a game changer for online and mobile privacy. Article published on June 24, 2020, available at https://www.fieldfisher.com/en/services/privacy-security-and-

consent, this will necessarily impact further data processing as is the custom nowadays: since consent is only valid if it is obtained in an informed manner, it is questionable whether the implementation of opt-in-mechanisms that are typically tailored as a one-time effort can be considered legally valid as this would mean that one single declaration of intent towards an unknown and/or growing number of legally independent entities that engage in different processing operations could suffice as opposed to the repeated solicitation of consent for various companies and different purposes. Apple recently released the latest version of its iPhone operating system, iOS 15: this new operating system brings a slew of privacy-specific features such as the "*Mail Privacy Protection*" feature and the "*Privacy Report*" feature which allows users to check how (often) apps are using (which of) their data.[892] IBM engaged in AI Explainability 360[893], "*a comprehensive open source toolkit of state-of-the-art algorithms that support the interpretability and explicability of machine learning models*." What distinguishes this initiative from others is that is underlines the need to tackle the diversity of explanation as there is no single approach to explaining algorithms.[894]

2. Technical standards

GDPR generally requires appropriate technical and organizational measures to protect personal data, and this is where the International Organization for Standardization (ISO) comes into play: given the complexity and growth of regulatory requirements, compliance is increasingly difficult to achieve, and that is why some companies consider certifications like ISO 27001, the international standard for Information Security Management Systems (ISMS); ISO 27701 is concerned with Privacy Information Management System (PIMS). ISO issued another standard for the protection of personally identifiable information in public clouds. ISO/IEC 27018:2014 is a new code of practice which promotes privacy protection in the cloud. It establishes guidelines "*in order to implement measures to protect personally identifiable information in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment*".[895] Key topics include controls, accessibility and portability as well as

information/privacy-security-and-information-law-blog/why-apples-consent-idfa-announcement-is-a-game-changer. Retrieved October 3, 2021.

[892] Steven Roosa, Daniel Rosenzweig: iOS 15: New Privacy Features Industry Should Note. Article published October 7 2021, available at https://www.ntanalyzer.com/blog/ios-15-new-privacy-features-industry-should-note/. Retrieved October 3, 2021.

[893] Background information on IBM's AI Explainability 360 can be found at http://aix360.mybluemix.net/?_ga=2.210214166.22327519.1624340710-1056213070.1624340710. Retrieved October 3, 2021.

[894] Aleksandra Mojsilovic: Introducing AI Explainability 360. Article published August 8 2019, available at https://www.ibm.com/blogs/research/2019/08/ai-explainability-360/#:~:text=AI%20Explainability%20360%20complements%20the%20ground-breaking%20algorithms%20developed,were%20built%20or%20in%20which%20environment%20they%20run.

[895] Source: https://www.iso.org/standard/61498.html. Retrieved October 3, 2021.

secondary use of data and data breaches.[896] Even though some GDPR requirements are not covered, ISO controls[897] can be a starting point for achieving the necessary technical and operational requirements to reduce risks of data processing activities as those standards deals with e.g. risk assessment, privacy by design and supplier relationships. Moreover, ISO intends to establish a framework for Artificial Intelligence: the joint technical committee of the International Organization for Standardization and the International Electro-technical Commission (IEC) are working on standards to ensure trustworthiness of AI technology.[898] The first meeting of the ISO AI committee was held in early 2018, and the following ISO standards address AI: ISO/IEC JTC 1/SC 41 (Internet of Things),[899] and ISO/IEC JTC 1/SC 38 (Cloud Computing and distributed platforms)[900] and ISO/IEC JTC 1/SC 37 (Biometrics).[901] Based on the Executive Order 13859, the American National Institute of Standards and Commerce (NIST) issued a "*plan for federal engagement in developing technical standards and related tools" in 2019 to develop technical standards for AI with the aim to encourage reliable, robust, and trustworthy AI technology*.[902] In 2021, NIST issued a report on trust and Artificial Intelligence in which they conclude that trust will be necessary of any human-AI collaboration: "*if the AI system has a high level of technical trustworthiness, and the values of the trustworthiness characteristics are perceived to be good enough for the context of use, and especially the risk inherent in that context, then the likelihood of AI user trust increases*."[903]

F. Guidance, recommendations and initiatives

I. Guidance and recommendations at international level[904]

1. OECD AI principles

The 2019 OECD principles on Artificial Intelligence[905] aim to promote AI that respects democratic values, human rights, the rule of law as well as transparency and diversity and are the first

[896] Michael Fekete: ISO/IEC 27018 – new code of practice promotes privacy protection in the cloud, 2014. Article published October 20 2014, available at https://www.lexology.com/library/detail.aspx?g=ff6d5e13-1f3e-4539-887e-20dfc12eb8fd. Retrieved October 3, 2021.
[897] Background on ISO standards can be found at https://www.iso.org/home.html. Retrieved October 3, 2021.
[898] Source: https://www.iso.org/standard/74438.html. Retrieved October 3, 2021.
[899] Source: https://www.iso.org/committee/6483279.html. Retrieved October 3, 2021.
[900] Source: https://www.iso.org/committee/601355.html. Retrieved October 3, 2021.
[901] Source: https://www.iso.org/committee/313770.html. Retrieved October 3, 2021.
[902] NIST: U.S. Leadership in AI - A plan for federal engagement in developing technical standards and related tools prepared in response to, draft submitted on August 9 2020, available at https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf. Retrieved October 3, 2021.
[903] National Institute of Standards and Commerce: Trust and Artificial Intelligence. Report published March 2021 and is available at https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8332-draft.pdf. Retrieved October 3, 2021.
[904] Given the fact that there is an intersection between, for instance, civil society and multistakeholder initiatives, it is not always possible to clearly distinguish and properly group various AI recommendations and guidelines.

intergovernmental standard that has been adopted by 42 countries. OECD’s principles have been developed by a 50+ member expert group on AI who named the following five complementary value-based AI principles:[906]

I. *“**AI should benefit people and the planet by driving inclusive growth, sustainable development and well-being***[907]*.*

II. ***AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society****.*

III. ***There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them****.*

IV. ***AI systems must function in a robust, secure and safe way throughout their life cycles*** *and* ***potential risks should be continually assessed and managed****.*

V. ***Organizations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles****”.*

Consistent with these value-based principles, the OECD also adopted recommendations[908] for national (government) AI policy priorities which shall also be read in the context of OECD’s Privacy Principles:

I. *“**Facilitate public and private investment in research & development to spur innovation in trustworthy AI****.*

II. ***Foster accessible AI ecosystems with digital infrastructure and technologies and mechanisms to share data and knowledge****.*

III. ***Ensure a policy environment that will open the way to deployment of trustworthy AI systems****.*

IV. ***Empower people with the skills for AI and support workers for a fair transition****.*

V. ***Co-operate across borders and sectors to progress on responsible stewardship of trustworthy AI****.”*

[905] Source: http://www.oecd.org/going-digital/ai/principles/. Retrieved October 3, 2021.

[906] Source: https://www.oecd.org/going-digital/ai/principles/#:~:text=The%20Recommendation%20identifies%20five%20complementary%20values-based%20principles%20for,proper%20functioning%20in%20line%20with%20the%20above%20principles. Retrieved October 3, 2021.

[907] Bold Italic means emphasis added.

[908] Details on OECD’s recommendations available at http://www.oecd.org/going-digital/ai/oecd-moves-forward-on-developing-guidelines-for-artificial-intelligence.htm. Retrieved October 3, 2021.

2. G20, G7 and World Economic Forum recommendations on AI

In 2019, the G20 formulated human-centered AI principles[909] which are inspired by OECD's AI principles. These guidelines stress that AI shall be fair, transparent and accountable and that it shall respect privacy, equality, diversity as well as internationally recognized labor rights. The latter is important since the use of AI is believed to create a new virtual workforce.[910] The G20 statement thus also addresses complementary digital economy issues. In addition, Think20, a task force of the G20 research and policy advice network that is working on the future of work and education in the digital age, focuses on AI-based learning technologies to overcome current educational challenges.[911] G20 AI principles are split into two sections, the first section deals with principles for responsible stewardship of trustworthy AI and focuses on:

i. *"**Inclusive growth, sustainable development and well-being**,*
ii. ***Human-centered values and fairness**,*
iii. ***Transparency and explainability**,*
iv. ***Robustness, security and safety**,*
v. ***Accountability**."*

The second section is about national policies and international co-operation for trustworthy AI and stresses the need for international co-operation, investing in AI research, fostering a digital ecosystem for AI, shaping a policy environment for AI, and building human capacity and preparing for labor market transformation.[912] In 2018, G7 leaders issued the Charlevoix Common Vision for the Future of Artificial Intelligence,[913] and the World Economic Forum published a White Paper on AI[914] in which they propose four central principles: fairness and active inclusion as well as the right to understanding and the right to redress. The World Economic Forum moreover suggests that companies take the following steps to prevent discriminatory outcomes: being transparent about efforts to identify,

[909] Source: https://www.mofa.go.jp/files/000486596.pdf. Retrieved October 3, 2021.

[910] Dennis Späth: Artificial Intelligence is transforming the workforce as we know it. Article published March 18, 2019, available at https://workplaceinsight.net/artificial-intelligence-is-transforming-the-workforce-as-we-know-it/. Retrieved October 3, 2021.

[911] Samed Olukoya: Think20 Says Artificial Intelligence (AI) Based Learning Technologies Can Overcome Current Educational Challenges. Article published August 25 2020, available at https://investorsking.com/2020/08/25/think20-says-artificial-intelligence-ai-based-learning-technologies-can-overcome-current-educational-hallenges/. Retrieved October 3, 2021.

[912] Source: https://www.g20-insights.org/wp-content/uploads/2019/07/G20-Japan-AI-Principles.pdf. Retrieved October 3, 2021.

[913] Source: https://www.mofa.go.jp/files/000373837.pdf. Retrieved October 3, 2021.

[914] The World Economic Forum: How to Prevent Discriminatory Outcomes in Machine Learning. The document is available at http://www3.weforum.org/docs/WEF_40065_White_Paper_How_to_Prevent_Discriminatory_Outcomes_in_Machine_Learning.pdf. Retrieved October 3, 2021.

prevent, and mitigate human rights risks; identifying human rights risks linked to business operations, and taking effective action to prevent and mitigate risks.

3. United Nations

a) IWGDPT's Working Paper and ITU's AI for good initiative

In 2018, the International Working Group on Data Protection in Telecommunications (IWGDPT) issued a working paper[915] which identified the following main issues with regard to data protection: lack of transparency and intelligibility, erosion of consent and purpose limitation, the risk of re-identification as well as risk of detecting sensitive information. Their key recommendations are Fairness and respect of fundamental human right, accountability, privacy and ethics by design and non-discrimination. Together with various other UN organizations and the Association for Computing Machinery, the International Telecommunication Union (ITU)[916] organized the AI for Good Global Summit, the leading United Nations platform to foster the dialogue on beneficial use of AI.[917] In accordance with the United Nations Sustainable Development Goals (SDG), this initiative is focusing on using AI for sustainable development. The summit established various focus groups, for example AI for Health, Machine Learning for Future Networks (5G), Environmental Efficiency for AI and other Emerging Technologies, AI for Autonomous and Assisted Driving and the AI for Good Repository; the ITU moreover intends to draft technical reports and specifications for machine learning.[918] AI for Good focuses on the following key areas: accountability, fairness, transparency, explicability, robustness, safety and security as well as inclusive growth, sustainable development and well-being based on human-centered values.

b) UNESCO: Recommendation on the Ethics of Artificial Intelligence, Beijing declaration on Artificial Intelligence and Education

In 2020, the United Nations Educational, Scientific and Cultural Organization (UNESCO) set up an international expert group composed of "*the world's leading experts on the social, economic and cultural challenges of Artificial Intelligence to draft internationally applicable recommendations on*

[915] The text of IWGDPT's working paper is available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2018/2018-IWGDPT-Working_Paper_Artificial_Intelligence.pdf. Retrieved October 3, 2021.
[916] ITU is UN's agency for information and communication technologies.
[917] Background information on the summit series is available on ITU's website at https://www.itu.int/en/ITU-T/AI/2018/Pages/default.aspx. Retrieved October 3, 2021.
[918] Corresponding information and documents can be found at https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx. Retrieved October 3, 2021.

ethical issues raised by the development and use of AI".[919] With the goal to develop the first global normative instrument on this key issue,[920] UNESCO's Ad Hoc Expert Group (AHEG)[921] provided a recommendation[922] on the ethics of Artificial Intelligence in which they stress the importance of human dignity, privacy, fairness, transparency, safety, accountability, human oversight as well as sustainability, diversity and inclusiveness, and the need to address social, economic, employment and environmental consequences of AI. UNESCO identified the following areas of policy action in the framework of their recommendation: governance, ethical stewardship, impact assessments, capacity building and international cooperation for AI Ethics.[923] UNESCO stresses that AI has the potential to address some of the biggest challenges in the field of education by allowing for innovative teaching and learning practices. Against this background, UNESCO published the Beijing Consensus on Artificial Intelligence and Education.[924] In addition, UNESCO published an AI Decision Makers' Toolkit[925] to help address certain issues that arise from AI's role in the context of education, including gender equality as well as challenges in the area of online disinformation and hate speech.

c) UNICEF: AI for Children

As part of their Artificial Intelligence for Children Policy project,[926] the United Nations Children's Fund (UNICEF) developed a policy guidance[927] on *"how to promote children's development in AI strategies and practices (...) to bring a balanced perspective to the policy table with clear, usable principles for implementing AI that supports child rights*" as a response to the fact that, despite the

[919] Source: https://en.unesco.org/news/unesco-appoints-international-expert-group-draft-global-recommendation-ethics-ai. Retrieved October 3, 2021.

[920] Background information is available at UNESCO's homepage. The corresponding blog entry "UNESCO appoints international expert group to draft global recommendation on the ethics of AI" has been published on March 3 2020 and is available at https://en.unesco.org/news/unesco-appoints-international-expert-group-draft-global-recommendation-ethics-ai. Retrieved October 3, 2021.

[921] Source: https://en.unesco.org/news/unesco-appoints-international-expert-group-draft-global-recommendation-ethics-ai. Retrieved October 3, 2021.

[922] AHEG's draft text of a recommendation on the ethics of artificial intelligence was published May 15 2020 and is available at https://ircai.org/wp-content/uploads/2020/07/Recommendation_first_draft_ENG.pdf. Retrieved October 3, 2021.

[923] Source: https://ircai.org/wp-content/uploads/2020/07/Recommendation_first_draft_ENG.pdf. Retrieved October 3, 2021.

[924] The corresponding press release was published June 25, 2019 and is available at UNESCO's website: https://en.unesco.org/news/first-ever-consensus-artificial-intelligence-and-education-published-unesco. The text of the Beijing Consensus on Artificial Intelligence and Education is available at https://unesdoc.unesco.org/ark:/48223/pf0000368303. Retrieved October 3, 2021.

[925] Background information on UNESCO's Decision Maker's Toolkit for AI is available at UNESCO's website: https://en.unesco.org/artificial-intelligence/decision-makers-toolkit. Retrieved October 3, 2021.

[926] Background information on UNICEF's project is available at https://www.unicef.org/globalinsight/featured-projects/ai-children. Retrieved October 3, 2021.

[927] UNICEF's Policy Guidance on AI for children has been published in September 2020 and is available at https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf. Retrieved October 3, 2021.

growing interest in and application of AI, little attention has so far been paid to how it affects children and their rights.[928]

d) United Nation's Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression

The report of the United Nation's Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression[929] dealt with implications of AI technologies for human rights and underlined the importance of freedom of opinion and expression, individual autonomy, the right to privacy and to effective remedy, the obligation of non-discrimination and the need for human rights impact assessments and audits.

e) UNICRI's center on AI and Robotics

In 2015, UNICRI, the United Nations Interregional Crime and Justice Research Institute established a center on AI and robotics to "*help focus expertise on Artificial Intelligence (AI) throughout the UN in a single agency.*"[930] The center's focus is on awareness-raising, exchange of information education, and harmonization of relevant stakeholders.

4. UNI Global Union top 10 Principles for Ethical Artificial Intelligence

UNI Global Union (UNI) is a global union federation for national and regional trade unions representing 650 trade unions in the fastest growing sectors in the world, skills and services.[931] UNI is concerned with protecting workers' rights and since Artificial Intelligence may change the "*Future World of Work*",[932] UNI joined the multi-stakeholder Partnership on AI (PAI)[933] and developed principles for ethical AI in order to "*put people and planet first*"[934] which demands AI to meet the following criteria: AI systems shall be transparent, equipped with an ethical black box, operate in a genderless and unbiased manner, adopt a human-in-command approach, serve people and planet, and ensure fundamental freedoms and rights. Finally, UNI calls for a ban on the attribution of responsibility to robots and the AI arms race.

[928] Source: https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children. Retrieved October 3, 2021.
[929] Source: https://freedex.org/wp-content/blogs.dir/2015/files/2018/10/AI-and-FOE-GA.pdf. Retrieved October 3, 2021.
[930] Source: https://futureoflife.org/ai-policy-united-nations/?cn-reloaded=1. Retrieved October 3, 2021.
[931] Source: https://uniglobalunion.org/. Retrieved October 3, 2021.
[932] UNI's website can be accessed at http://www.thefutureworldofwork.org. Retrieved October 3, 2021.
[933] Source: https://www.partnershiponai.org/. Retrieved October 3, 2021.
[934] Source: http://www.thefutureworldofwork.org/media/35420/uni_ethical_ai.pdf. Retrieved October 3, 2021.

III. Guidance and recommendations at European level

1. Ethics Guidelines for trustworthy AI

In 2018, 25 European countries signed a declaration of cooperation on Artificial Intelligence in which they declare their willingness to join forces and engage in a European approach to the topic.[935] In 2019, the High-Level expert group on Artificial Intelligence presented ethics guidelines for trustworthy Artificial Intelligence.[936] The High-Level Expert Group on Artificial Intelligence (HLEG) is an independent group of expert that was set up by the European Commission as part of the AI strategy in 2018.[937] On the one hand, they recognize that AI is a key driver for economic growth through the digitalization of industry; on the other hand, according to these guidelines, AI can only be considered trustworthy if it respects applicable laws and regulations and if it respects certain ethical principles and values. The guidelines explain the following conditions that AI systems must meet to be considered trustworthy:[938]

i. *"**Human agency and oversight**:[939] AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper oversight mechanisms need to be ensured, which can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches*

ii. ***Technical Robustness and safety**: AI systems need to be resilient and secure. They need to be safe, ensuring a fall-back plan in case something goes wrong, as well as being accurate, reliable and reproducible. That is the only way to ensure that also unintentional harm can be minimized and prevented.*

iii. ***Privacy and data governance**: besides ensuring full respect for privacy and data protection, adequate data governance mechanisms must also be ensured, taking into account the quality and integrity of the data, and ensuring legitimized access to data.*

iv. ***Transparency**: the data, system and AI business models should be transparent. Traceability mechanisms can help achieving this. Moreover, AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned. Humans need to be aware that they are interacting with an AI system and must be informed of the system's capabilities and limitations.*

[935] European Commission: EU Member States sign up to cooperate on Artificial Intelligence, news entry published April 10 2018, available at https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence. Retrieved October 3, 2021.

[936] European Commission: Ethics guidelines for trustworthy AI. Guideline published April 18 2019, available at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Retrieved October 3, 2021.

[937] Source: https://ec.europa.eu/futurium/en/ai-alliance-consultation. Retrieved October 3, 2021.

[938] The text of the guidelines is available in various languages at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Retrieved October 3, 2021.

[939] Bold means emphasis added.

v. ***Diversity, non-discrimination and fairness**: Unfair bias must be avoided, as it could have multiple negative implications, from the marginalization of vulnerable groups to the exacerbation of prejudice and discrimination. Fostering diversity, AI systems should be accessible to all, regardless of any disability, and involve relevant stakeholders throughout their entire life circle.*

vi. ***Societal and environmental well-being**: AI systems should benefit all human beings, including future generations. It must hence be ensured that they are sustainable and environmentally friendly. Moreover, they should take into account the environment, including other living beings, and their social and societal impact should be carefully considered.*

vii. ***Accountability**: Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes. Auditability, which enables the assessment of algorithms, data and design processes plays a key role therein, especially in critical applications. Moreover, adequate an accessible redress should be ensured."*

In order to assess whether or not an AI system that is being developed, deployed, procured or used, complies with HLEG's requirements of Trustworthy AI, the High-Level Expert Group on Artificial Intelligence furthermore issued an Assessment List for Trustworthy AI (ALTAI)[940] which aims to provide a basic self-evaluation tool for trustworthy AI.

2. European Ethical Charter on the Use of AI in Judicial Systems (CEPEJ)

Certain countries have taken steps to introduce algorithmic decisions in the area of justice or policing[941] for purposes like the prevention of offences, evaluation of the risk of recidivism and the assessment of the level of danger by using AI to ensure a better predictability of crime or decisions. It is therefore necessary to think about a corresponding legal framework. Consequently, the European Commission for the Efficiency of Justice (CEPEJ) came up with an Ethical Charter on the Use of AI in Judicial Systems and their Environment in 2018.[942] This first charter on AI in judicial systems aims at improving the quality and efficiency of the European judicial systems and at compliance with fundamental rights guaranteed in the European Convention on Human Rights and the Council of

[940] ALTAI is a self-assessment tool to help assess whether or not an AI system that is being developed, deployed, procured or used, complies with HLEG's requirements for Trustworthy AI. Background information on ALTAI can be found at https://altai.insight-centre.org/. Retrieved October 3, 2021.

[941] Orla Lynskey: Criminal justice profiling and EU data protection law: precarious protection from predictive policing, International Journal of Law in Context, vol. 15, issue 2, pp. 162-176.

[942] Source: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c. Retrieved October 15, 2021.

Europe Convention on the Protection of Personal Data.[943] CEPEJ names five basic principles which have to be obeyed when AI is used in the judicial area:[944]

i. *"**Principle of respect for fundamental rights**:[945] ensure that the design and implementation of artificial intelligence tools and services are compatible with fundamental rights.*
ii. ***Principle of non-discrimination**: Specifically prevent the development or intensification of any discrimination between individuals or groups of individuals.*
iii. ***Principle of quality and security**: With regard to the processing of judicial decisions and data, use certified sources and intangible data with models conceived in a multi-disciplinary manner, in a secure technological environment.*
iv. ***Principle of transparency, impartiality and fairness**: Make data processing methods accessible and understandable, authorize external audits.*
v. ***Principle "under user control":** Preclude a prescriptive approach and ensure that users are informed actors and in control of their choice."*

3. European Commission: White Paper on Artificial Intelligence

In early 2020, the European Commission presented its strategy for data and Artificial Intelligence. The EC altogether delivered four papers: a white paper on Artificial Intelligence,[946] a report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics,[947] as well as two communications, one on Europe's digital future[948] and one on the European strategy for data.[949] Despite the fact that EC's statements do not constitute a legal regime for AI, they nonetheless provide guidance on the European Commission's priorities and potential next steps. They furthermore show that the Commission aims at positioning the EU as a digital leader in terms of both, trustworthy AI and the wider data economy.[950] With regard to the future regulation of AI, the EC wants to pursue a uniform approach to avoid divergent member state requirements which may lead barriers within EU's

[943] Mie Oehlenschlager: First European Ethical Charter on AI in Judicial Systems. Article published on January 16, 2019, available at https://dataethics.eu/first-european-ethical-charter-on-ai-in-judicial-systems/. Retrieved October 15, 2021.
[944] Source: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c. Retrieved October 15, 2021.
[945] Bold means emphasis added.
[946] Source: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Retrieved October 15, 2021.
[947] Source: https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf. Retrieved October 15, 2021.
[948] Source: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf. Retrieved October 15, 2021.
[949] Source: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.
[950] Lisa Peets, Marty Hansen, Sam Jungyun Choi, Nicholas Shepherd, Anna Oberschelp de Meneses: European Commission Presents Strategies for Data and AI. Article published on February 20 2020, available at https://www.covingtondigitalhealth.com/2020/02/european-commissions-white-paper-on-artificial-intelligence-part-2-of-4/. Retrieved October 15, 2021.

single market.[951] The EC's white paper is acknowledging that AI may involve a variety of risks, for example for fundamental rights, privacy protection and non-discrimination as well as risks for safety and the effective functioning of the liability regime,[952] and that is why the EC wants high-risk systems to meet security, privacy and fairness requirements before they go live by identifying high-risk sectors and applications in advance. The European Commission consequently acknowledges the importance of the seven key requirements that have been identified in HLEG's guidelines:[953]

i. *"**Human agency and oversight**.[954] The principle of human agency is that a human should always be in ultimate control of an AI system. For example, an AI vehicle would not start without a human inserting a key and the vehicle can be manually overridden at any point if it malfunctions. The autonomous vehicle sector where the handover of control from human to machine and back again is one of main areas of contention and rife with practical problems,*

ii. ***Technical robustness and safety**: The results from AI systems should be reproducible, predictable and accurate and AI systems should also be protected against cyberattacks,*

iii. ***Privacy and data governance**: AI systems typically 'learn' from enormous sets of data from which they deduce relationships between the variables in such data. The data may be personal, and AI may be able to infer gender, sexual orientation, race, political and religious views. The sensitivity of this data is obvious and so it is incumbent on developers to ensure that AI systems are do not misuse this data or leak this information,*

iv. ***Transparency**: The inner workings of a AI system should be clearly explainable to all parties so that everyone (even those of a non-technical background) can understand the basic principles to which they work,*

v. ***Diversity non-discrimination and fairness**: An AI system is only as good as the data it uses to learn. If the data fed to the system is inherently biased or not representative then the AI system will make biased and discriminatory decisions. It is therefore necessary to have controls on the quality of the data used,*

vi. ***Societal and environmental wellbeing**: AI systems should be used to benefit society as a whole rather than individuals. In addition, sustainability and ecological impact should be taken into account when developing AI systems, and*

vii. ***Accountability**: If an AI system malfunctions and potentially causes harm then it should be possible to trace the manufacturers of the AI system to bring them to justice. This is a*

[951] Mark MacCarthy, Kenneth Propp: The EU's White Paper on AI: A Thoughtful and Balanced Way Forward. Article published March 5 2020, available at https://www.lawfareblog.com/eus-white-paper-ai-thoughtful-and-balanced-way-forward. Retrieved October 15, 2021.

[952] Source: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Retrieved October 15, 2021.

[953] Source: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Retrieved October 15, 2021.

[954] Bold means emphasis added.

> *difficult task because there are many parties involved in the creation of AI systems from the beginning to the end of the supply chain. AI systems should be traceable and should be audited at each stage of the supply chain in order to ensure their compliance."*

The EC moreover elaborates on specific requirements for certain AI applications such as "*those used for purposes of (remote) biometric identification*", however, the latter has been criticized, because the requirements are weaker than the ones suggested in a previous version of the paper which suggested a moratorium on facial recognition in public spaces for five years.[955] The EC was also criticized for the fact that the paper's AI guidelines only address high-risk technologies (e.g. biometrics, surveillance) or certain industries (e.g. energy) but not consumer-relevant (e.g. advertising) technology.[956]

4. HUMANE AI Net

Together with a network of more than 50 academic and industrial partners, the European Commission launched HUMANE AI Net to facilitate "*a European brand of trustworthy, ethical AI that enhances Human capabilities and empowers citizens and society to effectively deal with the challenges of an interconnected globalized world."*[957] The initiative originated in Germany at the German Research Center for Artificial Intelligence[958] and engages in numerous micro projects such as Defining AI for regulatory and policy purposes, Algorithmic Bias, Strategies for Adaptive User Interfaces or Ethical Chat-Bots and published a series of reports on reports on human-centered AI, including a research roadmap[959] and policy recommendations.[960] HUMANE AI Net's research agenda for human-centered AI is built on 5 pillars: societal awareness; legal and ethical bases for responsible AI; human-AI collaboration and interaction; multimodal perception and modeling as well as human-in-the-loop machine learning, reasoning, and planning.[961]

[955] MIT Technology Review, blog-entry published February 19 2020, available at https://www.technologyreview.com/2020/02/19/876455/european-union-artificial-intelligence-regulation-facial-recognition-privacy/. Retrieved October 15, 2021.

[956] Mark MacCarthy, Kenneth Propp: The EU's White Paper on AI: A Thoughtful and Balanced Way Forward. Article published March 5 2020, available at https://www.lawfareblog.com/eus-white-paper-ai-thoughtful-and-balanced-way-forward. Retrieved October 15, 2021.

[957] Background information on the HUMANE AI Net can be found at https://www.humane-ai.eu/. Retrieved October 15, 2021.

[958] Background information on the German Research Center for Artificial Intelligence is available at their homepage: https://www.dfki.de/en/web/. Retrieved October 15, 2021.

[959] Source: https://www.humane-ai.eu/wp-content/uploads/2020/01/D4.1-v3.pdf. Retrieved October 15, 2021.

[960] Source: https://www.humane-ai.eu/wp-content/uploads/2019/11/D21-HumaneAI-Concept.pdf. Retrieved October 15, 2021.

[961] Detailed information on HUMANE AI Net's research agenda is available at https://www.humane-ai.eu/research-roadmap/. Retrieved October 15, 2021.

5. Council of Europe Commissioner for Human Rights recommendation

In 2019, the Council of Europe's Commissioner for Human Rights issued a recommendation[962] which explains that "*finding the right balance between technological development and human rights protection is an urgent matter*" given the fact that AI-driven applications are nowadays part of everyday life. The document is aimed at Council of Europe (COE) member states; however, the findings concern anyone dealing with the design, development or implementation of AI. The document[963] names the following ten steps to protect human rights and unbox Artificial Intelligence:

i. *"**Human rights impact assessment**,*
ii. ***Public consultation**,*
iii. ***Obligation of member states to facilitate the implementation of human rights standards in the private sector**,*
iv. ***Information and transparency**,*
v. ***Independent oversight**,*
vi. ***Non-discrimination and equality**,*
vii. ***Data protection and privacy**,*
viii. ***Freedom of expression, assembly and association**, and the **right to work***
ix. ***Remedies**,*
x. ***Promotion of AI-literacy**."*

6. Council of Europe Recommendations on Human Right Impacts of Algorithmic Systems

The Council of Europe, the leading international organization for the protection of human rights as set forth in the European Convention on Human Rights[964] issued guidelines on how COE member states – currently 47 out of which 27 are EU member states – should legislate to make sure that human rights are addressed when Artificial Intelligence is used.[965] COE's recommendations are similar to HLEG's Ethics Guidelines for Trustworthy AI, but the interesting thing about COE's recommendations is that two sets of guidelines have been issued, one for the private sector which may serve for orientation purposes in the sense of best practices, and one for the public sector that could serve as guidance for

[962] Source: https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64. Retrieved October 15, 2021.
[963] The document includes a checklist with "Dos" and "Don'ts" with actions for each key area to serve as guidance when it comes to operationalizing recommendations.
[964] Further background information on the Council of Europe can be found at COE's homepage https://www.coe.int/en/web/about-us. Retrieved October 15, 2021.
[965] Source: https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154. Retrieved October 15, 2021.

future legislation.[966] COE's guidelines on addressing the human rights impacts of algorithmic systems name the following general principles (obligations) for states with respect to the protection and promotion of human rights and fundamental freedoms in the context of algorithmic systems:[967]

i. *"**Research, innovation, public awareness**[968] (including rights-promoting technology, human-centric and sustainable innovation as well as independent research),*
ii. ***Precautionary measures** (including impact assessments, staff management and interaction of systems / integrations),*
iii. ***Legislation** (including ongoing review, democratic participation and awareness, institutional framework),*
iv. ***Transparency, accountability and effective remedies** (including contestability, oversight),*
v. ***Data management** (including informational self-determination, infrastructure),*
vi. ***Analysis and modelling** (including safeguards, evaluation, testing)."*

Private sector actors shall consider with the following general principles in order to comply with human rights and fundamental freedoms in the context of algorithmic systems:

i. ***"Transparency, accountability and effective remedies**,*
ii. ***Appropriate privacy settings and consent rules**,*
iii. ***Responsibility to respect human rights**,*
iv. ***Contestability and effective remedies**,*
v. ***Avoidance of discrimination**,*
vi. ***Data quality and security**."*

7. European Parliament's resolutions and initiatives

a) Resolution on Civil Law Rules on Robotics

The European Parliament's Legal Affairs Committee dealt with issues surrounding the liability in robotics and published a study to evaluate and analyze a number of future European civil law rules in robotics[969] from a legal and ethical perspective. EP furthermore issued a resolution on Civil Law Rules

[966] Background information on the Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems that was adopted April 8 2020 is available at https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154. Retrieved October 15, 2021.
[967] Source: https://rm.coe.int/09000016809e1154. Retrieved October 15, 2021.
[968] Bold means emphasis added.
[969] European Civil Law Rules on Robotics, published in 2016, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf. Retrieved October 15, 2021.

on Robotics[970] which deals, amongst other things, with protecting humans against the risk of harm and manipulation by robots and discusses the establishment of a mandatory insurance scheme for specific categories of robots as well as the creation of a general fund for all intelligent autonomous robots or an individual fund for each category and the establishment of a specific legal status for robots, so that autonomous robots are responsible for any damage they cause.[971] The European Parliament suggests that robots should not be given a legal personality, even if robots interact with third parties independently.[972] The European Parliament continued its work and issued three further resolutions:

b) Resolution on a civil liability regime for AI

The European Parliament issued a resolution on a civil AI liability to address key issues like insurances, operator liability and different liability rules for different risks: the European Parliament suggested that those operating high-risk AI should be strictly liable for any resulting damage, material and immaterial harm.[973] The EP called for a harmonized legal framework for civil liability claims to prevent potential misuses of AI-systems[974] and the European Parliament also dealt with the issue of Artificial intelligence and civil law liability rules for drones.[975] Difficulties arise from the fact that the existing product liability has not been amended to reflect specific implications AI may involve: the European Commission has determined that the Directive, which has been in place for over 30 years, requires further work, but is still fit for purpose.[976] However, it seems that time has come to acknowledge that certain types of AI shall be subject to product safety as well as cyber-security rules to properly address imminent risk and potential damage resulting from interaction with humans.[977]

[970] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL) available at https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html. Retrieved October 15, 2021.

[971] Background information is provided by omitech robot in their blog post "Civil law rules on Robotics: the resolution of the European Union" which is available at https://robot.omitech.it/en/civil-law-rules-on-robotics-the-resolution-of-the-european-union/. Retrieved October 15, 2021.

[972] European Parliament: European Civil Law Rules on Robotics (2017), page 16, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf. Retrieved October 15, 2021.

[973] The European Parliament's resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL) is available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html. Retrieved October 15, 2021.

[974] European Parliament Research Service – blog entry published November 23 2020 by "Ask EP": What is the European Parliament's position on artificial intelligence? The blog post is available at https://epthinktank.eu/2020/11/23/what-is-the-european-parliaments-position-on-artificial-intelligence/.

[975] Source: https://op.europa.eu/en/publication-detail/-/publication/b4b77a1e-1554-11e9-81b4-01aa75ed71a1/language-en/format-PDF/source-search. Retrieved October 15, 2021.

[976] Report on on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) issued on May 7, 2018, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1525769201372&uri=COM:2018:246:FIN. Retrieved October 15, 2021.

[977] For example, self-driving car fatalities: 'Wired' reported about the latest Tesla car crash on May 16, 2019: https://www.wired.com/story/teslas-latest-autopilot-death-looks-like-prior-crash/. Retrieved October 15, 2021.

c) Resolution on intellectual property rights

The European Parliament moreover published a resolution on intellectual property rights:[978] the EP highlighted the benefits of AI development, and given key importance of these rights, the EP stressed the need for a common AI legislation to avoid massive litigation and called on the Commission to carry out an impact assessment regarding the protection of intellectual property rights in the context of AI and related technologies. Furthermore, the European Parliament once more underlined its position that robots or AI technologies should not have legal personality and that only humans have the ownership of intellectual property rights.

d) Resolution on the ethical aspects of Artificial Intelligence

The European Parliament also issued a resolution on the ethical aspects of AI and provided recommendations about the ethics needed in the framework of Artificial Intelligence:[979] the EP stressed that AI shall be tailored to human needs, values-based and built on safety, transparency as well as accountability and tailored to human needs and shall provide for privacy, sustainability, social responsibility as well as non-discrimination and workers' rights so that AI is always at the service of humans.

e) Special Committee on Artificial Intelligence in the digital age

Last, but not least, the EP established a special committee on Artificial Intelligence in 2020 called AIDA with the goal of setting out a long-term EU roadmap on AI to "*study the impact and challenges of rolling out AI, identify common EU-wide objectives, and propose recommendations on the best ways forward.*"[980] AIDA's 12-month mandate will pursue a horizontal approach, take third-country approaches to AI into consideration, organize stakeholder workshops and summarize their findings and recommendations in a final report.

[978] The European Parliament's resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI) is available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.html. Retrieved October 15, 2021.

[979] The European Parliament's resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL) is available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html#:~:text=European%20Parliament%20resolution%20of%2020%20October%202020%20with,artificial%20intelligence%2C%20robotics%20and%20related%20technologies%20%282020%2F2012%20%28INL%29%29. Retrieved October 15, 2021.

[980] Background information on the initiative can be found at the European Parliament's website, which is available at https://www.europarl.europa.eu/committees/en/aida/about. Retrieved October 15, 2021.

III. Intergovernmental cooperation: HLEG, GPAI, AHEG and ONE AI

Apart from EU's Highlevel Expert Group on Artificial Intelligence (HLEG)[981] that delivered Ethics Guidelines for trustworthy AI and UNESCO's Ad Hoc Expert Group (AHEG)[982] that published a recommendation on the ethics of artificial intelligence, there are further intergovernmental activities that are worthwhile mentioning: OECD's Network of Experts on AI (ONE AI)[983] which launched the OECD AI Policy Observatory[984] and is working on the classification of AI to provide a framework for assessing and classifying AI systems according to their impact.[985] The Global Partnership on AI (GPAI) was founded by 15 countries from all over the globe to "*bring together engaged minds and expertise from science, industry, civil society, governments, international organizations and academia to foster international cooperation*".[986] In summary, HLEG's and AHEG's focus area is AI Ethics, ONE AI's focus is AI classification, whereas GPAI is also concerned with responsible AI and the future of work.

IV. Expert Guidelines, civil society and multistakeholder recommendations

1. Universal Guidelines for Artificial Intelligence

The Universal Guidelines for Artificial Intelligence (UGAI)[987] have been announced at the 2018 International Data Protection and Privacy Commissioners Conference. More than 150 experts and 40 non-governmental organizations representing 30 countries around the world endorsed[988] the guidelines which some consider a "landmark policy"[989] – for good reason: apart from much-repeated provisions like accountability, transparency and fairness, those guidelines follow a comprehensive approach to protect individuals' rights, and they contain more far-reaching obligations, ranging from existing (but neglected) principles like data quality and accuracy to new requirements like the prohibition of secret

[981] Source: https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai. Retrieved October 15, 2021.

[982] Source: https://en.unesco.org/news/unesco-appoints-international-expert-group-draft-global-recommendation-ethics-ai. Retrieved October 15, 2021.

[983] Source: https://oecd.ai/network-of-experts. Retrieved October 15, 2021.

[984] Source: https://oecd.ai/about/#:~:text=The%20OECD%20AI%20Policy%20Observatory%20%28OECD.AI%29%20builds%20on,basis%20for%20the%20G20%20AI%20Principles%20endorsed%20. Retrieved October 15, 2021.

[985] Source: https://oecd.ai/network-of-experts/#:~:text=The%20upcoming%20OECD%20AI%20Systems%20Classification%20Framework%20provides,and%20technologies%3B%20labour%20and%20skills%3B%20and%20international%20cooperation. Retrieved October 15, 2021.

[986] Source: https://www.gpai.ai/. Retrieved October 15, 2021.

[987] Source: https://blog.epic.org/2018/10/23/universal-guidelines-artificial-intelligence-announced-brussels/. Retrieved October 15, 2021.

[988] A list of all organizations and individuals that have endorsed the UGAI is available at https://thepublicvoice.org/AI-universal-guidelines/endorsement/. Retrieved October 15, 2021.

[989] Candace Paul: Universal Guidelines for Artificial Intelligence Announced in Brussels. Article published October 23 2018, available at https://blog.epic.org/2018/10/23/universal-guidelines-artificial-intelligence-announced-brussels/. Retrieved October 15, 2021.

profiling and national scoring, making the true operators of an AI system known and a termination obligation when an institution loses control of an AI system. The UGAI require the following:

i. *“**Right to transparency**:*[990] *all individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, the logic, and techniques that produced the outcome.*

ii. ***Right to human determination**: all individuals have the right to a final determination made by a person.*

iii. ***Identification obligation**: the institution responsible for an AI system must be made known to the public.*

iv. ***Fairness obligation**: institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions.*

v. ***Assessment and accountability obligation**: an AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system.*

vi. ***Accuracy, reliability and validity obligations**: institutions must ensure the accuracy, reliability, and validity of decisions.*

vii. ***Data quality obligation**: institutions must establish data provenance, and assure quality and relevance for the data input into algorithms.*

viii. ***Public safety obligation**: institutions must assess the public safety risks that arise from the deployment of AI systems that direct or control physical devices, and implement safety controls.*

ix. ***Cyber-security obligation**: institutions must secure AI systems against cybersecurity threats.*

x. ***Prohibition on secret profiling**: no institution shall establish or maintain a secret profiling system.*

xi. ***Prohibition on unitary scoring**: no national government shall establish or maintain a general-purpose score on its citizens or residents.*

xii. ***Termination obligation**: an institution that has established an AI system has an affirmative obligation to terminate the system if human control of the system is no longer possible”*

2. Future of Life Institute: Asilomar AI Principles

The Future of Life Institute hosted a conference in 2017 where numerous researchers and thought leaders in law, economics, ethics as well as philosophy met to discuss beneficial Artificial

[990] Bold means emphasis added.

Intelligence.[991] The following twenty-three principles, called the AI Asilomar Principles, have been developed during the meeting:

"Research Issues[992]

i. ***Research Goal***: *The goal of AI research should be to create not undirected intelligence, but beneficial intelligence.*

ii. ***Research Funding***: *Investments in AI should be accompanied by funding for research on ensuring its beneficial use, including thorny questions in computer science, economics, law, ethics, and social studies, such as:*

   - *How can we make future AI systems highly robust, so that they do what we want without malfunctioning or getting hacked?*
   - *How can we grow our prosperity through automation while maintaining people's resources and purpose?*
   - *How can we update our legal systems to be fairer and more efficient, to keep pace with AI, and to manage the risks associated with AI?*
   - *What set of values should AI be aligned with, and what legal and ethical status should it have?*

iii. ***Science-Policy Link***: *There should be constructive and healthy exchange between AI researchers and policy makers.*

iv. ***Research Culture***: *A culture of cooperation, trust, and transparency should be fostered among researchers and developers of AI.*

v. ***Race Avoidance***: *Teams developing AI systems should actively cooperate to avoid corner-cutting on safety standards.*

Ethics and Values

vi. ***Safety***: *AI systems should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible.*

vii. ***Failure Transparency***: *If an AI system causes harm, it should be possible to ascertain why.*

viii. ***Judicial Transparency***: *Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.*

[991] Source: https://futureoflife.org/ai-principles/. Retrieved October 15, 2021.

[992] Bold means emphasis added.

ix. ***Responsibility**: Designers and builders of advanced AI systems are stakeholders in the moral implications of their use, misuse, and actions, with a responsibility and opportunity to shape those implications.*

x. ***Value Alignment**: Highly autonomous AI systems should be designed so that their goals and behaviors can be assured to align with human values throughout their operation.*

xi. ***Human Values**: AI systems should be designed and operated be compatible with ideals of human dignity, rights, freedoms, and cultural diversity.*

xii. ***Personal Privacy**: People should have the right to access, manage and control the data they generate, given AI systems' power to analyze and utilize that data.*

xiii. ***Liberty and Privacy**: The application of AI to personal data must not unreasonably curtail people's real or perceived liberty.*

xiv. ***Shared Benefit**: AI technologies should benefit and empower as many people as possible.*

xv. ***Shared Prosperity**: The economic prosperity created by AI should be shared broadly, to benefit all of humanity.*

xvi. ***Human Control**: Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.*

xvii. ***Non-subversion**: The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.*

xviii. ***AI Arms Race**: An arms race in lethal autonomous weapons should be avoided.*

Longer-term Issues

xix. ***Capability Caution**: There being no consensus, we should avoid strong assumptions regarding upper limits on future AI capabilities.*

xx. ***Importance**: Advanced AI could represent a profound change in the history of life on Earth and should be planned for and managed with commensurate care and resources.*

xxi. ***Risks**: Risks posed by AI systems, especially catastrophic or existential risks, must be subject to planning and mitigation efforts commensurate with their expected impact.*

xxii. ***Recursive Self-Improvement**: AI systems designed to recursively self-improve or self-replicate in a manner that could lead to rapidly increasing quality or quantity must be subject to strict safety and control measures.*

xxiii. ***Common Good**: Super-intelligence should only be developed in the service of widely shared ethical ideals, and for the benefit of all humanity rather than one state or organization."*

3. ACM's Statement on Algorithmic Transparency and Accountability

In 2017, the Association for Computing Machinery (ACM) issued a statement on Algorithmic Transparency and Accountability[993] which included seven principles designed to be consistent with ACM's Code of Ethics[994] and to address potential harmful bias[995] the use of AI may involve:

i. *"**Awareness**:*[996] *Owners, designers, builders, users, and other stakeholders of analytic systems should be aware of the possible biases involved in their design, implementation, and use and the potential harm that biases can cause to individuals and society.*

ii. ***Access and redress**: Regulators should encourage the adoption of mechanisms that enable questioning and redress for individuals and groups that are adversely affected by algorithmically informed decisions.*

iii. ***Accountability**: Institutions should be held responsible for decisions made by the algorithms that they use, even if it is not feasible to explain in detail how the algorithms produce their results.*

iv. ***Explanation**: Systems and institutions that use algorithmic decision-making are encouraged to produce explanations regarding both the procedures followed by the algorithm and the specific decisions that are made. This is particularly important in public policy contexts.*

v. ***Data Provenance**: A description of the way in which the training data was collected should be maintained by the builders of the algorithms, accompanied by an exploration of the potential biases induced by the human or algorithmic data-gathering process. Public scrutiny of the data provides maximum opportunity for corrections. However, concerns over privacy, protecting trade secrets, or revelation of analytics that might allow malicious actors to game the system can justify restricting access to qualified and authorized individuals.*

vi. ***Auditability**: Models, algorithms, data, and decisions should be recorded so that they can be audited in cases where harm is suspected.*

vii. ***Validation and Testing**: Institutions should use rigorous methods to validate their models and document those methods and results. In particular, they should routinely perform tests to assess and determine whether the model generates discriminatory harm. Institutions are encouraged to make the results of such tests public."*

[993] Source: https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf. Retrieved October 15, 2021.

[994] Source: https://ethics.acm.org/. Retrieved October 15, 2021.

[995] Renee Dopplick: New Statement on Algorithmic Transparency and Accountability by ACM U.S. Public Policy Council. Article published January 14 2017, available at https://techpolicy.acm.org/2017/01/new-statement-on-algorithmic-transparency-and-accountability-by-acm-u-s-public-policy-council/. Retrieved October 15, 2021.

[996] Bold means emphasis added.

4. The Toronto Declaration

The so-called Toronto Declaration[997] was announced by coalition of digital and human rights groups, including e.g. Human Rights Watch and Amnesty International. The declaration was the outcome of the RightsCon conference and, unlike many other guidelines and statements that discussed ethical aspects of Artificial Intelligence, the Toronto Declaration aims at embedding basic principles of equality and non-discrimination in machine learning.[998] It named 59 topics and action points altogether that emphasizes the importance of not only transparency and accountability, but also the necessity of human oversight and the right to effective remedy and above all, the right to equality and non-discrimination which means that whenever AI is applied, risks and potential discriminatory outcomes have to be considered so that human rights are respected. Given that algorithms advance in capability and increase in use in nearly all aspects of life,[999] from employment and education to policing and criminal justice, AI and machine learning may impact a variety of human rights such as the right to privacy, the freedom of expression, participation in cultural life, the right to remedy and the right to life.[1000] The Toronto declaration therefore demands that states have the obligation to promote, protect and respect human rights and that private sector actors have a responsibility to respect human rights.

5. Montreal declaration for a responsible development of Artificial Intelligence

The Montreal Declaration was announced at the conclusion of the 2017 Forum on socially responsible development of AI held in Montreal and aims to promote public debate and "*encourage a progressive and inclusive orientation to the development of Artificial Intelligence*".[1001] The Montreal Declaration for responsible AI development has three main objectives: to provide an open forum for discussion for AI to achieve equitable, inclusive, and ecologically sustainable AI, to foster the development of an ethical framework for AI, and to provide guidance for this major digital transition for the benefit of all by applying the following basic principles:[1002]

[997] Source: https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf. Retrieved October 15, 2021.

[998] Russell Brandom: New Toronto Declaration calls on algorithms to respect human rights. Article published May 16 2018, available at https://www.theverge.com/2018/5/16/17361356/toronto-declaration-machine-learning-algorithmic-discrimination-rightscon. Retrieved October 15, 2021.

[999] Source: preamble of the Toronto Declaration which is available at https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf. Retrieved October 15, 2021.

[1000] Human Rights Watch blog entry published on their homepage on July 3 2018, available at https://www.hrw.org/news/2018/07/03/toronto-declaration-protecting-rights-equality-and-non-discrimination-machine#. Retrieved October 15, 2021.

[1001] Source: https://www.montrealdeclaration-responsibleai.com/the-declaration. Retrieved October 15, 2021.

[1002] Source: https://5dcfa4bd-f73a-4de5-94d8-c010ee777609.filesusr.com/ugd/ebc3a3_506ea08298cd4f8196635545a16b071d.pdf. Retrieved October 15, 2021.

i. ***Well-being principle**:[1003] the development and use of artificial intelligence systems (AIS) must permit the growth of the well-being of all sentient beings.*
ii. ***Respect for autonomy principle**: AIS must be developed and used while respecting people's autonomy, and with the goal of increasing people's control over their lives and their surroundings.*
iii. ***Protection of privacy and intimacy**: Privacy and intimacy must be protected from AIS intrusion and data acquisition and archiving systems (DAAS).*
iv. ***Solidarity principle**: The development of AIS must be compatible with maintaining the bonds of solidarity among people and generations.*
v. ***Democratic participation principle**: AIS must meet intelligibility, justifiability, and accessibility criteria, and must be subjected to democratic scrutiny, debate, and control.*
vi. ***Equity principle**: The development and use of AIS must contribute to the creation of a just and equitable society.*
vii. ***Diversity and inclusion principle**: The development and use of AIS must be compatible with maintaining social and cultural diversity and must not restrict the scope of lifestyle choices or personal experiences.*
viii. ***Prudence principle**: The development and use of AIS must be compatible with maintaining social and cultural diversity and must not restrict the scope of lifestyle choices or personal experiences.*
ix. ***Responsibility principle**: The development and use of AIS must not contribute to lessening the responsibility of human beings when decisions must be made.*
x. ***Sustainable development principle**: The development and use of AIS must be carried out so as to ensure a strong environmental sustainability of the planet."*

6. FAT/ML's Principles for Accountable Algorithms

Fairness, Accountability, and Transparency in Machine Learning (FAT/ML) is an initiative that brings together "*a growing community of researchers and practitioners concerned with fairness, accountability, and transparency in machine learning*".[1004] FAT/ML discusses the idea that bias might inadvertently be encoded into automated decisions if the complexity of machine learning either reduces or replaces the needed justification for AI decisions to "*the algorithm made me do it*".[1005] FAT/ML is engaged in a series of projects and organizes events that deal with various aspects that have to be obeyed when AI is applied such as machine learning and the law, algorithmic bias, explicability of AI decisions or privacy-aware data mining.[1006] FAT/ML also issued Principles for

[1003] Bold means emphasis added.
[1004] This includes representatives from Microsoft, Google and universities.
[1005] Source: FAT/ML homepage https://www.fatml.org/. Retrieved October 15, 2021.
[1006] Source: https://www.fatml.org/resources/relevant-events. Retrieved October 15, 2021.

Accountable Algorithms,[1007] and they do not simply conclude with these principles, but furthermore provide a "*Social Impact Statement for Algorithms*" which shall serve as a guiding structure and which shall be used and revisited during all phases of the development process, i.e. design stage, pre-launch and post-launch to stress that only a repeated examination of the requirements ensures adherence to these principles. The Social Impact Statement should (at least) address their corresponding questionnaire that refers to specific steps that can be taken to address the requirements outlined in their principles. For transparency purposes, they propose that the statement shall be published so that the public can voice expectations for social impact of the system. FAT/ML's Principles for Accountable Algorithms[1008] read as follows:

i. *"**Responsibility**:[1009] Make available externally visible avenues of redress for adverse individual or societal effects of an algorithmic decision system, and designate an internal role for the person who is responsible for the timely remedy of such issues.*
ii. ***Explainability**: Ensure that algorithmic decisions as well as any data driving those decisions can be explained to end-users and other stakeholders in non-technical terms.*
iii. ***Accuracy**: Identify, log, and articulate sources of error and uncertainty throughout the algorithm and its data sources so that expected and worst case implications can be understood and inform mitigation procedures.*
iv. ***Auditability**: Enable interested third parties to probe, understand, and review the behavior of the algorithm through disclosure of information that enables monitoring, checking, or criticism, including through provision of detailed documentation, technically suitable APIs, and permissive terms of use.*
v. ***Fairness**: Ensure that algorithmic decisions do not create discriminatory or unjust impacts when comparing across different demographics (e.g. race, sex, etc.)."*

7. IAF's Fair Processing Principles and Fair and Open Use Act

The Information Accountability Foundation (IAF) is a global information policy think tank that focuses on "*effective information governance systems to facilitate information-driven innovation respectful of people's fundamental right to fair processing*".[1010] Despite the fact that IAF's Fair Processing Principles[1011] have not been written to specifically address Big Data activities or Artificial Intelligence applications, the document is valuable guidance in the area of AI as it addresses key issues

[1007] The text of FAT/ML's principles are available at https://www.fatml.org/resources/principles-for-accountable-algorithms. Retrieved October 15, 2021.
[1008] Source: https://www.fatml.org/resources/principles-for-accountable-algorithms. Retrieved October 15, 2021.
[1009] Bold means emphasis added.
[1010] Source https://informationaccountability.org/. Retrieved October 15, 2021.
[1011] IAF's Fair Processing Principles have been published on January 1 2019 and are available in the publications section of IAF's website: https://informationaccountability.org/publications/. Retrieved October 15, 2021.

of innovative technology. IAF lists the following key elements needed to ensure data is processed and used in a legitimate and responsible manner:

*“**Individual Rights***

i. ***Transparency**,*
ii. ***Beneficial purposes**,*
iii. ***Access and redress**,*
iv. ***Engagement and appropriate control**.*

Accountable Data Stewardship

v. ***Assessed and mitigated impacts**,*
vi. ***Legitimate and contextual uses**,*
vii. ***Onward responsibility**,*
viii. ***Remediation**,*
ix. ***Oversight**,*
x. ***Security**.”*

The Information Accountability Foundation moreover issued the Fair and Open Use Act[1012] which is a model for privacy legislation that focuses on fair processing: IAF stresses that lessons learned from GDPR and other privacy legislation show that it is “*time to place the onus on the organization to first and foremost achieve fair processing rather than placing the burden on the consumer*.”[1013] IAF’s model legislation is based on risk assessment to capture and control potentially bad outcomes and stresses the importance of effective information governance; it wants to break the paradigm that legacy systems placed on the individual instead of organizational responsibility, consequently, IAF’s model legislation flips that order[1014] since “*the old privacy paradigm that individual control is the keystone for effective fair processing is no longer fit for its purpose*.”[1015] IAF is convinced that legislation should target risks, and not stick to (the exercise of) individual’s rights, because organizations that get

[1012] Source: https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2021/05/FAIR-and-OPEN-USE-Act-May-26-2021-1.pdf?time=1623678345. Retrieved October 15, 2021.

[1013] Background information on the Fair and Open Use Act can be found at IAF’s homepage: https://informationaccountability.org/2021/06/50-year-heritage-of-the-fair-and-open-use-act/. Retrieved October 15, 2021.

[1014] Martin Abrams: Time to break the privacy legislative paradigm – IAF Model Legislation. Article published June 3 2021, available at https://informationaccountability.org/2021/06/time-to-break-the-privacy-legislative-paradigm-iaf-model-legislation/. Retrieved October 15, 2021.

[1015] Julie Cohen: How (not) to write a Privacy Law – disrupting surveillance-based business models requires government innovation. Article published March 23 2021, available at https://knightcolumbia.org/content/how-not-to-write-a-privacy-law. Retrieved October 15, 2021.

value from data must also be responsible stewards of that data:[1016] IAF builds on the FCRA's concept of permissible purpose and requires that personal data only be processed for specific legitimate uses. IAF presents the following eleven legitimate uses:[1017] a*dvertising or marketing purposes (subject to conditions), compliance with a legal obligation, protection against unlawful activity, requested product or service, affirmative express consent, routine business processes, public safety and health, knowledge discovery, information security, as well as journalism and research."* On the one hand, this should provide for a "*forward looking risk-based model legislation*",[1018] on the other hand, it should also allow for innovation by enabling controllers to use data and knowledge they extract from information. Interestingly, IAF distinguishes between several types of data, but not in the traditional sense of sensitive and non-sensitive personal data, but depending on the source and origin of information, that is[1019] "*personal data – provided data – observed data – inferred data – third party provided data."* A similar categorization of data is contained in Microsoft's Online Services Data Processing Addendum[1020] which names the following types of data: "*provided data*" in the context of customer, support and professional services data; "*collected or obtained data*" is used for so-called diagnostic data, and "*generated or derived data,*" which refers to service generated data. This distinction is not just a new perspective on types of information or data sets, but significant insofar as it may draw the line between (joint?) controllers.[1021] As a matter of fact, such a categorization seems to be needed, because it is naïve to believe that whatever an individual provides as information, this is not the basis of subsequent processing operations, but only the starting point: in many cases "*customer provided data*" is likely to be the smallest portion of information, be it in the banking sector where screenings against various sanction lists are mandatory for compliance reasons[1022] or in e-commerce where background checks for fraud prevention purposes are based on legitimate interests: the user thinks his shopping cart is about placing an order, the vendor knows it's where the individual risk profile is created, and depending on the circumstances, not only the user's preferred payment method

[1016] Martin Abrams, Marc Groman, Barb Lawler: Fair and Open Use Act – a demonstration of accountability-based legislation. Paper published May 27 2021.

[1017] Source: https://informationaccountability.org/2021/06/50-year-heritage-of-the-fair-and-open-use-act/. Retrieved October 15, 2021.

[1018] Martin Abrams: Time to break the privacy legislative paradigm – IAF Model Legislation. Article published on June 3 2021, available at https://informationaccountability.org/2021/06/time-to-break-the-privacy-legislative-paradigm-iaf-model-legislation/. Retrieved October 15, 2021.

[1019] Martin Abrams, Marc Groman, Barb Lawler: Fair and Open Use Act – a demonstration of accountability-based legislation. Paper published May 27 2021.

[1020] Source: https://www.microsoft.com/licensing/docs/view/Online-Services-Data-Protection-Addendum-DPA#:~:text=Online%20Services%20Data%20Protection%20Addendum%20%28DPA%29%20When%20you,to%20the%20Product%20Terms%20site%20%28and%20formerly%20OST%29. Retrieved October 15, 2021.

[1021] The "Privacycompany" investigated potential privacy risks related to the use of Microsoft Windows 10 Enterprise, Office 365 ProPlus and Office Online as well as the mobile Office apps on behalf of the Dutch Ministry of Justice and Security in 2019. Background information on their DPIA and the impact assessment itself are available at their homepage: https://www.privacycompany.eu/blogpost-en/new-dpia-on-microsoft-office-and-windows-software-still-privacy-risks-remaining-long-blog. Retrieved October 15, 2021.

[1022] Ernst & Young: Effective screening controls for sanctions and AML risk management, available at https://www.ey.com/Publication/vwLUAssets/ey-effective-screening-controls-for-sanctions-and-aml-risk-management/$FILE/ey-effective-screening-controls-for-sanctions-and-aml-risk-management.pdf. Retrieved October 15, 2021.

may be rejected, but the individual as such may get sorted out.[1023] So far, the focus within privacy legislation seems to be predominantly on content-level information, i.e. data which are visible in the frontend but this information is certainly the smaller volume of data in comparison to what is going on in the backend, and it would be interesting to know what the real ratio between these types of data is.

8. IEEE Ethically Aligned Design

The IEEE is a technical professional organization dedicated to the advancement of technology.[1024] Their “*Global Initiative*” deals with ethical considerations in Artificial Intelligence and autonomous systems (A/IS). Their comprehensive first edition of an Ethically Aligned Design (EAD)[1025] is based on three pillars: universal human values, political self-determination as well as data agency and technical dependability. The latter means that A/IS shall operate reliably and safely and deliver services that can be trusted. IEEE’s initiative is interesting insofar as it does not only name principles, but also explains how to incorporate those principles in practice and how those values can be embedded into systems. IEEE identified the following general principles for autonomous and intelligent systems:

i. *“**Human Rights**:*[1026] *A/IS shall be created and operated to respect, promote, and protect internationally recognized human rights.*

ii. ***Well-being**: A/IS creators shall adopt increased human well-being as a primary success criterion for development.*

iii. ***Data Agency**: A/IS creators shall empower individuals with the ability to access and securely share their data, to maintain people’s capacity to have control over their identity.*

iv. ***Effectiveness**: A/IS creators and operators shall provide evidence of the effectiveness and fitness for purpose of A/IS.*

v. ***Transparency**: The basis of a particular A/IS decision should always be discoverable.*

vi. ***Accountability**: A/IS shall be created and operated to provide an unambiguous rationale for all decisions made.*

vii. ***Awareness of Misuse**: A/IS creators shall guard against all potential misuses and risks of A/IS in operation.*

[1023] Omer Tene: Privacy: For the Rich or for the Poor? Concurring Opinions. Article published July 26 2012, available at http://www.concurringopinions.com/archives/2012/07/privacy-for-the-rich-or-for-the-poor.html. Retrieved October 15, 2021.

[1024] Source: https://www.ieee.org/. Retrieved October 15, 2021.

[1025] IEEE: Ethically aligned design – a vision for prioritizing human well-being with autonomous and intelligent systems, available at https://engagestandards.ieee.org/rs/211-FYL-955/images/EAD1e.pdf?mkt_tok=eyJpIjoiWkRVME1UVm1OREE1TVRSbSIsInQiOiIxY3RONFl6YXh0cWxSRUpLNE9taUtwQllpaXNkYktmd3FDM2lOQ1ZNXC9YUURKV3Z4b2dJc3d3ekNDREdTd24zMHNcL0xUTEFqeFFoYTN4NWNqQUZRclY0amMyTzhXeU9VXC9yNjhneWlIeHFHV3lSMU1rRGxmeUJSTU9cL3dDeXZmN1AifQ%3D%3D. Retrieved October 15, 2021.

[1026] Bold means emphasis added.

viii. ***Competence**: A/IS creators shall specify and operators shall adhere to the knowledge and skill required for safe and effective operation.”*

Moreover, IEEE offers an Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS) to create specifications for certification and advance accountability and transparency and this way, reduce algorithmic bias. IEEE says that the “*value of this certification process in the marketplace and society at large cannot be underestimated. The proliferation of systems in the form of smart homes, companion robots, autonomous vehicles or any myriad of products and services that already exist today desperately need to easily and visually communicate to consumers and citizens whether they are deemed “safe” or “trusted” by a globally recognized body of experts providing a publicly available and transparent series of marks*.”[1027]

V. Regulator and best practice guidelines

1. International Conference of Data Protection and Privacy Commissioners

During their 40th meeting in 2018, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) issued a Declaration on Ethics and Data Protection in Artificial Intelligence[1028] in which they underline the relevance of the empowerment of individuals and the need for the establishment of common governance principles on Artificial Intelligence. They stress that AI shall be designed in a responsible manner as part of an overall ethics by design approach, and set forth the following principles that have to be obeyed when developing and applying AI:

i. *Artificial intelligence and machine learning technologies should be designed, developed and used in respect of fundamental human rights and in accordance with the **fairness principle**[1029]*

ii. ***Continued attention and vigilance**, as well as accountability, for the potential effects and consequences of, artificial intelligence systems should be ensured (...);*

iii. *Artificial intelligence **systems transparency and intelligibility** should be improved, with the objective of effective implementation (...);*

iv. *As part of an overall “ethics by design” approach, artificial intelligence systems should be **designed and developed responsibly**, by applying the principles of **privacy by default and privacy by design** (...);*

v. ***Empowerment of every individual** should be promoted, and the exercise of individuals’ rights should be encouraged, as well as the creation of opportunities for public engagement (...);*

[1027] Source: https://standards.ieee.org/industry-connections/ecpais.html. Retrieved October 15, 2021.
[1028] Source: https://www.privacyconference2018.org/system/files/2018-10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf. Retrieved October 15, 2021.
[1029] Bold means emphasis added.

vi. ***Unlawful biases or discriminations*** *that may result from the use of data in artificial intelligence should be reduced and mitigated.*

2. Guidance at authority level

Apart from the above-mentioned (legally binding) instruments which deal with data protection and data subject rights (as part of their human rights), there are also other instruments at international level which shall be considered: back in 2009, data protection authorities from more than fifty countries[1030] approved the so-called Madrid Resolution on international privacy standards.[1031] This joint proposal integrates legislation from five continents and includes various principles and obligations any privacy protection legal system must strive to achieve compliance with laws applicable on data protection matters by implementing certain standards including the need to establish authorities to guarantee and supervise the rights of citizens.[1032] The purpose of the Madrid Resolution was to "*define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data (...) and the facilitation of the international flows of personal data needed in a globalized world*".[1033] In addition, numerous opinions on various data protection topics the so-called Article 29 Working Party[1034] issued[1035] for many years proved to be particularly useful from a privacy practitioner's point of view. Further supervisory authorities discussed the topic of Artificial Intelligence and issued corresponding guidance, for example, the Hambacher Erklärung[1036] was published in Germany; the French regulator CNIL issued a report[1037] on ethical issues with algorithms and Artificial Intelligence; the Norwegian data protection authority also reported[1038] on AI, and Latin American and Spanish DPAs issued a joint statement on data processing and Artificial Intelligence.[1039]

[1030] International Conference of Data Protection and Privacy Commissioners, source: https://icdppc.org/.

[1031] Source: https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf. Retrieved October 15, 2021.

[1032] Further information can be found at http://www.privacyconference2009.org/media/notas_prensa/common/pdfs/061109_estandares_internacionales_en.pdf. Retrieved October 15, 2021.

[1033] Source: https://iapp.org/news/a/when-the-worlds-dpas-get-together-resolutions-of-the-icdppc/. Retrieved October 15, 2021.

[1034] The Article 29 Working Party ceased to exist as of May 25 2018 and has been replaced by the European Data Protection Board (EDPB):https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492. Retrieved October 15, 2021.

[1035] Their documents are available at http://ec.europa.eu/justice/article-29/documentation/index_en.htm. Retrieved October 15, 2021.

[1036] The "Hambacher Erklärung" was issued by the conference of independent data protection supervisory authorities on April 3 2019, and is available at https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf. Retrieved October 15, 2021.

[1037] CNIL's report was published May 25 2018, and is available at https://www.cnil.fr/en/algorithms-and-artificial-intelligence-cnils-report-ethical-issues. Retrieved October 15, 2021.

[1038] Datatilsynet report was published in January 2018, and is available at https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf (Retrieved October 15, 2021). Norway is the only Scandinavian country that is not a member of the European Union. Therefore, strictly

3. FTC best practice guidance

The Federal Trade Commission (FTC) that can be considered the de-facto data protection authority for the United States[1040] issued new guidance on Artificial Intelligence and algorithms to explain how businesses can promote truth, fairness and equity in their use of AI.[1041] FTC's new guidance is focusing on best practices and lessons learned, and is based on their previous work in the area of AI which included a report on big data analytics and machine learning,[1042] and a hearing on algorithms, AI and predictive analytics.[1043] In its series of best practices, FTC provides the following advice for business when using AI:

i. ***"Start with the right foundation;***

ii. ***Watch out for discriminatory outcomes;***

iii. ***Embrace transparency and independence****;*

iv. ***Don't exaggerate what your algorithm can do or whether it can deliver fair or unbiased results;***

v. ***Tell the truth about how you use data;***

vi. ***Do more good than harm;***

vii. ***Hold yourself accountable – or be ready for the FTC to do it for you.***

VI. National initiatives

Various countries all over the world started working on national strategies to develop own frameworks and strengthen their competitive position with regard to Artificial Intelligence, for example China,[1044] India[1045], the U.S.A.[1046] and France.[1047] Some countries issued ethical codes, for example the United

speaking, their recommendations cannot be considered as guidance from an EU regulator. However, their paper may still serve as de-facto guidance.

[1039] Key recommendations are summarized by Odia Kagan in an article that was published October 24 2019, available at https://dataprivacy.foxrothschild.com/2019/10/articles/general-privacy-data-security-news-developments/latin-american-and-spanish-dpas-issue-joint-statement-on-data-processing-and-ai/. Retrieved October 15, 2021.

[1040] Odia Kagan: FTC Filling Role of De Facto US Privacy Regulator. Article published March 7 2019, available at https://dataprivacy.foxrothschild.com/2019/03/articles/general-privacy-data-security-news-developments/ftc-filling-role-of-de-facto-u-s-privacy-regulator/. Retrieved October 15, 2021.

[1041] The law firm Hunton Andrews Kurth provides background information on FTC's AI guidance in their blog: FTC Reiterates AI Best Practices. Article published April 23 2021, available at https://www.huntonprivacyblog.com/2021/04/23/ftc-reiterates-ai-best-practices/. Retrieved October 15, 2021.

[1042] FTC Report: Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues. The report was issued in 2016 and is available at https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report. Retrieved October 15, 2021.

[1043] FTC Hearing #7: The Competition and Consumer Protection Issues of Algorithms, Artificial Intelligence, and Predictive Analytics. The hearing took place in the framework of a joint event with the Howard University; corresponding materials are available at https://www.ftc.gov/news-events/events-calendar/ftc-hearing-7-competition-consumer-protection-21st-century. Retrieved October 15, 2021.

[1044] Source: https://futureoflife.org/ai-policy-china/. Retrieved October 15, 2021.

[1045] Source: https://futureoflife.org/ai-policy-india/. Retrieved October 15, 2021.

Kingdom[1048] and Australia,[1049] while others already took first steps to introduce AI in the area of justice, for example Latvia.[1050] The below initiatives in Asia, the Americas, Europe and Australia shall serve as explanatory examples are not exhaustive since the legal and business landscape is very dynamic:

1. Asia

Japan's AI R&D Guidelines[1051] have not been specifically designed for the Japanese market, but as a non-regulatory and non-binding international framework. Another interesting factor to consider is that these guidelines are not only concerned with overall consequences of AI applications; they shall also serve as "*draft guidelines for developers of AI systems to serve as basis for international discussion"* (e.g. G7, OECD):[1052] these guidelines shall ensure a balance between benefits & risks of AI and help achieve a human-centered society. The committee also stressed that those guidelines shall be constantly reviewed to allow for flexibly as necessary. In addition to these R&D Guidelines Japan issued for international discussion, the country was also working on Machine Learning Quality Management Guidelines to establish a basis for quality goals for machine learning-based products and services.[1053] Japan is traditionally very strong when it comes to robotics,[1054] but competitors do not sleep: already in 2008, South Korea enacted a general law on the "*intelligent robot industry*" which authorized the government to enact a charter on intelligent robot ethics.[1055] South Korea's government released an AI strategy and wants to position the country that is home to many well-known tech

[1046] Source: https://www.ai.gov/. Retrieved October 15, 2021.

[1047] France developed an AI strategy in2018. Paper published March 2018, available at https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf. Retrieved October 15, 2021.

[1048] Source: https://dataethics.eu/the-uk-data-ethics-framework-for-the-public-sector/#:~:text=The%20UK%20government%20is%20asking%20the%20public%20sector,such%20as%20the%20General%20Data%20Protection%20Regulation%2C%20GDPR. Retrieved October 15, 2021.

[1049] The Australian government issued a statement on AI Ethics in 2019. Background information and components are available at https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework. Retrieved October 15, 2021.

[1050] On 27 September 2018, the Council of Europe European Commission for the efficiency of justice (CEPEJ) and the Courts Administration of the Latvia organized a conference on "Artificial Intelligence at the Service of the Judiciary" in Latvia; the corresponding presentation and background information is available at https://www.coe.int/en/web/cepej/justice-of-the-future-predictive-justice-and-artificial-intelligence. Retrieved October 15, 2021.

[1051] A translation of Japan's Draft AI R&D Guidelines for international discussion (2019) is available at http://www.soumu.go.jp/main_content/000507517.pdf. Retrieved October 15, 2021.

[1052] Source: http://www.oecd.org/going-digital/ai-intelligent-machines-smart-policies/conference-agenda/ai-intelligent-machines-smart-policies-hirano.pdf. Retrieved October 15, 2021.

[1053] The original document was published in June 30 2020; the Japanese language version is available at https://www.cpsec.aist.go.jp/achievements/aiqm/ and an English version is available at https://www.cpsec.aist.go.jp/achievements/aiqm/AIQM-Guideline-1.0.1.37-summary-en-1.2.pdf. Retrieved October 15, 2021.

[1054] Valerie Thomas on behalf of the Regulatory Institute: Report on Artificial Intelligence part I: the existing regulatory landscape. Article published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/. Retrieved October 15, 2021.

[1055] Intelligent Robots Development and Promotion Act (Act No. 9014) of 2008 amended in 2016 by Act No. 13744, available at http://elaw.klri.re.kr/eng_service/lawView.do?hseq=39153&lang=ENG. Retrieved October 15, 2021.

companies like Samsung, Hyundai and LG as a global contender by investing in the creation of at least six new AI schools by 2020.[1056] However, China also released a corresponding program with the aim to become a world leader in AI by 2030: the country established an AI Governance Expert Committee and released the New Generation Artificial Intelligence Development Plan.[1057] In addition, China published eight non-binding AI principles to guide the development of Artificial Intelligence,[1058] and there are also local government AI policy initiatives throughout China: Shanghai issued its own implementation plan for AI[1059], Guangzhou launched[1060] an International Institute of AI, and Beijing plans to invest in an AI-focused industrial park[1061] and published their own Principles on AI that have been released by a coalition of universities and companies including big players like Alibaba and Tencent.[1062] Together with numerous research and education institutes as well as AI companies, China's standards administration moreover issued a white paper on AI standardization which also shows that the country takes strong efforts towards becoming a leader in modern technologies such as Big Data and AI after "*functioning as a factory to the world for almost four decades*".[1063] China also announced the formation of the National Artificial Intelligence Standardization Group and Expert Advisory Group to oversee the nation's AI development.[1064] Singapore recently introduced principles to promote "*Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector.*"[1065] Singapore's initiative is a good example that it is difficult to classify all those different initiatives appropriately: on the one hand, this is a national initiative, on the other hand, it might have the potential to lead the path forward for that specific

[1056] Kathleen Walch: Is South Korea Poised To Be A Leader In AI? Article published September 7 2018, available at https://www.forbes.com/sites/cognitiveworld/2018/09/07/is-south-korea-poised-to-be-a-leader-in-ai/#4a0f3d74fa2f. Retrieved October 15, 2021.

[1057] Source: https://flia.org/notice-state-council-issuing-new-generation-artificial-intelligence-development-plan/.

[1058] The guidelines were published June 17, 2019 by China's Ministry of Science and Technology. English translation is available at https://perma.cc/V9FL-H6J7. Retrieved October 15, 2021.

[1059] Source: http://chinainnovationfunding.eu/china-new-generation-artificial-intelligence-development-report-2019/. Retrieved October 15, 2021.

[1060] Joanna You, Louis Berney: Guangzhou International Institute of AI launched in Nansha. Article published December 15 2017, available at https://www.lifeofguangzhou.com/whatsNew/content.do?contextId=6987&frontParentCatalogId=199&frontCatalogId=200. Retrieved October 15, 2021.

[1061] Arjun Kharpal: China is building a giant $2.1 billion research park dedicated to developing A.I. Article published January 3 2018, available at https://www.cnbc.com/2018/01/03/china-is-building-a-giant-2-point-1-billion-ai-research-park.html. Retrieved October 15, 2021.

[1062] The full text of the Beijing AI Principles is available at https://www.baai.ac.cn/news/beijing-ai-principles-en.html. Retrieved October 15, 2021.

[1063] Rachana Gupta: China making big strides in artificial intelligence. Article published on September 6 2019, available at http://www.china.org.cn/opinion/2019-09/06/content_75178964.htm. Retrieved October 15, 2021.

[1064] Meghan Han: China Aims to Get the Jump on AI Standardization. Article published January 25 2018, available at https://syncedreview.com/2018/01/25/china-aims-to-get-the-jump-on-ai-standardization/#:~:text=China%20has%20just%20released%20its%20%E2%80%9CArtificial%20Intelligence%20Standardization,Standardization%20Management%20Committee%20Second%20Ministry%20of%20Industry%20%28%E5%9B%BD%E5%AE%B6%E6%A0%87%E5%87%86%E5%8C%96%E7%AE%A1%E7%90%86%E5%A7%94%E5%91%98%E4%BC%9A%E5%B7%A5%E4%B8%9A%E4%BA%8C%E9%83%A8%29. Retrieved October 15, 2021.

[1065] The text of Singapore's FEAT principles is available at https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf. Retrieved October 15, 2021.

industry. India's National Institution for Transforming India (NITI) published the nation's national strategy on Artificial Intelligence back in 2018,[1066] and the country's strategy focuses, amongst other things, on sectors like health and education as well as (smart city) infrastructure and mobility to increase social inclusion and addresses issues like ethics, bias and privacy.[1067] India's strategy paper proposes the creation of Centers of Research Excellence in AI, and in 2019, India's government formed a committee to push for an organized AI policy to further India's AI mission, and the Ministry of Electronics and Information Technology released its own proposal to set up a national AI program.[1068] In recent years, further countries developed national AI initiatives and plans, for example Malaysia,[1069] Indonesia[1070] or Taiwan.[1071]

2. North America

Recent developments in the United States are very interesting, it all started with the California Consumer Privacy Act (CCPA)[1072] and the Consumer Online Privacy Rights Act (COPRA).[1073] At present, more and more U.S. states are about to introduce privacy bills of their own; developments in the U.S.A. with regards to laws relating to algorithmic (automated) decision making and the use of Artificial Intelligence are so dynamic that corresponding legal news alerts are delivered on a weekly basis;[1074] therefore, the emerging legal landscape in the United States has to be closely monitored. Moreover, the White House published the "*Executive Order on Maintaining American Leadership in Artificial Intelligence*"[1075] in 2019 which, amongst other things, requires the National Institute of Standards and Commerce (NIST) to release a plan[1076] for federal engagement on AI standards that address both, technical issues and safety as well as some substantive concerns around AI like data

[1066] Source: https://niti.gov.in/national-strategy-artificial-intelligence. Retrieved October 15, 2021.

[1067] Source: http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf. Retrieved October 15, 2021.

[1068] Source: Artificial Intelligence Index Report 2021, Chapter 7: AI policy and national strategies. Report published 2021 and is available at https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report-_Chapter-7.pdf. Retrieved October 15, 2021.

[1069] Priyankar Bhunia: Plans for cloud-first strategy and national AI framework revealed at 29th MSC Malaysia Implementation Council Meeting. Article published October 28 2017, available at https://opengovasia.com/plans-for-cloud-first-strategy-and-national-ai-framework-revealed-at-29th-msc-malaysia-implementation-council-meeting/. Retrieved October 15, 2021.

[1070] Source: https://ai-innovation.id/strategi. Retrieved October 15, 2021.

[1071] Source: https://ai.taiwan.gov.tw/. Retrieved October 15, 2021.

[1072] The text of the bill is available at https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf. Retrieved October 15, 2021.

[1073] The text of the bill is available at https://www.cantwell.senate.gov/imo/media/doc/COPRA%20Bill%20Text.pdf. Retrieved October 15, 2021.

[1074] The U.S. law firm Husch Blackwell offers a free online State Privacy Law Tracker with weekly updates. The tracker is available at https://www.huschblackwell.com/2021-state-privacy-law-tracker.

[1075] Source: https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/. Retrieved October 15, 2021.

[1076] NIST: U.S. Leadership in AI - A plan for federal engagement in developing technical standards and related tools prepared in response to Executive Order 13859, draft submitted on August 9 2020, available at https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf. Retrieved October 15, 2021.

quality and explicability of AI decisions as well as ethical considerations.[1077] In the same year, Democrats from four key Senates released a Privacy and Data Protection Framework[1078] that should serve as the baseline for any comprehensive federal privacy and data protection legislation.[1079] It truly seems the AI arms race has begun[1080] as there seems to be a strong wish to shape the American AI policy: in the last three years, the U.S.A. engaged in many further initiatives like the Artificial Intelligence Act[1081], the Algorithmic Accountability Act,[1082] the AI in Government Act,[1083] the Future of AI Act,[1084] the Artificial Intelligence Reporting Act,[1085] the National Artificial Intelligence Initiative Act,[1086] the Advancing AI Research Act,[1087] the Growing Artificial Intelligence Through Research Act**[1088]** as well as the National Security Commission on Artificial Intelligence Act.[1089] Together with France, Canada issued a statement on Artificial Intelligence[1090] with the wish to promote human-centric AI that is based on human rights and values like inclusion and diversity – as well as innovation and economic growth.[1091] Canada issued a Directive on Automated Decision-Making,[1092] and Canada's National Research Council published an advisory statement on human ethics in Artificial Intelligence and Big Data research.[1093] The Canadian government announced the "*Declaration of the International*

[1077] Duane Pozza, Jacquelynn Ruff: The next phase of AI regulation in the US and abroad. Article published July 19 2019, available at https://www.wileyconnect.com/home/2019/7/19/the-next-phase-of-ai-regulation-in-the-us-and-abroad. Retrieved October 15, 2021.

[1078] The text of the Senate's principles is available at https://www.democrats.senate.gov/imo/media/doc/Final_CMTE%20Privacy%20Principles_11.14.19.pdf. Retrieved October 15, 2021.

[1079] Shiva Stella: Senate Releases Principles for Comprehensive Privacy Legislation. Article published on November 18 2019, available at https://www.publicknowledge.org/press-release/senate-releases-principles-for-comprehensive-privacy-legislation/. Retrieved October 15, 2021.

[1080] Source: AI Now 2019 Report published by the AI Now Institute, available at https://ainowinstitute.org/AI_Now_2019_Report.htm. Retrieved October 15, 2021.

[1081] Benjamin Muller: The Artificial Intelligence Act – a quick explainer. Article published May 4 2021, available at https://datainnovation.org/2021/05/the-artificial-intelligence-act-a-quick-explainer/. Retrieved October 15, 2021.

[1082] Source: https://www.congress.gov/bill/116th-congress/senate-bill/1108. Retrieved October 15, 2021.

[1083] Source: https://www.congress.gov/bill/115th-congress/senate-bill/3502. Retrieved October 15, 2021.

[1084] Source: https://www.congress.gov/bill/115th-congress/house-bill/4625. Retrieved October 15, 2021.

[1085] Source: https://www.congress.gov/bill/115th-congress/house-bill/6090/. Retrieved October 15, 2021.

[1086] Source: https://www.congress.gov/bill/116th-congress/house-bill/6216. Retrieved October 15, 2021.

[1087] Source: https://www.congress.gov/bill/116th-congress/senate-bill/3891. Retrieved October 15, 2021.

[1088] Source: https://www.congress.gov/bill/116th-congress/house-bill/2202. Retrieved October 15, 2021.

[1089] Source: https://www.congress.gov/bill/115th-congress/house-bill/5356/. Retrieved October 15, 2021.

[1090] Canada and France work with international community to support the responsible use of artificial intelligence. The corresponding press release from May 16, 2019 is available at https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2019/05/23_cedrico_press_release_ia_canada.pdf. Retrieved October 15, 2021.

[1091] Source: homepage of the Canadian government, blog entry published on June 7 2018, available at https://www.international.gc.ca/world-monde/international_relations-relations_internationales/europe/2018-06-07-france_ai-ia_france.aspx?lang=eng. Retrieved October 15, 2021.

[1092] Canada's Directive on Automated Decision-Making was published in April 2021, and is available at https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592. Retrieved October 15, 2021.

[1093] The advisory statement on human ethics in AI and Big Data research was published in 2017 and last modified in 2019. It is available at https://nrc.canada.ca/en/corporate/values-ethics/research-involving-human-participants/advisory-statement-human-ethics-artificial-intelligence-big-data-research-2017. Retrieved October 15, 2021.

Panel on AI"[1094] which states that participants in the IPAI will obey the following values for the development and use of AI:[1095]

i. *"**Promote a human-centric and ethical approach to AI that is grounded in human rights**,*

ii. ***Support a multi-stakeholder approach to AI**,*

iii. ***Stimulate innovation, growth and well-being through AI**,*

iv. Align efforts on AI with the principles of sustainable development and the goals of the 2030 Agenda for Sustainable Development,

v. ***Promote and protect democratic values, processes and institutions**,*

vi. ***Promote international scientific collaboration on AI,***

vii. ***Foster transparency and openness of AI systems**,*

viii. ***Strengthen diversity and inclusion through AI**,*

ix. ***Foster trust and accountability in AI**,*

x. ***Bridge digital divides.***"

3. Latin America

Mexico joined many other ambitious nations in their wish to establish themselves as a leader in digital technologies such as Artificial Intelligence and was the first country in Latin America to announce a national AI strategy.[1096] Mexico's approach is unique insofar as it focuses on the social impacts of AI, for example by addressing use cases like combating corruption, reducing crime, improving public health and increasing financial inclusion.[1097] Brazil's Ministry of Science, Technology, Innovations and Communications published the nation's strategy for digital transformation to harmonize and coordinate various governmental initiatives on digital issues.[1098] In addition, the government launched a national plan for the Internet of Things[1099] that will be supported by several "*AI laboratories*"[1100] to cover different areas and aspects of AI. Like Mexico, Brazil is also concerned with social impact of Big Data and Artificial Intelligence, which is why their strategy includes a

[1094] Meagan Simpson: Canada, France Governments Announce Declaration of the International Panel on AI. Article published May 16 2019, available at http://canada.ai/posts/canada-france-governments-announce-declaration-of-the-international-panel-on-ai. Retrieved October 15, 2021.

[1095] Source: https://www.canada.ca/en/innovation-science-economic-development/news/2019/05/declaration-of-the-international-panel-on-artificial-intelligence.html. Retrieved October 15, 2021.

[1096] Source: https://36dc704c-0d61-4da0-87fa-917581cbce16.filesusr.com/ugd/7be025_85f5cec6ea584d8a842d11ad401c0685.pdf. Retrieved October 15, 2021.

[1097] Emma Martinho-Truswell, Constanza Gomez Mont: Mexico leads Latin America as one of the first ten countries in the world to launch an artificial intelligence strategy. Article published May 24 2018, available at https://www.oxfordinsights.com/insights/2018/5/24/mexico-leads-latin-america-as-one-of-the-first-ten-countries-in-the-world-to-launch-an-artificial-intelligence-strategy. Retrieved October 15, 2021.

[1098] Source: https://www.gov.br/mcti/pt-br. Retrieved October 15, 2021.

[1099] Source: https://www.bnamericas.com/en/news/brazil-issues-decree-for-national-iot-plan. Retrieved October 15, 2021.

[1100] Source: https://agenciabrasil.ebc.com.br/en/geral/noticia/2019-11/brazil-unveils-eight-new-ai-labs. Retrieved October 15, 2021.

provision "*to evaluate such consequences and propose policies which maximize positive results and mitigate potential negative effects*."[1101] In the meantime, further South American countries like Colombia,[1102] Chile[1103] and Uruguay[1104] have been working on their own national AI strategies.

4. Europe

In addition to France's above-mentioned joint activities with Canada, the country also announced their "*mission for a meaningful AI*"[1105] which complements the aforementioned promotion of AI that shall be based on human rights and values like inclusion, diversity but also innovation and economic growth: the French strategy proposes that Artificial Intelligence should not be used to reinforce problems like inequality and global challenges like the climate crisis, but should be used to solve these problems by making ecology its first priority and by addressing impacts on ethics, employment and diversity.[1106] It can generally be said that Europe has a growing AI industry presence, which is led by the UK and followed by Germany[1107] as well as France,[1108] Spain,[1109] Sweden,[1110] the Netherlands[1111] and Italy.[1112] Many other countries dealt with the issue of Artificial Intelligence and published action plans and strategies of their own, for example Luxembourg,[1113] Lithuania,[1114] Malta[1115] or Norway.[1116] Finland reviewed the public sector use of automation and evaluated the introduction of mandatory due

[1101] Source: https://futureoflife.org/ai-policy-brazil/. Retrieved October 15, 2021.

[1102] Source: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf. Retrieved October 15, 2021.

[1103] Source: https://www.gob.cl/en/news/government-announces-artificial-intelligence-plan-be-developed-science-ministry/. Retrieved October 15, 2021.

[1104] Source: https://www.gub.uy/participacionciudadana/consultapublica. Retrieved October 15, 2021.

[1105] Cedric Villani: For a meaningful Artificial Intelligence – towards a French and European strategy. Report published March 2018, available at https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf. Retrieved October 15, 2021.

[1106] Alex Moltzau: The French National Strategy on Artificial Intelligence. Article published January 15 2020, available at https://towardsdatascience.com/the-french-national-strategy-on-artificial-intelligence-c8c8fcfdace1. Retrieved October 15, 2021.

[1107] FTI consulting: The global policy response to Artificial Intelligence, published February 2018.

[1108] Source: https://www.gouvernement.fr/en/franceia-the-national-artificial-intelligence-strategy-is-underway. Retrieved October 15, 2021.

[1109] Source: https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2020/20201202_enia.aspx. Retrieved October 15, 2021.

[1110] Source: https://www.government.se/information-material/2019/02/national-approach-to-artificial-intelligence/. Retrieved October 15, 2021.

[1111] Source: https://www.government.nl/documents/reports/2019/10/09/strategic-action-plan-for-artificial-intelligence. Retrieved October 15, 2021.

[1112] Source: https://ia.italia.it/en/ai-in-italy/. Retrieved October 15, 2021.

[1113] Source: https://digital-luxembourg.public.lu/initiatives/artificial-intelligence-strategic-vision-luxembourg#:~:text=Luxembourg%20intends%20to%20remain%20at%20the%20forefront%20of,experts%20in%20law%2C%20science%2C%20technology%2C%20ethics%20and%20humanities. Retrieved October 15, 2021.

[1114] Source: http://kurklt.lt/wp-content/uploads/2018/09/StrategyIndesignpdf.pdf. Retrieved October 15, 2021.

[1115] Source: https://malta.ai/. Retrieved October 15, 2021.

[1116] Source: https://www.regjeringen.no/en/dokumenter/nasjonal-strategi-for-kunstig-intelligens/id2685594/. Retrieved October 15, 2021.

diligence legislation,[1117] and AI initiatives are starting to emerge at regional level: the autonomous regions of Valencia[1118] and Catalonia[1119] introduced their own AI strategies. For the purposes of this paper, two countries may serve as examples, Germany and the UK: Germany has a strong tradition in data protection and technical innovation, and the UK has a well-established tech landscape and is traditionally strong in the area of research.[1120] In the UK, AI policy discussions intensified in recent years, and the government is focusing on various initiatives, supported by a government AI Policy Unit, an industry AI Council and an All Party Parliamentary Group which was established to address ethical issues, social impact, industry norms and regulatory options for AI.[1121] One of the key recommendations of the All Party Parliamentary Group was to appoint a Minister for AI to sit within the Cabinet,[1122] and, according to the House of Lords Select Committee on Artificial Intelligence report,[1123] further government action is needed. On top of the famous Alan Turing Institute[1124], the UK furthermore established a Centre for Data Ethics and Innovation (CDEI)[1125] that will be tasked with AI monitoring and testing potential interventions in the tech landscape. The CDEI is also looking at online (social media) targeting and issued a corresponding report[1126] for the government. In September 2018, the UK government launched an experiment with the World Economic Forum[1127] to develop procurement policies for AI.[1128] The UK government announced that it intended to seize the opportunity afforded by the UK's exit from the European Union to reform the UK's data protection

[1117] AccessNow: Europe's approach to artificial intelligence: how AI strategy is evolving, report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf. Retrieved October 15, 2021.

[1118] Source: http://www.presidencia.gva.es/documents/80279719/169117420/Dossier_en.pdf/c943f4aa-2822-4c5e-a3db-63a 45cca5bf5. Retrieved October 15, 2021.

[1119] Source: https://www.elnacional.cat/en/tech/artificial-intelligence-digital-strategy-catalonia_471462_102.html. Retrieved October 15, 2021.

[1120] Richard Stirling, Hannah Miller, Emma Martinho-Truswell: Oxford Institute Government AI Readiness Index. Article published in 2017, available at https://www.oxfordinsights.com/government-ai-readiness-index?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_recent_activity_details_all%3BeJ%2FPpiq8RzyLuLPtyf%2FYoA%3D%3D. Retrieved October 15, 2021.

[1121] The Future of Life Forum provides country-by-country information on AI. Details on the UK's AI initiatives are available at https://futureoflife.org/ai-policy-united-kingdom/. Retrieved October 15, 2021.

[1122] FTI consulting: The global policy response to Artificial Intelligence. Report published February 2018.

[1123] House of Lords Select Committee on Artificial Intelligence Report of Session 2017–19: HL Paper 100 AI in the UK: ready, willing and able? Report published 2018, available at https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf. Retrieved October 17, 2021.

[1124] That is, the National Institute of AI. They explain that they "*bring the best placed legislators together to understand the impact of Artificial Intelligence and the regulatory approaches*", source: https://instituteofai.org/about/. Retrieved October 17, 2021.

[1125] Background information on UK's Centre for Data Ethics and Innovation is available at their website: https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation. Retrieved October 17, 2021.

[1126] CDEI's report was published in February 2020 and is available at https://www.gov.uk/government/publications/cdei-review-of-online-targeting/online-targeting-final-report-and-recommendations. Retrieved October 17, 2021.

[1127] In March 2018, the World Economic Forum issued a White Paper on AI: How to Prevent Discriminatory Outcomes in Machine Learning. The document is available onlie at http://www3.weforum.org/docs/WEF_40065_White_Paper_How_to_Prevent_Discriminatory_Outcomes_in_Machine_Learning.pdf. Retrieved October 17, 2021.

[1128] Source: https://www.eurasiareview.com/21092018-uk-partners-with-world-economic-forum-to-develop-first-artificial-intelligence-procurement-policy/. Retrieved October 17, 2021.

regime,[1129] and the UK government also announced it intends to revisit the nation's AI strategy,[1130] which might have implications for data protection as there are discussions around, for example, softening the conditions around (re-)use of personal data for research and considerations if data protection legislation and the ICO is the right forum and regulator for determining fairness in profiling and automated decision-making.[1131] In Germany,[1132] the recently published expert opinion of the German Data Ethics Commission[1133] underlines the need for a human-centric approach and confirms core principles like transparency and explicability and robustness as well as values like non-discrimination. The expert opinion of the German Data Ethics Commission distinguishes between algorithm-based (suggestion-only), algorithm-driven (limited leeway) and fully automated decisions. It moreover pursues further ideas by presenting a total of not less than 75 recommendations for the use of Artificial Intelligence, including the call for a regulation for Algorithmic Systems and by suggesting various new approaches to AI: a labeling requirement (e.g. for so-called bots); licensing procedures; product liability; a risk-based regulatory approach based on a graded model for AI reflecting the degree of criticality involved in the data processing activity; a specific right to access for researchers and journalists in sectors that are of particular interest to society; a specific duty with regard to interconnectivity in certain sectors (e.g. messaging services, social media). The idea of a right to data ownership that has been discussed in the literature[1134] as one possible way to strengthen individuals' rights is not recommended by the commission since the introduction of new exclusive rights is believed to complicate the legal framework rather than solving existing problems.

5. Australia and New Zealand

In order to build Australia's Artificial Intelligence capability and help raise trust in AI technologies, the country developed an AI ethics framework to guide businesses and governments when they design,

[1129] Marcus Evans, Lara White, Sahar Bhaimia: UK Government sets out proposals to shake up UK data protection laws. Article published September 28 2021, available at https://www.dataprotectionreport.com/2021/09/uk-government-sets-out-proposals-to-shake-up-uk-data-protection-laws/. Retrieved October 17, 2021.

[1130] Source: https://www.gov.uk/government/publications/national-ai-strategy?utm_medium=email&utm_campaign=govuk-notifications&utm_source=d5d1f14b-b826-4931-92a2-706e1e5ee6de&utm_content=immediately. Retrieved October 17, 2021.

[1131] Marcus Evans, Peter McBurney, Michael Sinclair: Article published September 27 2021, available at https://www.insidetechlaw.com/blog/the-uk-national-ai-strategy-regulation-data-protection-and-ipr-in-the-mix. Retrieved October 17, 2021.

[1132] The country's AI strategy was presented in November 2018 and is available at https://ec.europa.eu/knowledge4policy/publication/germany-artificial-intelligence-strategy_en. Retrieved October 17, 2021.

[1133] The "Gutachten der Datenethikkommission" was published in October 2019 and is retrieved from https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=92BB855CAF2B68DFB5D0EB3D32FD72E4.2_cid287?__blob=publicationFile&v=5. Retrieved October 17, 2021.

[1134] Udo Kornmeier, Anne Baranowski: Eigentum an Daten – Zugang statt Zuordnung, Der Betriebsberater 2019, pp. 1219-1225.

develop and implement AI:[1135] the outcome of their program is a set of voluntary AI ethics principles including background information on how it was developed as well as guidance on when and how to apply those principles. Moreover, the country's leading standards organization released a discussion paper on developing standards for Artificial Intelligence which underlines the importance of the development of AI standards for the future use of this cutting-edge technology.[1136] Australia's neighbor New Zealand launched a AI forum[1137] in 2017 to connect the country's AI community including citizens, business, academia, and the government and to advance New Zealand's AI ecosystem through advocacy and collaboration.[1138] Since the forum is a not-for-profit, non-governmental body, the forum's work cannot be considered a national strategy, however, their report[1139] may serve as a basis to shape New Zealand AI landscape. In addition, New Zealand also launched an initiative for the government's data system, the Algorithm Charter for Aotearoa[1140].

6. Israel and the Middle East

Despite the fact that Israel is a small country, the nation is determined to be the next major artificial intelligence player.[1141] Israel is heavily engaged in AI and launched a national AI program, however, lack of budget threatens its implementation.[1142] In the framework of "*Smart Dubai*", which is an initiative that fosters digitalization and technologies like Blockchain and Artificial Intelligence, Dubai issued AI ethics principles and guidelines to "*deliver detailed guidance for the crucial issues of fairness, accountability, transparency and explainability of the algorithms at the heart of AI systems. We would like to see the Dubai AI Ethics Guidelines evolve into a universal, practical and applicable*

[1135] Source: https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework#:~:text=To%20help%20build%20trust%20in%20AI%2C%20we%E2%80%99ve%20committed,Australian%20Government%E2%80%99s%20commitment%20to%20build%20Australia%E2%80%99s%20AI%20capabilities. Retrieved October 17, 2021.

[1136] Meaghan Powell, Lesley Sutton: AI regulation: the push for Australian standards. Article published July 29 2019, available at https://www.gtlaw.com.au/insights/ai-regulation-push-australian-standards. Retrieved October 17, 2021.

[1137] Source: https://aiforum.org.nz/. Retrieved October 17, 2021.

[1138] Source: https://www.mbie.govt.nz/dmsdocument/5754-artificial-intelligence-shaping-a-future-new-zealand-pdf. Retrieved October 17, 2021.

[1139] Source: http://resources.aiforum.org.nz/AI+Shaping+A+Future+New+Zealand+Report+2018.pdf. Retrieved October 17, 2021.

[1140] Source: https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter/#:~:text=The%20Algorithm%20charter%20for%20Aotearoa%20New%20Zealand%20is,o%20Te%20M%C4%81tauranga%20%E2%80%94%20The%20Ministry%20of%20Education. Retrieved October 17, 2021.

[1141] Éanna Kelly: Israel sets out to become the next major artificial intelligence player. Article published July 2 2019, available at https://sciencebusiness.net/news/israel-sets-out-become-next-major-artificial-intelligence-player. Retrieved October 17, 2021.

[1142] Meir Orbach: Israel launches national AI program, but lack of budget threatens its implementation. Article published December 22 2020, available at https://www.calcalistech.com/ctech/articles/0,7340,L-3883355,00.html. Retrieved October 17, 2021.

framework informing ethical requirements for AI design and use."[1143] Dubai's AI principles focus on ethics, humanity, inclusiveness and security[1144] and Dubai moreover offers a free self-assessment AI ethics tool to provide practical help for the public and private sector as well as anyone "*interested in how ethical AI is applied in society and city service settings*".[1145] Given the importance of AI for various industries and in particular for autonomous weapons and drones, Israel and UAE defense companies partner on Artificial Intelligence.[1146] In recent years, further countries in the Arabian Peninsula engaged in their own national AI strategies, for example Qatar.[1147]

VII. Other

1. Rome Call for AI Ethics

Individual and societal implications of certain AI applications are so significant that even the Vatican raised the issue in their 2020 conference "*The Good Algorithm*", the Vatican Academy for Life concluded the session with the Rome Call for AI Ethics.[1148] Microsoft and IBM are the first signatories to this AI ethics code that calls for a human-centered approach.[1149] The initiative focuses on the responsibility that comes with new digital technologies. The Rome Call for AI Ethics comprises three impact areas ethics, education and rights and names the following six principles:[1150]

i. ***"Transparency***[1151]*: In principle, Artificial Intelligence systems must be explainable.*

ii. ***Inclusion****: the needs of all human beings must be taken into consideration so that all can benefit form and enjoy the best possible conditions to express themselves and grow.*

iii. ***Responsibility****: Designers and developers of Artificial Intelligence solutions must act responsibly and transparently.*

[1143] The "Smart Dubai" website is available at https://www.smartdubai.ae/initiatives/ai-ethics. Retrieved October 17, 2021.

[1144] Dubai's AI principles and guidelines were published in 2018 and are available at https://www.smartdubai.ae/pdfviewer/web/viewer.html?file=https://www.smartdubai.ae/docs/default-source/ai-ethics-resources/ai-ethics.pdf?sfvrsn=a9081451_8. Retrieved October 17, 2021.

[1145] Source: https://www.smartdubai.ae/initiatives/ai-principles-ethics. Retrieved October 17, 2021.

[1146] Seth Frantzman: Israel and UAE defense companies partner on Artificial Intelligence. Article published April 21 2021, available at https://nationalinterest.org/blog/buzz/israel-and-uae-defense-companies-partner-artificial-intelligence-183274. Retrieved October 17, 2021.

[1147] Joseph Varghese: Qatar launches strategy to tap AI for future. Article published October 29 2019, available at https://www.gulf-times.com/story/645930/Qatar-launches-strategy-to-tap-AI-for-future#:~:text=The%20National%20AI%20Strategy%20is%20a%20blueprint%20produced,collaboration%20between%20the%20government%20and%20a%20research%20institute. Retrieved October 17, 2021.

[1148] Vatican workshop on ethics in AI: Artificial Intelligence 2020 RenAIssance – a human-centric Artificial Intelligence (2020), presentation held on February 28 2020, available at http://www.academyforlife.va/content/dam/pav/documenti%20pdf/2020/CALL%2028%20febbraio/02_Brad%20Smith_20200228%20Vatican%20AI%20v07.pdf. Retrieved October 17, 2021.

[1149] Joe Fay: Vatican signs up IBM and Microsoft as AI ethics apostles. Article published March 2 2020, available at https://devclass.com/2020/03/02/vatican-signs-up-ibm-and-microsoft-as-ai-ethics-apostles/.

[1150] Source: https://www.romecall.org/the-call/. Retrieved October 17, 2021.

[1151] Bold means emphasis added.

iv. ***Impartiality**: Systems should not be created or operated according to bias, in view to protect human equality and dignity.*

v. ***Reliability**: Artificial Intelligence systems must be able to operate reliably.*

vi. ***Security and privacy**: Artificial Intelligence systems must work securely and respect the privacy of users."*

2. Hippocratic Oath for Data Scientists

Another noteworthy initiative is the Hippocratic Oath for Data Scientists: the interesting idea behind this voluntary commitment is that, unlike medical staff that is trained on and aware of ethics aspects of their work from the beginning, this is not common in data science – despite the fact that even players like Microsoft say it could make sense to "*bind coders to a pledge like that taken by physicians to first do no harm*."[1152] Since many activities in the area of data science can have serious consequences for individuals and society,[1153] data scientists who process data and design algorithms should respect the following three principles:[1154]

i. *"**Responsibility and Neutrality**:[1155] Every data scientist has to assume his responsibilities in the event of breaches or conflicts of interest, and he must alert if any illegal acts related to data are observed. He must also exercise his professional activity respecting the privacy and dignity of people in all their dimensions.*

ii. ***Transparency**: As a data scientist, I have the right to inform all stakeholders in an understandable and precise manner about the purposes, modalities and potential implications of my use of data.*

iii. ***Equity**: I will always ensure that individuals or groups are not discriminated on the basis of illegal or illegitimate criteria, directly or indirectly, related to my data work."*

The previous explanations have shown that the rapid spread of Artificial Intelligence systems has led to a rise in various (best practice, ethics and human rights-based) guidelines and recommendations to help with the use and further development of such applications. In summary, the current legal framework for AI can be grouped as follows: there is legislation for specific processing operations

[1152] Tom Simonite reports about Microsoft's related publication in his 2018 blog post: Should Data Scientists Adhere to a Hippocratic Oath? Article published August 2 2018, available at https://www.wired.com/story/should-data-scientists-adhere-to-a-hippocratic-oath/. Retrieved October 17, 2021.

[1153] Lori Sherer: Data Scientists, Take a Hippocratic Oath: While the ethics of analytical tools can be tricky to parse, five basic principles can help data scientists address the challenge. Article published June 13 2018, available at https://www.bain.com/insights/data-scientists-take-a-hippocratic-oath-forbes/ Retrieved October 17, 2021.

[1154] Kamal Chouhbi: Hippocratic Oath for Data Scientists – the ethical checklist that every data scientist must follow. Article published Ocrober 6 2020, available at https://towardsdatascience.com/hippocratic-oath-for-data-scientists-407d2db15a78. Retrieved October 17, 2021.

[1155] Bold means emphasis added.

(e.g.) automated decision making, for specific industries (e.g. finance or health), and for specific technology (e.g. facial recognition) as well as rules for accountability for (unintended) consequences by the use of AI (e.g. criminal, civil), and there are moreover numerous voluntary ethics codes.[1156] However, as for the latter, there has been little focus on analyzing these efforts to understand the main principles behind these frameworks. To that end, the Berkman Klein Center for Internet and Society evaluated numerous AI principles documents to detect potential common standards; their research uncovered a growing consensus around eight key thematic trends:[1157]

i. *"**Privacy**[1158] including control over use of data, consent, privacy by design, recommendations for data protection laws, the ability to restrict processing, as well as the right to erasure and rectification,*

ii. ***Accountability including** recommendation for new regulations, impact assessments, evaluation and auditing requirement, verifiability and replicability as well as liability and legal responsibility and the ability to appeal, environmental responsibility and the creation of a monitoring body and remedies for automated decisions,*

iii. ***Safety and security** including reliability, predictability and security by design*

iv. ***Transparency and explainability** including open source data and algorithms, notifications when interacting with AI and whenever AI makes a decision about an individual, regular reporting requirements and the right to information and finally, open procurement (for governments),*

v. ***Fairness and non-discrimination** including the prevention of bias, equality, inclusiveness in design and impact as well as representative and high quality data,*

vi. ***Human control of technology** including human review of automated decisions and the ability to opt out of automated decisions,*

vii. ***Professional responsibility** including multistakeholder collaboration, responsible design, consideration of long-term effects as well as accuracy and scientific integrity,*

viii. ***Promotion of human values** including leveraged to benefit society, human flourishing and access to technology."*

The researchers stress that, by sharing their observations, thy hope that policymakers and others "*working to maximize the benefits and minimize the harms of AI will be better positioned to build on existing efforts and to push the fractured, global conversation on the future of AI toward*

[1156] Maya Medeiros: A legal framework for artificial intelligence. Article published November 20 2019, available at https://www.socialmedialawbulletin.com/2019/11/a-legal-framework-for-artificial-intelligence/. Retrieved October 17, 2021.

[1157] Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy, Madhulika Srikumar: Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. Berkman Klein Center Research Publication No. 2020-1 published February 14 2020, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482. Retrieved October 17, 2021.

[1158] Bold means emphasis added.

consensus."[1159] Obviously, such research is very welcome and of great value, but the problem with all these initiatives is that, regardless of whether the guideline or recommendation is issued at international or national level or published by civil society, multi-stakeholder or intergovernmental organizations or if it originated in the private sector – but the problem is that, at present, most of the these initiatives are legally not binding.[1160] Governments around the world are working towards trustworthy AI, but there is no consensus on how to best regulate AI: there is agreement that transparency is a minimum requirement, and discussions started shifting in the direction of human rights protections with growing calls to ban facial recognition, but there is "*significant divergence regarding what stakeholders want to see in the upcoming EU legislation and their respective national policies*", and some legislators even expressed the fear of over-regulation.[1161]

G. Future developments to consider

I. Proposed regulations at EU level

1. Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

The PECD shall be replaced by a regulation[1162] which may be of great importance as it would directly affect businesses and especially marketers[1163] by new rules on the need for consent and the use of content, cookies and metadata[1164] which may potentially lead to even restrictions for the collection and use of personal data. There discussions around the proposal for an ePrivacy regulation have been

[1159] Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy, Madhulika Srikumar: Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. Berkman Klein Center Research Publication No. 2020-1 published February 14 2020, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482. Retrieved October 17, 2021.

[1160] See AlgorithmWatch's AI Ethics Guidelines Global Inventory: https://inventory.algorithmwatch.org/. Retrieved October 17, 2021.

[1161] Accessnow: Europe's approach to Artificial Intelligence: How AI strategy is evolving. Report published December 2020, and is available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf. Retrieved October 17, 2021.

[1162] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010. Retrieved October 17, 2021.

[1163] Background information on the relationship between PECD and GDPR is provided by the law firm of Brinkhof Advokaten who prepared a paper in 2018 for CIPL, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-brinkhof_epr_study.pdf. Retrieved October 17, 2021.

[1164] The law firm of Linklaters provide an overview on the status of the ePrivacy Regulation, available at https://www.linklaters.com/de-de/insights/publications/tmt-news/tmt-news---june-2017/eu---status-of-the-proposed-eprivacy-regulation-tighter-cookie-rules-and-more. Retrieved October 17, 2021.

going on for several years[1165] since the European Union Parliament, Commission and Council took differing positions which lead to the result that this new regulation did not come into force at the same time as the GDPR as originally planned. Already in 2017, a first draft of the ePrivacy Regulation was proposed which contained additional rules to extend and particularize the GDPR by addressing the use of electronic communications, metadata, cookies, direct marketing as well as nuisance calls.[1166] Latest developments point to important changes from the individual's perspective, for example by allowing the processing of electronic communications data without the user's consent to ensure the integrity of communications services, identifying malware or in cases where EU (member states) laws require the processing for the prosecution of criminal offences or prevention of threats to public security; the draft also allows for metadata to be used to detect fraud and to process metadata for compatible purposes – or to protect "users' vital interests" such as in monitoring for the spread of epidemics.[1167] This use case is an example for consequences for individuals' privacy protections and choices in the framework of the COVID-19-epidemic. In early 2021, the Council of the European Union issued a press release in which they explain key provisions of the most current version of the draft ePrivacy regulation:[1168] the draft does not prevent the use of cookie walls, meaning that a service can be made conditional on accepting cookies, provided that the service provider offers an equivalent option that does not require the acceptance of cookies; when required under EU or member state law for the prevention, investigation, detection or prosecution of criminal offences or prevention of threats to public security, the draft furthermore allows for an exception from the requirement to obtain consent and to delete/anonymize device data and/or metadata once it is no longer needed to provide the service.[1169] In their press release, the Council stresses their awareness regarding cookie consent fatigue, which is why end users will be able to give consent to the use of certain types of cookies by whitelisting one or several providers in their browser settings.[1170] This sounds fairly easy, but includes the risk that users

[1165] History and discussion points are summarized by the European Digital Rights (EDRi), an association of civil and human rights associations from across Europe. The text is available at https://edri.org/tag/eprivacy-regulation/. Retrieved October 17, 2021.

[1166] Ceyhun Pehlivan, Peter Church: EU: The ePrivacy Regulation - Let the trilogue begin! Article published February 12 2021, available at https://www.linklaters.com/en/insights/blogs/digilinks/2021/february/eu---the-eprivacy-regulation---let-the-trilogue-begin. Retrieved October 17, 2021.

[1167] The lawfirm Hunton Andrews Kurth provided details on the final terms of the draft regulation in their 2021 blog: EU Member States Agree on Council's Text for the ePrivacy Regulation. Article published February 2021, available at https://www.huntonprivacyblog.com/2021/02/10/eu-member-states-agree-on-councils-text-for-the-eprivacy-regulation/. Retrieved October 17, 2021.

[1168] Council of the EU Press release: Confidentiality of electronic communications: Council agrees its position on ePrivacy rules, published February 10 2021, available at https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/. Retrieved October 17, 2021.

[1169] Lara White, Fiona Bundy-Clarke: Tentative further steps towards an agreed ePrivacy Regulation. Article for the law firm of Norton Rose Fulbright published February 15 2021, available at https://www.dataprotectionreport.com/2021/02/tentative-further-steps-towards-an-agreed-eprivacy-regulation/. Retrieved October 17, 2021.

[1170] Council of the EU Press release: Confidentiality of electronic communications: Council agrees its position on ePrivacy rules, published February 10 2021, available at https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/. Retrieved October 17, 2021.

may not be aware of the scope of their decision, and the question also is whether other techniques might be able to tell the same – or even more – about a user than cookies: Google started testing Federated Learning of Cohorts (FLoC)[1171] to replace third-party cookies. Some commented that this technology is more harmful than cookies since it will "*make your browser do the profiling (...) by boiling down your recent browsing activity into a behavioral label, and then sharing it with websites and advertisers*."[1172] On the occasion of a meeting of the Improving Web Advertising Business Group at the World Wide Web Consortium in early 2021, Google announced that it will not be introducing FLoC in the European Union for the time being.[1173] The fact that Google is omitting an area to which GDPR applies suggests that there is awareness of the potential implications, and that FloC may raise fundamental privacy issues, starting with the processing of personal data, as well as identifiability within those clusters and issues of controllership and consequently, accountability.[1174] A related issue arises in the area of Re-purposing of data: under this draft, it will be admissible to process pseudonymized metadata and device information for purposes other than those for which they have been initially collected, provided that those new processes are compatible with the original purposes, which leads to uncertainty as criteria are fairly loosely defined, and the question is also how such information may be used over time taking into account developments in technology.[1175] However, it should also be noted that data that have been processed on the basis of consent or public interest cannot be repurposed in this way and can only be shared with third parties in an anonymized form, and use of re-purposed metadata to determine the nature or characteristics of an individual or to build a profile of them is not permitted to the extent this would significantly affect them[1176] – and this raises the question of where to draw the line between significant and insignificant. The draft text proposes a transition period of two years, so that businesses have time to adapt, but given that there are still

[1171] Source: https://blog.google/products/chrome/privacy-sustainability-and-the-importance-of-and/. Retrieved October 17, 2021.

[1172] Bennett Cyphers for the Electronic Frontier Foundation: Google's FLoC Is a Terrible Idea. Article published March 3 2021, available at https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea. Retrieved October 17, 2021.

[1173] Allison Schiff: Google Will Not Run FLoC Origin Tests In Europe Due To GDPR Concerns. Article published March 23 2021, available at https://www.adexchanger.com/platforms/google-will-not-run-floc-origin-tests-in-europe-due-to-gdpr-concerns/. Retrieved October 17, 2021.

[1174] Dieter Petereit: Google wird seine Tracking-Alternative FLoC zunächst nicht in Europa einführen. Der Suchmaschinenriese will erst die rechtliche Basis klären. DSGVO-Verstöße können schließlich sehr teuer werden. Article published March 24 2021, available at https://t3n.de/news/huch-dsgvo-googles-floc-scheitert-1369031/. Retrieved October 17, 2021.

[1175] Lara White, Fiona Bundy-Clarke: Tentative further steps towards an agreed ePrivacy Regulation. Article for the law firm of Norton Rose Fulbright published February 15 2021, available at https://www.dataprotectionreport.com/2021/02/tentative-further-steps-towards-an-agreed-eprivacy-regulation/. Retrieved October 17, 2021.

[1176] Lara White, Fiona Bundy-Clarke: Tentative further steps towards an agreed ePrivacy Regulation. Article for the law firm of Norton Rose Fulbright published on February 15 2021, available at https://www.dataprotectionreport.com/2021/02/tentative-further-steps-towards-an-agreed-eprivacy-regulation/. Retrieved October 17, 2021.

significant divergences[1177] between the Council and Parliament, the final version of this new regulation will be anxiously awaited, which is truly no surprise as the draft ePrivacy regulation touches on key privacy concerns like consent and cookie requirements, the re-use of personal data, and data retention. That is why privacy rights organizations raised their voice to underline their belief that this draft erodes privacy protections that were included in previous drafts.[1178] Ongoing controversy and diverging opinions at EU-level as well as the time delay in implementation further complicated the legal landscape, for example because some member states like Germany are still working on their national laws to transpose the existing regulation and at the same time, take into consideration the proposed ePrivacy regulation:[1179] Germany introduced a new Telecommunications Telemedia Data Protection Act (TTDSG) which combines data protection provisions from the existing Telemedia Act (TMG) and the Telecommunications Act (TKG), including provisions on the protection on the secrecy of telecommunications. According to the new law that shall be applied as of December 2021, consent would not be required in certain instances, and the law also paves the way for consent management services known as PIMS (Personal Information Management Systems) which allows users to indicate whether, where and under which conditions they consent or refuse to the setting of cookies.[1180] This should make annoying cookie banners unnecessary as service providers could automatically forward relevant choices to the respective website, and given the fact that NGOs like "*None Of Your Business*" (NYOB) recently filed more than 400 complaints against "*nerve-wracking cookie banners*"[1181] and paywalls which requires users "*to buy back their own data at an exorbitant price*",[1182] this seems truly necessary.

[1177] Andrew Cormack: ePrivacy Regulation – one step closer. Article published February 12 2021, available at https://regulatorydevelopments.jiscinvolve.org/wp/2021/02/12/eprivacy-regulation-one-step-closer/. Retrieved October 17, 2021.

[1178] Marianno Delli Santi: ePrivacy Regulation – an open letter from 30 civil society organizations: our letter to the European Parliament asking them to stand up against online tracking. Article published April 14 2021, available at https://www.openrightsgroup.org/publications/eprivacy-regulation-an-open-letter-from-30-civil-society-organisations/. Retrieved October 17, 2021.

[1179] Intersoft Consulting Services : TTDSG: Neues Datenschutzgesetz als Alternative zur ePrivacy-VO? Article published on their company website on October 7 2020, available at https://www.dr-datenschutz.de/ttdsg-neues-datenschutzgesetz-als-alternative-zur-eprivacy-vo/. Retrieved October 17, 2021.

[1180] Alexander Bugl: TMG and TKG to become TTDSG at December 1 2021. Article published August 25 2021, available at https://buglundkollegen.de/tmg-and-tkg-become-to-ttdsg-at-december-1-2021/#:~:text=TMG%20and%20TKG%20become%20to%20TTDSG%20at%20December,law%2C%20the%20Telecommunications%20Telemedia%20Data%20Protection%20Act%20%28TTDSG%29. Retrieved October 17, 2021.

[1181] Source: NYOB's website. Blog entry published August 10 2021, available at https://noyb.eu/en/noyb-files-422-formal-gdpr-complaints-nerve-wrecking-cookie-banners. Retrieved October 17, 2021.

[1182] Source: NYOB's website. Blog entry published August 13 2021, available at https://noyb.eu/en/news-sites-readers-need-buy-back-their-own-data-exorbitant-price. Retrieved October 17, 2021.

2. Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters

In order to allow for law enforcement and judicial authorities access electronic evidence needed to investigate and prosecute delinquents easily and quickly, two new rules[1183] were proposed in 2018. At first sight, this proposal does not have much to do with Big Data, but this development shows important new developments such as the ability to publish (disclose) data on an ad hoc basis is becoming increasingly important,[1184] and this might in fact influence the design of Big Data applications. But what is even more significant is that some authors claim that this proposal "*continues with the disastrous development in dealing with digital platforms: the outsourcing of fundamental rights protection to providers*".[1185] The obligation for service providers to cooperate with law enforcement authorities[1186] may be highly desirable from a legislator's point of view. But it must not be forgotten that private sector companies are neither responsible nor qualified for the protection of fundamental rights: How shall an average company[1187] decide whether or not the EPOC[1188] cannot be executed because based on the sole information contained in the EPOC it is apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive, the addressee shall also send the Form in Annex III to the competent enforcement authority in the member state of the addressee".[1189] As a consequence, providers criticize both, the effort associated with the new instruments and the planned transfer of responsibility for checking the legality of the orders.[1190] If

[1183] A proposal for a regulation on European production and preservation orders for electronic evidence in criminal matters (see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN), and a proposal for a directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN). Retrieved October 17, 2021.

[1184] A requirement that is already common in other jurisdictions, for example the US CLOUD Act (Clarifying Lawful Overseas Use of Data Act) enables US authorities to access data from US providers, even if they are stored in clouds outside the United States. The text of the law is available at https://www.congress.gov/bill/115th-congress/senate-bill/2383/text. Retrieved October 17, 2021.

[1185] Free translation of a statement within the article "E-Evidence – Outsourcing von Grundrechtsschutz" provided by Martin Schallbruch published in the CR-online-blog in May 2018, available at https://www.cr-online.de/blog/2018/05/10/e-evidence-outsourcing-von-grundrechtsschutz-teil-3/. Retrieved October 17, 2021.

[1186] Vanessa Franssen's article "The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement? has detailed background information on the proposal. It was published in October 2018 and is available at http://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/. Retrieved October 17, 2021.

[1187] Any provider is affected regard of its size, meaning that SMEs are also concerned.

[1188] EPOC is the abbreviation for "European Production Order Certificate" and is, like the "European Preservation Order Certificate" (EPOC-PR) one of the cooperation instruments implementing the principle of mutual recognition. Detailed background information on the proposal on electronic evidence can be found in LIBE's assessment of the draft which is available at http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf. Retrieved October 17, 2021.

[1189] Text of Article 9 (5) of the draft proposal.

[1190] Martin Schallbruch: E-Evidence – Outsourcing von Grundrechtsschutz. Article published May 2018, available at https://www.cr-online.de/blog/2018/05/10/e-evidence-outsourcing-von-grundrechtsschutz-teil-3/. Retrieved October 17, 2021.

this shift of responsibilities represents (part of) the next generation data protection framework,[1191] then such a development shall not be welcomed.

3. Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market

In early 2019, the European Parliament, the Council of the EU and the Commission agreed on new copyright rules[1192] in order to be fit for the digital era and bring tangible benefits to all creative sectors, such as the press, researchers or cultural heritage institutions as well as citizens.[1193] The proposal turns the established notice-and-takedown-principle on its head and introduces a new platform liability regime: service providers have to take certain efforts to ensure the unavailability of copyright protected work, and one of the solutions for this purpose are so-called upload filters. On the one hand, this sounds like a fair distribution of revenues from the online use of copyright works to the benefit of creators and publishers. On the other hand, this initiative faced a lot of criticism[1194] as it is feared that any such filtering might lead to censorship and a further strengthening of data monopolies. Smaller platforms, due to cost and efforts involved with the implementation of upload filters, will likely use centralized filtering mechanisms offered by third parties, i.e., companies which already invested time and money in corresponding technology. Some thus believe that, by requiring Internet platforms to perform automatic filtering all of the content that is uploaded by individuals, this may lead to a transformation of the Internet from an open platform into a tool for automated surveillance and control.[1195] Given the specific technology needed for such filters and owing to the fact that a large volume of data has to be processed, it seems likely that a huge part of the data traffic will run through the hands of a few large providers,[1196] which is why some fear that this would lead to the emergence of

[1191] For example, the German „Netzwerkdurchsetzungsgesetz" (network enforcement law) which was introduced 2017 imposes compliance rules and fines for providers of social network platforms and is criticized as some authors fear that it narrows the freedom of expression and that it may lead to censorship, see https://www.sueddeutsche.de/digital/netzwerkdurchsetzungsgesetz-beginnt-jetzt-das-grosse-loeschen-1.3809895-2. Retrieved October 17, 2021.

[1192] Source: Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0593:FIN. Retrieved October 17, 2021.

[1193] European Commission press release: http://europa.eu/rapid/press-release_IP-19-528_en.htm. Retrieved October 17, 2021.

[1194] An overview over the debate is provided by the Electronic Frontier Foundation, available at https://www.eff.org/de/deeplinks/2018/06/internet-luminaries-ring-alarm-eu-copyright-filtering-proposal. Retrieved October 17, 2021.

[1195] More than 70 Internet and computing luminaries including Tim Berners-Lee and co-founders of Mozilla, Wikipedia and many other have spoken out against this concrete provision. They wrote a joint letter to the president of the European Parliament, which is available at https://www.eff.org/files/2018/06/13/article13letter.pdf. Retrieved October 17, 2021.

[1196] Source: Interview with Ulrich Kelber, Germany's Federal Data Protection Commissioner, available at https://www.sueddeutsche.de/digital/ulrich-kelber-datenschutz-upload-filter-1.4366777. (Retrieved October 17, 2021). Ulrich Kelber therefore concludes that upload filters are "dangerous and wrong".

a data oligopoly.[1197] Another concern is that, because content filter technology is costly, small platforms might opt for data-for-service collaborations with Big Tech players in such a way that user data is offered in return for filtering services – an agreement that would probably be justified by the fact that a compliance requirement must be met. Finally, one further option has already been communicated by certain content-service-providers: the exclusion of European users with the help of so-called Geo-Blocking.[1198] Moreover, filters will have to be programmed in a manner to also take into consideration relevant specific legal exceptions such as quotations, criticism or parody[1199] in order to function properly. They will also be able to distinguish whether or not film material was used by a film critic, which is legal, or by a user attempting to illegally distribute the film, which is inadmissible. Either way – the collection of such meta-data leads to the fact that platforms using such filters would be considered controllers that process personal data.[1200] The question that arises in this context is the legality of such processing activities and the compatibility of centralized filtering mechanisms with the Charta of Fundamental rights. In line with the principle of proportionality laid down in Article 52 (1) of the Charta, the Regulation requires all legal obligations to be proportionate with respect to the legitimate aim which is pursued.[1201] But if one compares the filtering obligation under Article 17 (4b, c) of the Copyright Directive to existing CJEU case law with regard to fundamental rights as stipulated in Article 7 (the right to private life) and Article 8 (the right to protection of personal data) of the Charta, it is questionable whether the obligation to use upload filters meets the requirements of a balance between the right to intellectual property, the freedom to conduct business and the right to protection of personal data.[1202] In the famous Schrems decision,[1203] the CJEU stressed that legislation which grants public bodies generalized access to the content of communication violates both, the principle of proportionality and the right to private life. The CJEU concluded that "*legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter*." Due to the fact that the Copyright Directive

[1197] Intersoft Consulting Services: EU-Urheberrechtsreform: Upload-Filter und Datenschutz. Article published March18 2019, available at https://www.datenschutzbeauftragter-info.de/eu-urheberrechtsreform-upload-filter-und-datenschutz/. Retrieved October 17, 2021.

[1198] On March 8, 2019, the CEO of Twitch brought the exclusion of EU users into play. The corresponding news-release published April 3 2019 is available at https://www.golem.de/news/uploadfilter-twitch-erwaegt-ausschluss-von-eu-nutzern-1904-140416.html?utm_source=nl.2019-04-03.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter. Retrieved October 17, 2021.

[1199] Today's upload filter technology does not seem to be able to recognize parody, source: https://reform.communia-association.org/issue/upload-filters/. Retrieved October 17, 2021.

[1200] Malte Engeler: Copyright Directive – does the best effort principle comply with GDPR? Article published March 23 2019, available at https://www.telemedicus.info/copyright-directive-does-the-best-effort-principle-comply-with-gdpr/. Retrieved October 17, 2021.

[1201] GDPR Article 6 (3).

[1202] In his article, Malte Engeler argues that the filtering obligation in the Copyright Directive violates the Charta: Copyright Directive – does the best effort principle comply with GDPR? Article published March 23 2019, available at https://www.telemedicus.info/copyright-directive-does-the-best-effort-principle-comply-with-gdpr/. Retrieved October 17, 2021.

[1203] Recital 94 of the decision which is available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CJ0362&from=EN. Retrieved October 17, 2021.

would effectively require the processing of communication between a user and the platform, some therefore believe that this directive is in breach with freedom of expression and privacy.[1204] In addition, another problem is that the CJEU addressed public bodies, but the Copyright Directive takes private companies into duty, this way shifting the protection of individual freedoms to the private sector or, rather algorithms that shall have the capacity to decide upon the admissibility of uploading content.

4. Digital Services and Digital Markets Act

As part of the European Union's digital strategy, the European Commission published[1205] the Digital Services Act package which consists of the Digital Services Act (DSA) and the Digital Markets Act (DMA) in late 2020. DSA and DMA intend to regulate the provision of services over the Internet,[1206] the Digital Services Act and the Digital Markets Act have two main goals:[1207] "*to create a safer digital space in which the fundamental rights of all users of digital services are protected, and to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally*." The DSA applies to intermediary services offering network infrastructure such as Internet access providers and hosting (including cloud) services as well as online platforms and will replace the e-Commerce directive which was adopted in 2000.[1208] Since the DSA will modernize the e-Commerce Directive that many consider to be the "*backbone of EU's Internet legislation*",[1209] this initiative represents a major reform of European Internet regulations.[1210] Amongst other things, i.e. from a data subject perspective, the DSA introduces requirements such as enhanced online advertising transparency requirements, notice and action mechanisms, certain safeguards and the possibility to

[1204] Many claim that upload filters are not able to recognize existing legal exceptions and as a result: freedoms such as the right of quotation or parody, source: https://creativecommons.org/2017/02/22/copyright-filtering-mechanisms-dont-cant-respect-fair-use/. Retrieved October 17, 2021.

[1205] The corresponding press release "Europe fit for the Digital Age: Commission proposes new rules for digital platforms" was published December 15, 2020 and is available at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347. Retrieved October 17, 2021.

[1206] Vagelis Papakonstantinou, Paul de Hert: Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI. Article published April 1 2021, available at https://lsts.research.vub.be/en/20210401. Retrieved October 17, 2021.

[1207] The European Commission provides corresponding background information on their website: https://ec.europa.eu/digital-single-market/en/digital-services-act-package. Retrieved October 17, 2021.

[1208] Victor Timon, Helen Hart: EU plans changes to e-commerce and competition law. Arcticle published June 10 2020, available at https://www.lewissilkin.com/en/insights/eu-plans-changes-to-e-commerce-and-competition-law. Retrieved October 17, 2021.

[1209] Christoph Schmon for the Electronic Frontier Foundation (EFF): Our EU Policy Principles: Platform Liability. Article published July 9 2020, available at https://www.eff.org/deeplinks/2020/07/effs-eu-policy-principles-platform-liability-and-monitoring. Retrieved October 17, 2021.

[1210] Christoph Schmon, Karen Gullo for the Electronic Frontier Foundation (EFF): Euopean's Commission proposed Digital Services Act, got several things right, but improvements are necessary to put users in control. Article published December 15 2020, available at https://www.eff.org/deeplinks/2020/12/european-commissions-proposed-regulations-require-platforms-let-users-appeal. Retrieved October 17, 2021.

challenge platforms' content moderation decisions.[1211] The European Data Protection Supervisor welcomed the initiative but at the same time stressed the importance of protecting individuals, for example from targeted online advertising or from automated decision making and profiling in the framework of so-called recommender systems;[1212] the EDPS also underlined the relevance of a co-operation between relevant authorities. The DMA applies to organizations which qualify as so-called "*gatekeepers*", for example search engines and social networks and aims at ensuring a higher degree of competition and a fairer business environment.[1213] From a privacy perspective, the DMA will require gatekeepers to refrain from unfair behaviors such as blocking users from uninstalling any pre-installed software or apps or restricting users from accessing services that may have been acquired outside of the gatekeeper's platform.[1214] The EDPS underlined that the DMA should enhance consent mechanisms, clarify the scope of the data portability obligation, consider effective anonymization, and introduce (minimum) interoperability standards,[1215] and once again called for a structured approach between all authorities responsible for compliance with the DSA, DMA as well as other applicable regulations. The DMA foresees the creation of a Digital Markets Advisory Committee[1216], and the DSA provides for the establishment of a European Board for Digital Services,[1217] meaning that new bodies are created at EU level.

5. Data Governance Act

The draft Data Governance Act (DGA) focuses on the availability and sharing of data by allowing for re-use of data, by establishing providers of data sharing services as trusted (i.e. neutral) intermediaries, and by creating a European Data Innovation Board to ensure consistent practice and facilitate cooperation between the competent authorities.[1218] The DGA has been designed to be fully compliant

[1211] The European Commission explains DSA requirements at their website, which is available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en. Retrieved October 17, 2021.

[1212] EDPS press release from February 10 2021, available at https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opinions-digital-services-act-and-digital_en. Retrieved October 17, 2021.

[1213] DMA requirements are summarized on the European Commission's website, which is available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en. Retrieved October 17, 2021.

[1214] The law firm of Hunton Andrews Kurth commented on the DMA in their 2021 blog post: EDPS Publishes Opinion on Digital Services Act and Digital Markets Act. Article published February 17 2021, available at https://www.huntonprivacyblog.com/2021/02/17/edps-publishes-opinion-on-digital-services-act-and-digital-markets-act/. Retrieved October 17, 2021.

[1215] The text of EDPS' opinion on the Proposal for a Digital Markets Act (Opinion2/2021) is available at https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf.

[1216] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en. Retrieved October 17, 2021.

[1217] Source: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en. Retrieved October 17, 2021.

[1218] Background information on the Data Governance Act is provided by the law firm Hunton Andrews Kurth in their 2020 blog post from December 2 2020: European Commission Publishes Draft Data Governance Act, which is available at https://www.huntonprivacyblog.com/2020/12/02/european-commission-publishes-draft-data-governance-act/. Retrieved October 17, 2021.

to GDPR, however, the challenge already starts with terminology[1219]: under the DGA, data means any digital representation of acts, facts or information and any compilation of the same, including sound as well as visual or audiovisual recording. In addition, the DGA uses a novel (unique) set of terms, for example "*data holder*" and "*data user*" which is different from the terminology used in the General Data Protection Regulation.[1220] The DGA moreover introduces the idea of data altruism to make data available for altruistic purposes[1221], and it is questionable whether this truly matches GDPR's requirements with regards to purpose limitation, transparency and consent as well as rules on compatible re-use of personal information or existing privileges for research purposes. In this context, the European Data Protection Supervisor and the European Data Protection Board adopted a joint opinion on the DGA[1222] in which they recommend aligning the DGA with present (GDPR) rules on the protection of personal data to ensure that the level of protection of individuals' personal data is not affected, and that obligations set out in applicable data protection legislation are not altered. They furthermore suggest to clarify the data altruism purposes and to define compatible purposes for which further processing of personal information may be lawful. In light of possible risks for data subjects related to the processing of their data by data sharing service providers or data altruism organizations, the EDPS and the EDPS consider that envisaged requirements for these entities are not sufficient; the EDPS and the EDPS therefore recommends exploring alternatives such as codes of conduct or a certification mechanisms.[1223] Finally, it should also be noted that, despite the fact that the European Commission addresses the issue of data localization requirements in their Q&As on the Data Governance Act,[1224] some authors claim that the EU is about to violate international law: under its World Trade Organization commitments, the EU must allow access to its market to data processing from abroad.[1225] The Data Governance Act foresees the establishment of a European Data Innovation

[1219] The text of the Data Governance Act is available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:767:FIN. Retrieved October 17, 2021.

[1220] Vagelis Papakonstantinou, Paul de Hert: Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI. Article published April 1 2021, available at https://lsts.research.vub.be/en/20210401. Retrieved October 17, 2021.

[1221] Stephanie Lopes: Key insights from the leaked EU Data Governance Act. Article published November 6 2020, available at https://digitalbusiness.law/2020/11/key-insights-from-the-leaked-eu-data-governance-act/. Retrieved October 17, 2021.

[1222] EDPB's and EDPS' joint opinion on the Data Governance Act was published March 10, 2021 on EDPB's website and is available at https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinion-data-governance-act-dga_en. Retrieved October 17, 2021.

[1223] EDPB's and EDPS' joint opinion on the Data Governance Act was published March 10, 2021 on EDPB's website and is available at https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinion-data-governance-act-dga_en. Retrieved October 17, 2021.

[1224] Regulation on data governance – Questions and Answers published November 25 2020, available at https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2103#Data%20sharing. Retrieved October 17, 2021.

[1225] Vincent Manancourt, Melissa Heikkilä: Legal experts: EU data proposals break international law. Article published November 4 2020, available at https://www.politico.eu/article/legal-experts-eu-data-proposals-break-international-law/. Retrieved October 17, 2021.

Board,[1226] together with the two other bodies foreseen by the DSA and the DMA, and this altogether creates three new oversight bodies. As much as oversight, enforcement and governance shall be welcomed, this results a multiplicity of supervisors on top of national data protection, consumer protection and competition regulatory agencies – as well as courts[1227] that deal with individual claims[1228] or competition[1229] or antitrust cases.[1230]

6. Data Act

In 2020, the European Commission proposed the Data Governance Act as part of the European Strategy for data,[1231] and the Data Act is a follow up on that proposal with the objective "*to propose measures to create a fair data economy by ensuring access to and use of data, including in business-to-business and business-to-government situations.*"[1232] The public consultation on the Data Act is currently open,[1233] and the European Commission stresses that "*the initiative would not alter data protection legislation and would seek to preserve incentives in data generation. Under this initiative, a review of Directive 96/9/EC on the legal protection of databases is also planned in order to ensure continued relevance for the data economy*."[1234] The proposed Data Act wants to encourage sharing of data – including non-personal information[1235] – to realize the full potential of EU's data economy by:[1236] promoting fairness (i.e. ensuring fair distribution of usage rights along the value chain; identifying contractual unfairness where there is unequal bargaining power compromising competition), by enabling for greater legal certainty (i.e. safeguarding intellectual property rights; clarifying if database rights can cover machine-generated data; ensuring that the rights under the

[1226] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767. Retrieved October 17, 2021.

[1227] To quote Politico: Have a GDPR complaint? Skip the regulator and take it to court, source: https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/. Retrieved October 17, 2021.

[1228] Lars Lensdorf, Robert Henrici, Moritz Hüsch, Nicholas Shepherd: A New Day for GDPR Damages Claims in Germany? Article published February 25 2021, available at https://www.insideprivacy.com/data-privacy/a-new-day-for-gdpr-damages-claims-in-germany/. Retrieved October 17, 2021.

[1229] Daniel Heymann: DSGVO und UWG – Wettbewerbsrecht und Datenschutz. Article published July 26 2019, available at https://www.petersenhardrahtpruggmayer.de/de/news/dsgvo-und-uwg-wettbewerbsrecht-und-datenschutz/. Retrieved October 17, 2021.

[1230] Eva Witzleb, Pascal Schumacher: Datenschutz vs. Kartellrecht - Die nächste Runde. Article published May 6 2021, available at https://www.noerr.com/de/newsroom/news/datenschutz-vs-kartellrecht.

[1231] Source: https://digital-strategy.ec.europa.eu/en/policies/strategy-data. Retrieved October 17, 2021.

[1232] Source: https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-data-act. Retrieved October 17, 2021.

[1233] Source: https://data.europa.eu/en/news/public-consultation-data-act. Retrieved October 17, 2021.

[1234] Background information on the Data Act is provided on the European Commission's homepage: https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-data-act. Retrieved October 17, 2021.

[1235] Trisha Jalan: European Commission proposes Data Act 2021 to increase data sharing between businesses and governments. Article published February 21 2020, available at https://www.medianama.com/2020/02/223-european-commission-data-sharing/. Retrieved October 17, 2021.

[1236] Seiko Hidaka: EU's possible Data Act: What can we anticipate from the Inception Impact Assessment and the Consultation? Article published July 5 2021, available at https://www.dataprotectionreport.com/2021/07/eus-possible-data-act-what-can-we-anticipate-from-the-inception-impact-assessment-and-the-consultation/. Retrieved October 17, 2021.

Database Directive do not impede cross-border data flows and data sharing), and by ensuring portability (i.e. introducing (mandatory?) interoperability requirements in order to allow for easy switching of providers without contractual, technical and/or economic barriers. This legal initiative would thus allow for addressing the following problems that limit data sharing at present: lack of legal clarity, lack of economic incentives, lack of trust and fear of misappropriation by third parties and imbalances in negotiating power.[1237] In the context of data economy, the proposed Data Act would furthermore need to be coordinated with other legislative measures, such as intellectual property rights or trade secrets.[1238] At present, the specific content of the Data Act is still largely open. In particular, the specific formulation of the individual proposed claims and obligations still requires considerable detailed work.[1239]

7. Machinery Regulation

The proposal for a regulation of the European Parliament and of the Council on machinery products (Machinery Regulation) has been published in April 2021[1240] and shall replace the current Machinery Directive[1241] which, amongst other things, is about the protection of workers and citizens.[1242] The Machinery Directive was thus concerned with safety and health, and the Machinery Regulation is intended to complement the draft AI Regulation:[1243] while the AI-relevant draft addresses risks of AI systems, the draft of a new Machinery Regulation seeks to ensure the safe integration of AI systems into machinery products such as robots or industrial production lines to safeguard users and

[1237] Seiko Hidaka: EU's possible Data Act: What can we anticipate from the Inception Impact Assessment and the Consultation? Article published July 5 2021, available at https://www.dataprotectionreport.com/2021/07/eus-possible-data-act-what-can-we-anticipate-from-the-inception-impact-assessment-and-the-consultation/. Retrieved October 17, 2021.

[1238] Europe's Commissioner for the Internal Market, Thierry Breton said that "*The Data Act will unlock vast troves of industrial data and contribute to the emergence of a sovereign single market for data. European data, in particular industrial data, needs to be shared, stored and processed in line with European rules such as data protection, respect of intellectual property and trade secrets*." Source: https://data.europa.eu/en/news/public-consultation-data-act. Retrieved October 17, 2021.

[1239] Torsten Kraul, Max von Schönfeld, Marvin Bartels: Europäische Datenstrategie: EU-Kommission veröffentlicht Folgenabschätzung zum Data Act. Article published June 24 2021, available at https://www.noerr.com/de/newsroom/news/europaische-datenstrategie-eu-kommission-veroffentlicht-folgenabschatzung-zum-data-act?etcc_cmp=Noerr_news+072021&etcc_med=Newsletter. Retrieved October 17, 2021.

[1240] The text of the Machinery Regulation is available at https://beta.op.europa.eu/en/publication-detail/-/publication/1f0f10ee-a364-11eb-9585-01aa75ed71a1. Retrieved October 17, 2021.

[1241] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (Machinery Directive), source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0042#:~:text=%20Text%20%201%20Where%20a%20Member%20State,concerned%20without%20delay.%0AThe%20Commission%20shall%20consider%2C...%20More%20. Retrieved October 17, 2021.

[1242] The European Commission provides background on EU's machinery legislation at their website: https://ec.europa.eu/growth/sectors/mechanical-engineering/machinery_en. Retrieved October 17, 2021.

[1243] The European Commission's press release on new rules on AI: Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence was published on April 21 2021 and is available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682. Retrieved October 17, 2021.

consumers. The Machinery Regulation also seeks to provide more legal clarity and at the same time, reduce manufacturers' administrative and financial burden as companies would only need to undertake one conformity assessment for both the AI Regulation and the Machinery Regulation.[1244]

8. Proposal for a renewed NIS Directive

Only two years after its implementation, the EU Commission proposed[1245] an update of the Directive on Security of Network and Information Systems, also known as “NIS2 Directive”. Like the present Directive on Security of Network and Information Systems, the new NIS2 Directive aims at strengthening security requirements, but it also aims at streamlining reporting obligations and introduces more stringent supervisory measures and stricter enforcement requirements, including harmonized sanctions across the EU, and furthermore addresses the management of supply chains risks.[1246] The current NIS Directive[1247] (also known as the Cyber-security Directive) applies to operators of essential services such as water supply or energy as well as digital service providers, including providers of cloud computing services and online services. The present NIS Directive has been criticized for its scope and application,[1248] and the proposed NIS2 Directive takes up this criticism and does not distinguish between operators of essential services and digital service providers: it expands the scope of the present Directive by adding new sectors in accordance with their criticality for the economy and society. Cloud service providers are now categorized as essential entities, which is a major change and adds to the fact that the use of cloud computing for Big Data and AI is governed by many data privacy and security laws. Moreover, fines of up to 10 million Euro or 2 % of the total worldwide turnover (whichever is higher) are foreseen, and non-compliant entities risk that their relevant authorizations are suspended or have senior management suspended from exercising managerial functions.[1249]

[1244] The European Commission published questions and answers on new rules on AI on April 21 2021 press release: New rules for Artificial Intelligence – Questions and Answers, which https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683#3. Retrieved October 17, 2021.

[1245] Background information provided by the European Commission at https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union. Retrieved October 17, 2021.

[1246] Background information is provided by the European Parliamentary Research Blog by Mar Negreiro: The NIS2 Directive: A high common level of cybersecurity in the EU. Article published February 22 2021, available at https://epthinktank.eu/2021/02/22/the-nis2-directive-a-high-common-level-of-cybersecurity-in-the-eu-eu-legislation-in-progress/. Retrieved October 17, 2021.

[1247] Text of the Directive on Security of Network and Information Systems available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC. Retrieved October 17, 2021.

[1248] Matthew Buckwell: EU Commission Proposes to Update the NIS/Cybersecurity Directive Only Two Years After Implementation. Article published January 2021, available at https://www.twobirds.com/en/news/articles/2021/global/eu-commission-proposes-to-update-the-nis-cybersecurity-directive-only-two-years-after-implementation. Retrieved October 17, 2021.

[1249] Thomas Declerck: New EU Cybersecurity Strategy: European Commission Accelerates Push for EU to Lead in Cybersecurity Regulation. Article published December 24 2020, available at

9. Proposal for a Directive on the resilience of critical entities

The proposed NIS2 Directive should not be seen in isolation, but in the context[1250] of other initiatives to enhance the resilience of critical systems, and for which the European Union established the European Program for Critical Infrastructure Protection (EPCIP) already in 2006[1251] with the overall goal to increase the level of security and decrease the number and severity of incidents including data breaches. Consequently, the European Commission proposed another directive to replace the current Critical Infrastructure Directive,[1252] the Directive on the resilience of critical entities:[1253] under this directive EU member states must, among other things, designate authorities, identify nationally critical infrastructures and services and evaluate their vital functions which are in scope of the directive; critical entities would be subject to specific oversight and would have to implement appropriate technical and organizational measures and conduct risk assessments.[1254]

10. 5G Security and Internet of Secure Things

As part of their cyber-security strategy, the European Union is also dealing with IoT and 5G, which many believe to be "the next big thing" despite increased infrastructure cost: this future mobile network will allow for better performance by processing a much higher volume of data and by connecting more devices to a single source,[1255] and connectivity and capacity are key to Big Data applications. This initiative shows that the EU wants to lead efforts for a secure digitalization[1256] and that there is awareness of the importance of security and resilience of IoT and investment in trustworthy digital technologies: this is truly needed since the number of cyber-attacks continues to

https://www.jdsupra.com/legalnews/new-eu-cybersecurity-strategy-european-47823/. Retrieved October 17, 2021.

[1250] Background information is provided by the European Commission's in their roadmap and impact assessment information which was published June 25 2020, available at: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/06/090166e5d0c95543-1.pdf. Retrieved October 17, 2021.

[1251] The Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection is available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33260&from=EN. Retrieved October 17, 2021.

[1252] The text of the current European Critical Infrastructure Directive is available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF. Retrieved October 17, 2021.

[1253] Text of the proposed Directive on the resilience of critical entities is available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_impact_assessment_swd-2020-358_en.pdf. Retrieved October 17, 2021.

[1254] Further details are provided on the European Commission's homepage: the corresponding press release was published December 16 2020, and is available at https://ec.europa.eu/home-affairs/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential_en. Retrieved October 17, 2021.

[1255] Rohith Bhaskar: 5G: Why is it the next big thing? Article published February 22 2021, available at https://www.moneycontrol.com/news/technology/5g-why-is-it-the-next-big-thing-6555881.html. Retrieved October 17, 2021.

[1256] Thomas Declerck: New EU Cybersecurity Strategy: European Commission Accelerates Push for EU to Lead in Cybersecurity Regulation. Article published December 24 2020, available at https://www.jdsupra.com/legalnews/new-eu-cybersecurity-strategy-european-47823/. Retrieved October 17, 2021.

rise and because society's digital transformation has been intensified by the recent COVID-19 crisis.[1257]

11. Proposal for a review of the Directive on the re-use of public sector information

In the framework of Big Data discussions and the use of artificial intelligence in Industry 4.0, people tend to forget that not only Big Tech companies are data-driven; truth is, the public sector is one of the most data-intensive sectors. This erroneous perception is confirmed by the fact that this proposal attracted much less attention in contrast to the proposal for a copyright reform. The reason for this new proposal was the intention to create a "common data space"[1258] within the European Union, and consequently, the European Commission adopted a new proposal[1259] for a revision of the PSI Directive. This proposal aims to overcome existent (market entry) barriers which prevent the re-use of public sector information, especially for data which are generated by utilities and the transport sector as well as research data resulting from public funding. Such (real-time) data has tremendous re-use potential, and that is particularly true for dynamic data since this type of data is believed to be one of the most commercially valuable types of data.[1260] Due to the fact that the proposal suggests a full re-use of public sector information, it is questionable how this relates to the principle of purpose limitation GDPR sets forth. The protection of personal data is recognized as a fundamental right and therefore, it cannot be simply overruled. But the proposal addresses this problem as it provides for an exception to the scope of the PSI Directive for reasons relating to the protection of personal data.[1261] However, problems may arise given that other terms are used[1262] and because definitions of terms are not the same.[1263] It was moreover suggested to introduce mandatory data protection impact assessments for specific sectors dealing with sensitive data such as the health sector which take the conditions for re-use into account.[1264] Even though further developments have to be awaited, it seems already clear at this stage that certain (foreseeable) challenges prevail in the context of re-use of public

[1257] Information on EU's cyber-security strategy is available at the European Commission's website at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy. Retrieved October 17, 2021.

[1258] Background information provided by the European Commission on their website, available at https://ec.europa.eu/digital-single-market/en/proposal-revision-public-sector-information-psi-directive. Retrieved October 17, 2021.

[1259] Source: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0234:FIN. Retrieved October 17, 2021.

[1260] Statement by the European Commission on their website, available at https://ec.europa.eu/digital-single-market/en/proposal-revision-public-sector-information-psi-directive. Retrieved October 17, 2021.

[1261] See article 1 (2 g) of the PSI proposal.

[1262] For instance, the term document. GDPR does not address documents, but personal data.

[1263] EDPS opinion 5/2018 on the proposal for a Directive on the re-use of Public Sector Information (PSI), p. 11 available at https://edps.europa.eu/sites/edp/files/publication/2018-0246_psi_directive_opinion_en_de.pdf. Retrieved October 17, 2021.

[1264] EDPS opinion 5/2018 on the proposal for a Directive on the re-use of Public Sector Information (PSI), p. 13 available at https://edps.europa.eu/sites/edp/files/publication/2018-0246_psi_directive_opinion_en_de.pdf. Retrieved October 17, 2021.

sector information, for example, the potential weakening of purpose limitation and the risk of loss of transparency.

12. Proposal for an Artificial Intelligence Act

Following their above-mentioned white paper on AI and a public consultation period, the European Commission published its proposal for a regulation[1265] on a European approach for Artificial Intelligence in early 2021:[1266] "*The Commission is proposing the first ever legal framework on AI which addresses the risks of AI and positions Europe to play a leading role globally*." These landmark rules are an ambitious attempt to regulate AI and represent a major step towards a comprehensive legal framework for Artificial Intelligence, setting out a cross-sectoral regulatory approach for the use of AI with the aim to pave a way to both, ethical use of AI technologies and ensuring that the EU remains competitive in this regard.[1267] It is important to note that the new regulation shall not replace existing rules; the Commission stresses that the present legal framework however should be improved.[1268] As any regulation, the rules would apply directly with no need for further implementation at member state level, and this shows that the Commission wants to establish consistent rules for AI and improve legal certainty. However, the fact that the regulation will have to pass the European Parliament and the European Council makes it likely that there will be adjustments, also because various stakeholders' standpoints and interests on such a complex topic as AI will have to be considered; another factor to consider is that the regulation will come into force 24 months after it has been adopted, it is questionable whether some of the provisions will be overtaken by technological progress before they even apply, meaning that the regulation, or parts thereof, would perhaps not be future-proof.[1269] The Artificial Intelligence Act defines AI as: "*any software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs, such as content, predictions, recommendations, or decisions influencing the environments they interact with*." This definition can be questioned from a technical point of view,[1270] and there is no agreed definition of AI amongst experts in industry or law, there are only common

[1265] If adopted by the European Parliament and Council, the Artificial Intelligence Act would apply directly across the EU.

[1266] Source: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence. Retrieved October 22, 2021.

[1267] See the Commission's press release which was published April 21 2021 and is available at https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682. Retrieved October 22, 2021.

[1268] Brahim Benichou, Jan De Bruyne, Thomas Gils, Ellen Wauters: Regulating AI in the European Union: Seven Key Takeaways. Article published February 25 2020, available at https://ai-laws.org/2020/02/regulating-ai-in-the-european-union-seven-key-takeaways/. Retrieved October 22, 2021.

[1269] Jetty Tielemans: A look at what's in the EU's newly proposed regulation on AI. Article published April 21 2021, available at https://iapp.org/news/a/a-look-at-whats-in-the-eus-newly-proposed-regulation-on-ai/. Retrieved October 22, 2021.

[1270] Jay Modrall: EU proposes new Artificial Intelligence Regulation. Article published April 16 2021, available at https://www.nortonrosefulbright.com/en/knowledge/publications/fdfc4c27/eu-to-propose-new-artificial-intelligence-regulation. Retrieved October 22, 2021.

elements in various definitions (such as digital, technology, learning, reasoning),[1271] and another factor to consider is the dual-use characteristics of AI: as much as AI can serve the good, it can also serve the bad.[1272] It also must not be forgotten that what was considered AI ten years ago might not be considered AI today. This broad definition is intended to determine the scope of regulation and to be technology-neutral and as future-proof as possible[1273], but that also means that software which is traditionally not necessarily classified as AI would be covered by the new regulation. The extent to which the terms "software", "AI system", etc. currently proposed in the AI Regulation can be further clarified is likely to be of crucial importance to the success of the AI Regulation Act since this will reduce remaining ambiguities.[1274] Moreover, just like GDPR, the Artificial Intelligence Act will apply to the private and public sector, and more importantly, the draft AI Regulation intends to capture "*all parties involved in the AI value chain*,"[1275] that is:

- Providers (i.e., entity / person that develops or has an AI system developed) who place AI systems on the EU market or put them into service in the EU irrespective of whether they are established within the EU. (…) Where the provider is not established in the EU and where an importer cannot be identified, an authorized representative in the EU must be appointed,
- Users of AI systems (i.e., the entity / person using an AI system) established in the EU – except where the AI system is used in the course of a personal non-professional activity,
- Providers and users of AI systems established outside the EU where the output produced by the AI system is used in the EU,[1276]
- Manufacturers of products are covered and are responsible for compliance as if they were the provider of the high-risk AI system,
- Distributors, importers, users and other third parties will also be subject to providers' obligations if they place a high-risk AI system on the market or into service under their name

[1271] Valerie Thomas: Report on Artificial Intelligence on behalf of the Regulatory Institute, Part I: The existing regulatory landscape. Article published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/. Retrieved October 22, 2021.

[1272] Miles Brundage et al: The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Article published February 2018, available at https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217. Retrieved October 22, 2021.

[1273] Keily Blair, James Hall, Christian Schröder, Heather Sussman, Shannon Yarovsky: The new EU approach to the regulation of Artificial Intelligence. Article published May 10 2021, available at https://www.jdsupra.com/legalnews/the-new-eu-approach-to-the-regulation-4438826/. Retrieved October 22, 2021.

[1274] Jens Peter Schmidt: European Commission proposes world's first ever regulatory framework on Artificial Intelligence. Article published March 23 2021, available at https://www.noerr.com/en/newsroom/news/european-commission-proposes-worlds-first-ever-regulatory-framework-on-artificial-intelligence-ai. Retrieved October 22, 2021.

[1275] Jay Modrall: EU proposes new Artificial Intelligence Regulation. Article published April 16 2021, available at https://www.nortonrosefulbright.com/en/knowledge/publications/fdfc4c27/eu-to-propose-new-artificial-intelligence-regulation. Retrieved October 22, 2021.

[1276] William Long, Francesca Blythe, Lauren Cuyvers, Monika Zdzieborska: EU Commission Issues Draft AI Regulation. Article published April 23 2021, available at https://datamatters.sidley.com/eu-commission-issues-draft-ai-regulation. Retrieved October 22, 2021.

> or trademark, modify the intended purpose of a high-risk AI system already on the market or in service or make a substantial modification to a high-risk AI system. In that case, the original provider is relieved of responsibility."[1277]

The implications that come with further terminology and definitions should not be underestimated: there are voices that say that, once all of EU's legal initiatives enter into force, one and the same company could be both, "controller" and "processor" under GDPR, "data holder" under the DGA and "distributor" under the AI regulation, meaning that consistency would be substantially hampered.[1278] Like GDPR, Article 71 of the new regulation allows for high fines of up to 30,000,000 Euro or of up to 6% of total annual worldwide turnover, whichever is higher, depending on the type of violation: the highest fines will apply to infringements on prohibited practices, medium-range fines are foreseen for non-compliance, and the lowest fines apply to the supply of incorrect, incomplete or misleading information to notified bodies and competent authorities. Unlike the GDPR, the draft regulation does not provide for a right to compensation, which, on the one hand, may provide comfort. On the other hand, that does not mean that a private right of action is not given if the conditions of GDPR Art. 82 are met. Like the GDPR, the Artificial Intelligence Act will have extraterritorial effect, the regulation will apply to users of AI systems located within the EU as well as providers and users of AI systems located outside the EU where the output is used in the EU and providers which place on the market or put into service AI systems in the EU regardless of where they are located.[1279] This may lead to the so-called "Brussels-effect"[1280] which guides the way companies are doing business, because multinational organizations would adjust their global operations to EU standards to be compliant. Apart from the extraterritorial scope and high fines, various other provisions of the regulation echo the GDPR, for example the fact that the Artificial Intelligence Act foresees for incident notifications or the fact that certain accountability, documentation and enforcement provisions apply:[1281] as for the latter, the Commission's proposal foresees for the creation of the European AI Board that would be entrusted with various tasks such as sharing of best practices, ensuring consistent application and harmonized

[1277] Jay Modrall: EU proposes new Artificial Intelligence Regulation. Article published April 16 2021, available at https://www.nortonrosefulbright.com/en/knowledge/publications/fdfc4c27/eu-to-propose-new-artificial-intelligence-regulation. Retrieved October 22, 2021.

[1278] Vagelis Papakonstantinou, Paul de Hert: Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI. Article published April 1 2021, available https://lsts.research.vub.be/en/20210401. Retrieved October 22, 2021.

[1279] Keily Blair, James Hall, Christian Schröder, Heather Sussman, Shannon Yarovsky: The new EU approach to the regulation of Artificial Intelligence. Article published May 10 2021, available at https://www.jdsupra.com/legalnews/the-new-eu-approach-to-the-regulation-4438826/. Retrieved October 22, 2021.

[1280] Anu Bradford: The Brussels Effect - How the European Union Rules the World, Oxford University Press 2020.

[1281] Diletta De Cicco, Charles-Albert Helleputte: The EU Artificial Intelligence Act, paper prepared on behalf of Steptoe in May 2021, available at https://www.steptoeinternationalcomplianceblog.com/files/2021/05/AI_Infographic-1.pdf. Retrieved October 22, 2021.

implementation of the regulation and issuance of opinions and recommendations.[1282] It is important to note that the Board will be complemented by a public database of all stand-alone high risk AI systems: this is an interesting development many welcome as it represents a new dimension of transparency[1283] different from mere information obligations under GDPR that can typically be described as one-time efforts addressed to data subjects as opposed to official bodies.

The regulation is the first piece of legislation that is solely focused on Artificial Intelligence, i.e. identification, classification, documentation and monitoring of AI with a specific emphasis on high risk AI. Even though the proposal does not define high risk, the proposal provides for criteria[1284] to be used to determine whether a system shall be classified as a high-risk application of AI, and the draft regulation also explains that risk shall be interpreted in line with existing product safety legislation. Content and structure of the proposal can be described as follows:[1285] first, the scope of the new proposed rules is defined; second, the draft proposal explains which AI systems are considered unacceptable, for example due to violation of fundamental rights. Title III of the draft contains specific rules for high-risk AI systems. Title IV of the draft AI Act is concerned with transparency obligations for systems that interact with humans; title V explains the objective of the creation of an innovation-friendly legal framework, which demonstrates that the European Commission is aware of the potential of Artificial Intelligence. Title VI is about governance; title VII addresses the work of the Commission and national authorities. Title VIII and IX set forth reporting obligations for AI providers and promote the voluntary application of requirements that are applicable to high-risk systems to providers of non-high-risk AI systems. Finally, title XII foresees that the Commission regularly evaluates the need for a revision of Annex III and prepares regular reports on the review of the regulation.[1286] In the explanatory memorandum within the draft proposal of the Artificial Intelligence Act, the Commission explains that the European Commission "*puts forward the proposed regulatory framework on Artificial Intelligence with the following specific objectives:*

[1282] Keily Blair, James Hall, Christian Schröder, Heather Sussman, Shannon Yarovsky: The new EU approach to the regulation of Artificial Intelligence. Article published May 10 2021, available at https://www.jdsupra.com/legalnews/the-new-eu-approach-to-the-regulation-4438826/. Retrieved October 22, 2021.

[1283] Friederike Reinhold, Angela Müller for AlgorithmWatch: AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence – A major step with major gaps. Article published April 22 2021. AlgorithmWatch's response is available at https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/. Retrieved October 22, 2021.

[1284] Jetty Tielemans: A look at what's in the EU's newly proposed regulation on AI. Article published April 21 2021, available at https://iapp.org/news/a/a-look-at-whats-in-the-eus-newly-proposed-regulation-on-ai/. Retrieved October 22, 2021.

[1285] Nikita Lukianets: A (more) visual guide to the proposed EU Artificial Intelligence Act. Article published May 3 2021, available at https://futurium.ec.europa.eu/en/european-ai-alliance/open-discussion/more-visual-guide-proposed-eu-artificial-intelligence-act. Retrieved October 22, 2021.

[1286] Nikita Lukianets: A (more) visual guide to the proposed EU Artificial Intelligence Act. Article published May 3 2021, available at https://futurium.ec.europa.eu/en/european-ai-alliance/open-discussion/more-visual-guide-proposed-eu-artificial-intelligence-act. Retrieved October 22, 2021.

- *Ensure that AI systems placed on the Union market are safe and respect existing law on fundamental rights and Union values;*
- *Ensure legal certainty to facilitate investment and innovation in AI;*
- *Enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;*
- *Facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation."*

The Artificial Intelligence Act thus wants to balance between protecting individuals and allowing for technological innovation[1287] based on balancing of risk. Unlike the low risk vs. high risk approach that was discussed in the Commission's 2020 White Paper on AI, the regulation differentiates between various levels of potential risks posed by AI: the Artificial Intelligence Act sets forth a four-tiered risk framework that recognizes the varying levels of risk posed by AI systems to one's health, safety, and/or fundamental rights and sets out proportionate requirements and obligations per risk level; in accordance with possible risks, each tier aims to set adequate requirements for providers and users of AI applications.[1288] The proposal starts with listing types of AI practices that are prohibited:[1289]

1. *"Placing on the market, putting into service or using an AI system that deploys subliminal techniques beyond a person's consciousness to materially distort a person's behavior in a manner that causes that person or another person physical or psychological harm.*
2. *Placing on the market, putting into service or using an AI system that exploits vulnerabilities of a specific group of persons due to their age, physical or mental disability to materially distort the behavior of a person pertaining to the group in a manner that causes that person or another person physical or psychological harm.*
3. *Placing on the market, putting into service or using an AI system by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons with the social score leading to detrimental or unfavorable treatment that is either unrelated to the contexts in which the data was originally generated or unjustified or disproportionate.*
4. *Use of "real-time" remote biometric identification (read: facial recognition) systems in publicly accessible spaces for law enforcement purposes, subject however to broad*

[1287] Jamie Humphreys, Edward Turtle: European Parliament publishes its proposals for new AI laws. Article published October 28 2020, available at https://products.cooley.com/2020/10/28/regulating-ai-eu-proposes-legal-framework-for-artificial-intelligence/. Retrieved October 22, 2021.

[1288] Cailean Osborne: The European Commission's Artificial Intelligence Act highlights the need for an effective AI assurance ecosystem. Article for the Centre for Data Ethics and Innovation published May 11 2021, available at https://cdei.blog.gov.uk/2021/05/11/the-european-commissions-artificial-intelligence-act-highlights-the-need-for-an-effective-ai-assurance-ecosystem/. Retrieved October 22, 2021.

[1289] Jens Peter Schmidt: European Commission proposes world's first ever regulatory framework on Artificial Intelligence. Article published March 23 2021, available at https://www.noerr.com/en/newsroom/news/european-commission-proposes-worlds-first-ever-regulatory-framework-on-artificial-intelligence-ai. Retrieved October 22, 2021.

> *exemptions that, in turn, are subject to additional requirements, including prior authorization for each individual use to be granted by a judicial authority or an independent administrative body in the member state where the system is used*."

It is foreseeable that the latter point will lead to controversial discussion: fighting crimes is an argument that is regularly used in the context of technologies like video surveillance and more sophisticated techniques like (real-time) facial recognition, however, this needs to be balanced against individuals' fundamental rights and freedoms. The European Data Protection Supervisor commented on the Artificial Intelligence Act that this is a welcomed initiative, but that ban on remote biometric identification in public space – a provision which was included in a previous leaked version of the regulation[1290] – is necessary.[1291] Moreover, this particular section of the draft has numerous exceptions, for example, targeted search for victims and prevention, detection, localization or prosecution of certain crimes.[1292] In addition, the draft does not cover other purposes (e.g. non-law-enforcement), other uses (e.g. non-publicly accessible spaces) or other players (e.g. private sector uses of biometric identification technologies), which leads to legal uncertainty in relation to other existing laws, namely GDPR and the Law Enforcement Directive as well as national laws.[1293] Finally, the example of Clearview AI, which is an app developed by a private company that allows to identify individuals based on a single picture, shows how controversial the discussion around the use of biometric information is when it comes to data protection: Clearview's technology has been used by police in many countries (e.g. Australia[1294]), but at the same time, data protection supervisory authorities in several countries including the United Kingdom, France, Italy, Greece and Austria are dealing with complaints[1295] or already issued fines (e.g. Sweden)[1296] or ordered the (partial) deletion of individual's

[1290] AccessNow: Europe's approach to artificial intelligence: how AI strategy is evolving. Report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf. Retrieved October 22, 2021.

[1291] EDPS press release: Artificial Intelligence Act: a welcomed initiative but ban on remote biometric identification in public space is necessary, published April 23 2021, available at https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en#:~:text=The%20European%20Commission%E2%80%99s%20legislative%20proposal%20for%20an%20Artificial,according%20to%20the%20EU%E2%80%99s%20values%20and%20legal%20principles. Retrieved October 22, 2021.

[1292] Diletta De Cicco, Charles-Albert Helleputte: The EU Artificial Intelligence Act, paper prepared on behalf of Steptoe in May 2021, available at https://www.steptoeinternationalcomplianceblog.com/files/2021/05/AI_Infographic-1.pdf. Retrieved October 22, 2021.

[1293] Theodore Christakis, Mathis Becuywe: Pre-market requirements, prior authorisation and Lex Specialis – novelties and logic in the facial recognition-related provisions of the draft AI Regulation. Article published May 4 2021, available at https://europeanlawblog.eu/2021/05/04/pre-market-requirements-prior-authorisation-and-lex-specialis-novelties-and-logic-in-the-facial-recognition-related-provisions-of-the-draft-ai-regulation/. Retrieved October 22, 2021.

[1294] Ariel Bogle: Australian Federal Police officers trialed controversial facial recognition tool Clearview AI. Article published on April 15 2020, available at https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894. Retrieved October 22, 2021.

[1295] Source: https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe. Retrieved October 22, 2021.

biometric information (e.g. Germany).[1297] Against this background, this particular section within the draft AI Regulation faced harsh criticism; some institutions comment that the draft Act "*missed an opportunity to clearly draw red lines and close loopholes*".[1298] Others point to the fact that facial recognition has already been banned in many U.S. states,[1299] which is remarkable insofar as the U.S.A and the EU historically took a different approach on privacy: not the European principle of prohibition subject to permission but the idea that everything is allowed as long as it is not forbidden. As for high-risk AI applications, these can roughly be divided into high-risk sectors (e.g., healthcare, employment, finance) and high-risk purposes (e.g. automated driving, energy distribution, recruitment), for example:[1300]

- Management and operation of critical infrastructures such as traffic and electricity,
- Education or Vocational training, for example determining access to education,
- Employment (i.e., during the recruitment, promotion or termination process,
- Evaluation of access to essential resources, benefits and services,
- Law enforcement (e.g., assessing risks of re-offending),
- Immigration and border control and asylum.

The following general requirements will apply to high-risk AI:[1301] human oversight, adequate risk management, appropriate transparency obligations, documentation to allow for compliance assessments, logging of activities to ensure traceability as well as a high level of accuracy, robustness and security and the use of high-quality training, validation and testing data sets.[1302] High risk AI will

[1296] Natasha Lomas: Sweden's data watchdog slaps police for unlawful use of Clearview AI. Article published February 12 2021, available at https://techcrunch.com/2021/02/12/swedens-data-watchdog-slaps-police-for-unlawful-use-of-clearview-ai/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAALgmrj2j7lIqtPjUw9cgbbjI_LwuKoMDVdLqwxaBB4vNzCgFK7Pbz7Ez_PA0oQOMd7Csz70S7acDJmzPURaBLxCvcCrHG9kAiK1112tsVuo1yTd_vtJ3XMiwQYkT2_yofnTUP6pgIpte0masI6OagPfoQ91ZjZA16T2v7bBqJRwp. Retrieved October 22, 2021.

[1297] Source: https://www.dataguidance.com/news/hamburg-hmbbfdi-issues-decision-initiating. Retrieved October 22, 2021.

[1298] Friederike Reinhold, Angela Müller for AlgorithmWatch: AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence – A major step with major gaps. Article published April 22 2021, available at https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/. Retrieved October 22, 2021.

[1299] Melissa Heikkila for POLITICO: AI: Decoded: US states move to ban facial recognition -AI and structural racism. Article published May 12 2021, available at https://www.politico.eu/newsletter/ai-decoded/politico-ai-decoded-ai-gov-us-states-move-to-ban-facial-recognition-ai-and-structural-racism/. Retrieved October 22, 2021.

[1300] The law firm Hunton Andrews Kurth provides details on the proposed AI Act in their 2021 blog post: European Commission publishes proposal for Artificial Intelligence Act. Article published April 22 2021, available at https://www.huntonprivacyblog.com/2021/04/22/european-commission-publishes-proposal-for-artificial-intelligence-act/. Retrieved October 22, 2021.

[1301] Diletta De Cicco, Charles-Albert Helleputte: The EU Artificial Intelligence Act, paper prepared on behalf of Steptoe in May 2021, and is available at https://www.steptoeinternationalcomplianceblog.com/files/2021/05/AI_Infographic-1.pdf. Retrieved October 22, 2021.

[1302] Marta Delgado Echevarría et al: European Union – Regulating Artificial Intelligence: European Commission Launches Proposals. Article published April 30 2021, available at be subject to certain restrictions; in particular, conformity assessments will be required, meaning that certification will become mandatory for such AI applications.[1303] In this regard, the EU takes a "cradle to grave approach:"[1304] high-risk AI systems will be subject to review throughout their life cycle, including mandatory risk management, documentation requirements, as well as post-market monitoring and incident reporting. Many welcomed the draft AI's proposal to create an EU database on high-risk AI systems[1305] that includes information on (see Annex VIII) the AI system (including status, trade name and any other additional reference allowing for identification as well as information on the member states in which the AI system is to or has been placed on the market, put into service or made available; the type, number and expiry date of the certificate issued by the notified body including; a description of the intended purpose of the AI system; a copy of the conformity certificate (where required); a URL for additional information (optional); electronic use instructions and provider information. It is important to note that the majority of obligations applies to so-called providers, but Chapter 2 and 3 of Title III also establish obligations for importers (covered under Article 26 of the draft AI Act) and distributors (covered under Article 27 of the draft AI Act) as well as users (covered under Article 29 of the draft AI Act),[1306] and this shows that the regulation aims at capturing all parties involved in the making available in the market and use of AI.[1307] AI systems that are used as a products or safety components, for example in medical devices, are listed in Annex II and will require to third-party ex-ante assessments, meaning that external entities will review the AI application before it can be put into service;[1308] other high risk AI systems specified in Annex III of the draft regulation will require first-party ex-ante conformity assessments (i.e. self-assessments prior to their use), as well as ex-post quality and risk management assessments and post-market monitoring. As regards

https://www.jonesday.com/en/insights/2021/04/regulating-artificial-intelligence-european-commission-launches-proposals?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration. Retrieved October 22, 2021.

[1303] Brahim Benichou, Jan De Bruyne, Thomas Gils, Ellen Wauters: Regulating AI in the European Union: Seven Key Takeaways. Article published February 25 2020, available at https://ai-laws.org/2020/02/regulating-ai-in-the-european-union-seven-key-takeaways/. Retrieved October 22, 2021.

[1304] Jetty Tielemans: A look at what's in the EU's newly proposed regulation on AI. Article published April 21 2021, available at https://iapp.org/news/a/a-look-at-whats-in-the-eus-newly-proposed-regulation-on-ai/. Retrieved October 22, 2021.

[1305] Krzysztof Izdebski: Comment on AI Regulation Proposal. EU Database on High-risk AI Systems. Article published April 28 2021, available at https://epf.org.pl/en/2021/04/28/comment-on-ai-regulation-proposal-eu-database-on-high-risk-ai-systems/. Retrieved October 22, 2021.

[1306] Keily Blair, James Hall, Christian Schröder, Heather Sussman, Shannon Yarovsky: The new EU approach to the regulation of Artificial Intelligence. Article published on May 10 2021, available at https://www.jdsupra.com/legalnews/the-new-eu-approach-to-the-regulation-4438826/. Retrieved October 22, 2021.

[1307] Marta Delgado Echevarría et al: European Union – Regulating Artificial Intelligence: European Commission Launches Proposals. Article published April 30 2021, available at https://www.jonesday.com/en/insights/2021/04/regulating-artificial-intelligence-european-commission-launches-proposals?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration. Retrieved October 22, 2021.

[1308] Cailean Osborne: The European Commission's Artificial Intelligence Act highlights the need for an effective AI assurance ecosystem. Article for the Centre for Data Ethics and Innovation. Article published May 11 2021, available at https://cdei.blog.gov.uk/2021/05/11/the-european-commissions-artificial-intelligence-act-highlights-the-need-for-an-effective-ai-assurance-ecosystem/. Retrieved October 22, 2021.

conformity assessments, reference is made to existing requirements in EU product safety laws (see Annex II),[1309] however, the AI Regulation's self-assessment-approach faced criticism: while industry often prefers a deregulated landscape when it comes to using technology, because it is believed that regulation stifles innovation,[1310] legislative history in the course of industrial revolutions and across various sectors, be it transportation, chemical engineering, communications, aviation or biotechnology and digitization has shown that voluntary codes or self-regulation may simply not work, and that regulatory discussions should not primarily focus on specific harms or individual risks but also take the systemic and structural risk of Artificial Intelligence into consideration.[1311] Some say that time will tell whether voluntary codes and ethics standards will be sufficient to mitigate the risks posed by AI but some believe that where AI applications have an impact on human rights, legislation is required to protect those human rights.[1312] Finally, the Artificial Intelligence Act furthermore sets forth that minimal or no risk AI (e.g. spam filters) will be permitted with no restrictions, but providers of such AI applications are encouraged to adhere to voluntary codes of conduct or apply voluntary labeling schemes.[1313] AI systems which pose a limited risk (e.g. chat-bots) – perhaps the majority of applications – will be subject to transparency obligations to allow for informed decisions.[1314]

II. Considerations for international data transfers

Owing to the fact that processing of personal data in many cases cannot be limited to a single country or the European Union / the European Economic Area and a small number of non-EU countries,[1315] further rules were needed to serve as standards and safeguards for international data transfers.[1316] At present, a diversified toolkit of mechanisms to transfer data to third countries exists such as, for

[1309] Jetty Tielemans: A look at what's in the EU's newly proposed regulation on AI. Article published April 21 2021, available at https://iapp.org/news/a/a-look-at-whats-in-the-eus-newly-proposed-regulation-on-ai/. Retrieved October 22, 2021.

[1310] Valerie Thomas on behalf of the Regulatory Institute: Report on Artificial Intelligence part I: the existing regulatory landscape. Article published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/. Retrieved October 22, 2021.

[1311] Julia Black, Andrew Murray: Regulating AI and Machine Learning: Setting theRegulatory Agenda, European Journal of Law and Technology, vol 10, issue 3, 2019. An online version of the paper is available at https://ejlt.org/index.php/ejlt/article/view/722/980. Retrieved October 22, 2021.

[1312] Alan Turing Institute: AI, ethics and the law: what challenges and what opportunities. Article published January 18 2018, available at https://aticdn.s3-eu-west-1.amazonaws.com/2018/03/140318-Ai-ethics-and-the-law-public-panel-report.pdf. Retrieved October 22, 2021.

[1313] Lisa Peets, Marty Hansen, Sam Jungyun Choi, Nicholas Shepherd, Anna Oberschelp de Meneses: European Commission Presents Strategies for Data and AI. Article published February 20, 2020, available at https://www.covingtondigitalhealth.com/2020/02/european-commissions-white-paper-on-artificial-intelligence-part-2-of-4/. Retrieved October 22, 2021.

[1314] Cailean Osborne: The European Commission's Artificial Intelligence Act highlights the need for an effective AI assurance ecosystem. Article published May 11 2021, available at https://cdei.blog.gov.uk/2021/05/11/the-european-commissions-artificial-intelligence-act-highlights-the-need-for-an-effective-ai-assurance-ecosystem/. Retrieved October 22, 2021.

[1315] Further information can be found at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en. Retrieved October 17, 2021.

[1316] More information is available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0007&from=EN. Retrieved October 17, 2021.

example, a set of Standard Contractual Clauses (SCCs),[1317] Binding Corporate Rules[1318] as well as several adequacy decisions.[1319] GDPR Article 45 (9) makes clear that pre-GDPR adequacy decisions remain in force. One of the well-known legal instruments in this regard was the so-called Privacy Shield.[1320] The EU-US Privacy Shield was adopted in 2016[1321] and reviewed on an annual basis[1322] to ensure a constant level of adequacy for the protection of personal data. One the one hand, businesses this framework as it brings legal clarity; on the other hand, the EU-US Privacy Shield, like its precursor "Safe Harbor",[1323] faced criticism – already the European Parliament passed a non-binding resolution in which it asked the European Commission to suspend the Privacy Shield framework as it fails to provide an adequate level of protection.[1324]

1. EU-US Privacy Shield framework

The Privacy Shield has in fact been invalidated by the European Court of Justice in summer 2020[1325] because the U.S. does not have an adequate level of data protection given that authorities have administrative access powers and due to the lack of legal protection options for EU citizens. While the appropriateness of Standard Contractual Clauses has been confirmed, the protection of personal data in the context of US national security has been questioned.[1326] Consequently, a coalition of civil society groups sent a letter to President Biden "*urging the administration to ensure that any new transatlantic data transfer deal is coupled with the enactment of surveillance reforms and comprehensive data protection legislation*" since otherwise, concerns about data transfers to the United States will remain.[1327] As a reaction to the invalidation of the Privacy Shield, many national supervisory

[1317] Source: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en. Retrieved October 17, 2021.

[1318] Relevant information on the respective process can be found at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en. Retrieved October 17, 2021.

[1319] Source: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en. Retrieved October 17, 2021.

[1320] Source: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en. Retrieved October 22, 2021.

[1321] Further information is available at http://europa.eu/rapid/press-release_IP-16-2461_en.htm. Retrieved October 22, 2021.

[1322] The corresponding report is available at https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf. Retrieved October 22, 2021.

[1323] It was struck down by the European Court of Justice on October 6, 2015, source: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=2393. Retrieved October 22, 2021.

[1324] Source: https://www.dataprotectionreport.com/2018/07/european-parliament-asks-for-suspension-privacy-shield/. (Retrieved October 22, 2021). In this regard, the parliament's resolution cites a number of reasons like the Facebook/Cambridge Analytica case or the Foreign Intelligence Surveillance Act.

[1325] Source: file:///C:/Users/kvarn/AppData/Local/Temp/cp200091en.pdf.

[1326] Source: http://curia.europa.eu/juris/document/document.jsf?docid=221826&doclang=EN. Retrieved October 22, 2021.

[1327] The Electronic Privacy Information Center's (EPIC) letter was issued June 10 2021, and is available at https://epic.org/international/Data-Flows-Negotiations-Coalition-Letter-June2021.pdf. Retrieved October 22, 2021.

authorities issued – divergent – guidance[1328] to help with "*transfer impact assessments*".[1329] Companies are still left with uncertainty and unclear homework with regards to vendor screenings to demonstrate that they evaluated service suppliers processing their (employee, customer) data abroad, because there are more and more regulator decisions which underline the inadmissibility of data transfers to the U.S.: Already in April 2021, the supervisory authority of Portugal, who specifically referred to the "*Schrems II*" decision, issued a resolution which required the National Institute of Statistics to suspend, within twelve hours, the transfer of data collected as part of the 2021 census surveys to the US or any other third country without adequate data protection.[1330] The European Data Protection Supervisor issued a decision against the European Parliament after EP Members alleged that the Parliament's use of cookies violated data protection law, including requirements regarding the transfer of personal data outside of the EU.[1331] Shortly after the EDPS' decision, the Austrian regulator took a similar position in the framework of Google Analytics in a complaint that was initiated by Max Schrems' NGO "*None of Your Business*".[1332] Developments in the context of "BREXIT"[1333] caused further unrest, however, in early 2021, the European Commission launched a "*process towards the adoption of two adequacy decisions for transfers of personal data to the United Kingdom, one under the General Data Protection Regulation and the other for the Law Enforcement Directive*"[1334], a step that many welcomed and some predicted.[1335] In June 2021, the European Commission adopted these two adequacy decisions, meaning that organizations in the EU can transfer personal data to organizations in the UK without restriction, and with no need to use SCCs to ensure an adequate level of protection.[1336]

[1328] The International Association of Privacy Professionals (IAPP) provides an overview on this topic; they published DPA and government guidance on "Schrems II", which is available at https://iapp.org/resources/article/dpa-and-government-guidance-on-schrems-ii-2/. Retrieved October 22, 2021.

[1329] The term refers to recommendations issued by the European Data Protection Board regarding "*supplementary measures to ensure compliance with data protection laws when transferring personal data from Europe*". The recommendations have been published on June 21 2021, and are available https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

[1330] Nigel Parker: Schrems II – Portuguese DPA suspends data transfer to the US by public entity that relied on standard contractual clauses. Article published May 7 2021, available at https://www.allenovery.com/en-gb/global/blogs/digital-hub/schrems-ii-portuguese-dpa-suspends-data-transfer-to-the-us-by-public-entity-that-relied-on-standard-contractual-clauses.

[1331] Source: file:///C:/Users/kvarn/AppData/Local/Temp/Case-2020-1013-EDPS-Decision_bk.pdf.

[1332] Source: https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal.

[1333] The European Data Protection Supervisor: Information note on international data transfers after Brexit issued on July 18 2019, available at https://edps.europa.eu/sites/edp/files/publication/19-07-16_for_translation_note_on_personal_data_transfers_post-brexit_en.pdf. Retrieved October 22, 2021.

[1334] European Commission Press release published February 19 2021, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661. Retrieved October 22, 2021.

[1335] Oliver Patel, Nathan Lea: EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows, published in May 2020 by the UCL European Institute, available at https://www.ucl.ac.uk/european-institute/sites/european-institute/files/privacy_shield_brexit_and_the_future_of_transatlantic_data_flows_1.pdf. Retrieved October 22, 2021.

[1336] European Commission press release: Commission adopts adequacy decisions for the UK, published June 28 2021, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183. Retrieved October 22, 2021.

2. Binding Corporate Rules and Standard Contractual Clauses

Together with Binding Corporate Rules which some consider the "*gold standard for international data transfers*",[1337] Standard Contractual Clauses have been and will be a major legal instrument for international data transfers. As a follow-up to the Privacy Shield decision, SCCs have been updated – and widely commented at local[1338] and EU level[1339] – to reflect some of the concerns that were raised in the context of the decision. However, the path forward may still not be crystal clear as the European Commission and Ireland's data regulator are investigating if the proposed new Standard Contractual Clauses could cause complications when used under Irish law.[1340] Developments are generally very dynamic in this area: the EDPB and EDPS commented on the European Commission's new framework and issued a joint statement in which they requested various amendments[1341] which some consider substantial revisions,[1342] and the European Commission is not the only body that is working on a final set of new Standard Contractual Clauses. The UK's Information Commissioner is preparing a bespoke set of Standard Contractual Clauses to facilitate transfers of personal data,[1343] and Brazil's data protection law is another example of a legal framework that also allows for international transfers of personal data based on contractual instruments such as binding corporate rules and standard clauses.[1344] Even though companies will have 18 months to substitute the European Commission's

[1337] Lukas Feiler, Wouter Seinen: BCRs as a robust alternative to Privacy Shield and SCCs. Article published July 23 2020, available at https://iapp.org/news/a/binding-corporate-rules-as-a-robust-alternative-to-privacy-shield-and-sccs/. Retrieved October 22, 2021.

[1338] For example, one of the German regulators recommended actions and amendments to SCCs. The guidance was published August 25 and updated on September 9 2020 and is available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/LfDI-BW-Orientierungshilfe-zu-Schrems-II.pdf. Retrieved October 22, 2021.

[1339] On January 15 2021, the EDPB and EDPS published their joint opinions on two sets of SCCs (one on SCCs for contracts between controllers and processors, and one on SCCs for transfer of personal data to third countries), available at https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_en. Retrieved October 22, 2021.

[1340] Sam Clark for Global Data Review: Draft SCC clash with Irish law reaches European Commission. Article published February 25 2021, available at https://globaldatareview.com/data-privacy/draft-scc-clash-irish-law-reaches-european-commission. Retrieved October 22, 2021.

[1341] The EDPB and EDPS adopted joint opinions on new sets of SCCs: press release published January 15 2021, available at https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_en. Retrieved October 22, 2021.

[1342] Molly Martinson: Work in progress – substantial revisions recommended to the European Commission's draft new Standard Contractual Clauses. Article published January 28 2021, available at https://practicalprivacy.wyrick.com/blog/work-in-progress-substantial-revisions-recommended-to-the-european-commissions-draft-new-standard-contractual-clauses. Retrieved October 22, 2021.

[1343] Cynthia O'Donoghue, Asel Ibraimova: ICO announces it is working on bespoke UK set of Standard Contractual Clauses. Article published 5 May 2021, available at https://www.technologylawdispatch.com/2021/05/privacy-data-protection/ico-announces-it-is-working-on-bespoke-uk-set-of-standard-contractual-clauses/. Retrieved October 22, 2021.

[1344] Renato Leite Monteiro: The new Brazilian General Data Protection Law — a detailed analysis. Article published August 15 2018, available at https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/. Retrieved October 22, 2021.

new SCCs,[1345] it is very likely to become more difficult for controllers in future to match all requirements and fulfill all contractual obligations.

3. Derogations, Codes of Conduct, Certifications

Apart from specific legal frameworks like the Privacy Shield or instruments like BCRs and SCCs, there are other legal possibilities for international data transfers:[1346] despite the exceptional character of derogations under GDPR Art. 49 which require a restrictive application, it is worthwhile noting that derogations are being discussed as a further option for international data transfers.[1347] As regards derogations under GDPR Art. 49, the International Association of Privacy Professionals published on overview in which they first explain that already the judge-rapporteur in the "*Schrems II*" case elaborated on the possibility of reliance on the GDPR Article 49 derogations; second, they stress that organizations must be aware of additional considerations in the context of derogations provided in various GDPR Recitals, and finally, they summarize how likely various derogations may be applicable as alternative ways of transferring personal data in particular scenarios.[1348] If exemptions for certain processing activities become recognized, this could lead companies to abandon their current reluctance to rely on such derogations and, to some extent, amend their documented set of data transfer mechanisms. GDPR furthermore allows for other mechanics to justify international transfers, for example an approved Code of Conduct pursuant to GDPR Article 40 and an approved certification mechanism pursuant to GDPR Article 42,[1349] in each case together with binding and enforceable commitments of the controller or processor in the third country to apply appropriate safeguards including as regards data subjects' rights. The European Union Agency for Cyber-security ENISA offers a certification framework for products, processes, and services[1350] but at present, there is no formal certification to confirm GDPR compliance. However, what is available are guidelines issued by

[1345] Cynthia O'Donoghue, Andreas Splittgerber, Asel Ibraimova: European Commission issues New Standard Clauses for data transfers outside the EEA: Act within 18 months. Article published June 4 2021, available at https://www.technologylawdispatch.com/2021/06/global-data-transfers/european-commission-issues-new-standard-clauses-for-data-transfers-outside-the-eea-act-within-18-months/. Retrieved October 22, 2021.

[1346] In 2017, the Centre for Information Policy Leadership prepared a corresponding white paper with background information: "Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy", available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final__-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf. Retrieved October 22, 2021.

[1347] Francesca Gaudino: International Data Transfer Solutions under GDPR. Article published April 19 2020, available at https://globalcompliancenews.com/international-data-transfer-solutions-under-gdpr-23032020/. Retrieved October 22, 2021.

[1348] Ruth Boardman, Louise Hutt, Antonia Boyce at Bird & Bird for IAPP: Article 49 derogations – summary table with examples. Article published May 12 2021, available at https://iapp.org/media/pdf/resource_center/article_49_derogations_summary_table_with_examples_iapp.pdf. Retrieved October 22, 2021.

[1349] GDPR Article 46 (2e) and (2f).

[1350] See the European Commission website on the Cyber-Security Act for details on ENISA's certification framework: https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en. Retrieved October 22, 2021.

the European Data Protection Board on certification (criteria) in accordance with GDPR Articles 42 and 43.[1351] In addition, the European Commission completed a study on GDPR certification mechanisms pursuant to GDPR Art 42, 43[1352] in which more than one hundred certification schemes have been identified, but only two schemes were highlighted as potential candidates to provide formal certification: the first one is ISDP 10003 offered by ACCREDIA, a scheme that is in line with ISO 17065:2012 and "*provides principles and lines of control for a complete compliance assessment of an organization's internal processes regarding protection of personal data with particular reference to proper risk management*."[1353] The second is the "European Privacy Seal" offered by EuroPrise for products, services and websites.[1354] As for Codes of Conduct pursuant to GDPR Article 40, the EDPB adopted two Codes of Conduct for cloud providers,[1355] which certainly helps to demonstrate compliance but cannot be considered a formal (GDPR) certification. The same applies to various other certifications, for example ISO 27001 on information security management, ISO 27017, a complementary standard to ISO 27001 for could services, or ISO 27018 which is yet another complementary standard that contains guidelines applicable to cloud service providers that process personal data.[1356] However, developments with cloud providers should be closely monitored: the invalidation of the Privacy Shield lead to additional compliance efforts in the framework of vendor screenings, and it is a positive signal that various stakeholders are working on an EU Cloud Code of Conduct[1357] to propose a legal solution for the transfer of personal data outside the EU as an alternative to the annulled EU-U.S. Privacy Shield. Such a Code of Conduct must of course be approved by data protection authorities, but the Belgian regulator already expressed that they are "*impressed by the efforts and resources dedicated by this industry-group to implement best practices for the cloud industry that are both hands-on and respectful of the data subjects*."[1358]

[1351] On June 4, 2019, the European Data Protection Board published "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation", source: https://edpb.europa.eu/our-work-tools/our-documents/nasoki/guidelines-12018-certification-and-identifying-certification_en. Retrieved October 22, 2021.

[1352] European Commission: Data Protection Certification Mechanisms, Study on Articles 42 and 42 of the Regulation EU 2016/679. The final report on the GDPR certification study was issued in February 2019 and is available at https://ec.europa.eu/info/sites/default/files/data_protection_certification_mechanisms_study_final.pdf. Retrieved October 22, 2021.

[1353] Source: https://in-veo.com/en/certification/isdp-10003-2020-data-protection. Retrieved October 22, 2021.

[1354] Source: https://www.euprivacyseal.com/EPS-en/certifications-offered. Retrieved October 22, 2021.

[1355] EDPB adopts opinions on first transnational Codes of Conduct: press release published May 20 2021, available at https://edpb.europa.eu/news/news/2021/edpb-adopts-opinions-first-transnational-codes-conduct-statement-data-governance-act_en. Retrieved October 22, 2021.

[1356] Background information on various ISO standards is available at the German Federal Office for Information Security Bundesamt für die Sicherheit der Informationstechnik) on their website: https://www.bsigroup.com/en-GB/ISO-IEC-27018/. Retrieved October 22, 2021.

[1357] Source: https://eucoc.cloud/en/home.html. Retrieved October 22, 2021.

[1358] John Garrett: EU data protection code to replace US/EU data rules. Article published September 16 2020, available at https://www.iteuropa.com/news/eu-data-protection-code-replace-useu-data-rules#:~:text=The%20EU%20Cloud%20Code%20of%20Conduct%20General%20Assembly,personal%20data%20to%20third%20countries%20around%20the%20world. Retrieved October 22, 2021.

4. Data trustee models

Further promising initiatives to help face challenges with (undesired) international transfer of personal data have been discontinued[1359] in the meantime, for example the data trustee model Microsoft pursued with the German Telekom[1360] with the help of data centers located in Germany, a set up that would prevent that data are accessed by or shared with governmental agencies – i.e. external governmental access: it should be noted that the issue of government access to personal information is neither novel nor unique to the USA, there are numerous laws that require companies to provide personal data to public authorities, e.g. for financial transactions or regarding telecommunications, and in 2018, the European Union proposed an e-Evidence regulation that envisages that law enforcement and judicial authorities access electronic evidence for investigation purposes.[1361] Interestingly, it was announced in early 2021 that the German Telekom will again provide a "Cloud Privacy Service for GDPR compliant use of Microsoft 365".[1362] Data will be encrypted, which obviously is a key measure when it comes to facilitating international data transfers: in August 2021, the Belgian Council of State decided that encryption is a sufficient measure for U.S. data transfers.[1363]

5. Technical solutions

Various other options have been discussed at technical level to avoid (government) access to data including personal information, for example encryption or anonymization as well as data localization or the use of so-called private clouds or synthetic data – but they all come along with their own factual limitations, technical difficulties or legal challenges: anonymization of data is difficult to achieve; many studies have shown that supposedly anonymous data can be re-identified[1364]. Similar problems

[1359] Background information on Microsoft's decision summarized by Esat Dedezade: Microsoft to deliver cloud services from new data centers in Germany in 2019 to meet evolving customer needs. Article published August 31 2018, available at https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/. Retrieved October 22, 2021.

[1360] The project started in 2015, see https://www.webwire.com/ViewPressRel.asp?aId=200848. Retrieved October 22, 2021.

[1361] A proposal for a regulation on European production and preservation orders for electronic evidence in criminal matters (see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN), and a proposal for a directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN). Retrieved October 22, 2021.

[1362] Hans Peter Schüler: Cloud Privacy Service zur DSGVO-konformen Nutzung von Microsoft 365. Article published September 6 2021, available at https://www.heise.de/hintergrund/Cloud-Privacy-Service-zur-DSGVO-konformen-Nutzung-von-Microsoft-365-6171165.html. Retrieved October 22, 2021.

[1363] Tanguy Van Overstraeten, Julie De Meyer: Belgium: Council of State approves US data transfer. Article published September 16 2021, available at https://www.linklaters.com/th-th/insights/blogs/digilinks/2021/september/belgium-council-of-state-approves-us-data-transfer. Retrieved October 22, 2021.

[1364] Researchers of the Massachusetts Institute of Technology (MIT) published a study in December 2018 explaining that anonymous data can be re-identified. The corresponding press release is available at https://www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized. Retrieved October 22, 2021.

have been reported for so-called synthetic, i.e. artificially manufactured, data which are currently being discussed[1365] as a privacy-friendly solution, for example in the area of healthcare.[1366] Encryption may not work for all datasets and the future of such a protective measure is questionable as the EU is thinking about prohibiting encryption[1367] to better fight (online and cyber) crime – but apart from individuals' legitimate security interests, it must not be forgotten that secure communication is essential for a free press or professional secrecy, which makes the balancing of interests very hard. The use of private clouds sounds promising, but apart from access issues, private clouds could simply be less secure than public clouds: cloud service providers can spend much more on security tools than any large, but single enterprise could: the cost of security is diluted across millions of users to fractions of a cent.[1368]

6. Adequacy decisions

Adequacy decisions are the most effective mechanism for international data transfers as organizations are not required to put in place any specific measures; consequently, some "*third countries*" stared adapting their data protection laws to be more in line with the GDPR (for example, Brazil) in the hope to obtain the adequacy status one day.[1369] At present, only a handful of tcountries have been recognized as adequate by the European Commission.[1370] In this regard, the Republic of Korea was the latest addition,[1371] and conversations on EU-Japan mutual adequacy arrangements commenced.[1372] The problem with adequacy decisions is that the Commission adopts adequacy decisions at a slow pace because the European Commission is cautious and wants to ensure that adequacy decisions will prevail. In the framework of the European Parliament's annual review of data-transfer agreements, it was discussed whether California could have its own Privacy Shield arrangement separate from the

[1365] Steven Bellovin, Preetam Dutta, Nathan Reiting: Privacy and Synthetic Datasets, Stanford Technological Law Review 2019, vol. 22, issue 1, available at https://law.stanford.edu/wp-content/uploads/2019/01/Bellovin_20190129-1.pdf. Retrieved October 22, 2021.

[1366] Bill Siwicki: Is synthetic data the key to healthcare clinical and business intelligence? Article published February 21 2020, available at https://www.healthcareitnews.com/news/synthetic-data-key-healthcare-clinical-and-business-intelligence. Retrieved October 22, 2021.

[1367] Katarzyna Lasinska: Encryption Policy Issues in the EU. Article published May 25 2018, available at https://www.globalpolicywatch.com/2018/05/encryption-policy-issues-in-the-eu/. Retrieved October 22, 2021.

[1368] Jim O'Reilly: Data Protection in the Public Cloud. Article published March 15 2018, available at https://www.networkcomputing.com/data-centers/data-protection-public-cloud-6-steps. Retrieved October 22, 2021.

[1369] Olivier Proust: What future for the transfers of personal data? Article published January 18 2022, available at https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/what-future-for-the-transfers-of-personal-data.

[1370] Source: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[1371] Source: https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-republic-korea-annexes_en.

[1372] Source: https://ec.europa.eu/newsroom/just/items/724795/en.

rest of the U.S. given that California indeed introduced strong privacy rules.[1373] This is a truly interesting development, because many of the Big Tech players have their headquarters in California, and an arrangement with a sub-federal territory is indeed possible under GDPR, because adequacy status can be granted to regions as opposed to countries.[1374] Such a development could once more reshape the global landscape for data transfers.

7. Data Localization, Data Residency and Data Sovereignty

Finally, local data storage has been discussed as an appropriate response to concerns in the framework of international data transfers and global data processing. In fact, many countries around the globe already have specific data localization requirements: some introduced rules for selected industries or certain providers such as social media companies[1375] or for public service providers or for certain types of data like government data, telecommunications (metadata), health records, payment information or geo-data.[1376] It can generally be said that various jurisdictions distinguish between data localization, data residency and data sovereignty[1377]: data residency refers to the geographic location of data storage for regulatory reasons, and data sovereignty is about data being hosted in a country to which the country's laws apply to ensure the country remains in control.[1378] Additionally, many countries restrict transfer of information which they consider relevant for national security, for example information that is relevant for military technology.[1379] However, recent developments show that local data storage might be even more difficult to achieve in the future: Microsoft is experimenting with underwater datacenters[1380] and reports that they are 'reliable, practical and use energy sustainably'. The interesting

[1373] Jennifer Baker: EU Parliament debates: Could California be considered 'adequate' on its own? Article published January 9, 2020, available at https://iapp.org/news/a/eu-parliament-debates-could-california-be-considered-adequate-on-its-own/. Retrieved October 22, 2021.

[1374] Jennifer Baker: California Dreamin': Is a Single State EU Data Protection Deal on the Cards? Article published January 20, 2020. The article refers to a statement by Bruno Gencarelli who heads the International data flows and protection unit at the European Commission (DG Justice and Consumers), and is available at https://www.cpomagazine.com/data-protection/california-dreamin-is-a-single-state-eu-data-protection-deal-on-the-cards/. Retrieved October 22, 2021.

[1375] Begüm Yavuzdoğan Okumuş, Direnç Bada: Turkish Data Localization Rules In Effect For Social Media Companies. Article published October 14 2020, available at https://gun.av.tr/insights/articles/turkish-data-localization-rules-in-effect-for-social-media-companies?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration. Retrieved October 22, 2021.

[1376] An overview is provided by John Selby in his 2017 paper: Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? International Journal of Law and Information Technology, vol. 25, issue 3, pp. 213–232, available at https://doi.org/10.1093/ijlit/eax010. Retrieved October 22, 2021.

[1377] Background information on data localization, data residency and data sovereignty is provided by Benjamin Vitaris in his article: Data Residency: Meaning, Laws, & Requirements, published July 30 2020, available at https://permission.io/blog/data-residency/. Retrieved October 22, 2021.

[1378] For instance, Australia, see the Australian Privacy Principles (APPs) law, available at https://www.oaic.gov.au/privacy/australian-privacy-principles/. Retrieved October 22, 2021.

[1379] Berkeley Lab provides examples of export-controlled data and explains technical data: https://exportcontrol.lbl.gov/definition/technical-data-technology/. Retrieved October 22, 2021.

[1380] Source: https://news.microsoft.com/innovation-stories/project-natick-underwater-datacenter/. Retrieved October 22, 2021.

question here would be which law(s) are applicable in such scenarios. Moreover, data localization and data residency is questionable from both, a data security and a data protection perspective: common reasons for such initiatives are the fight against espionage and crime, strengthening of cyber-security and the pursuit of resilience. But technically speaking "*physical access to a server or device containing data is neither a necessary nor a sufficient condition for access to information (...). On the other hand, logical access is both necessary, and may be sufficient to provide access to data in an intelligible form, regardless of geographic location*".[1381] While no general statement can be made as to whether local data storage may raise security concerns since not all local data centers may have the same (state of the art) level of safety and security, such issues may still arise when using one (single i.e. vulnerable point of failure) location which some therefore describe as the Galapagos syndrome:[1382] a comfortable short-term solution that may lead to long-term extinction. The above examples of why national legislators came up with data localization and data sovereignty should not be seen in isolation: reverse and / or social engineering may also result in loss of know-how from a company and data breach from an individual's perspective; in this regard, data localization cannot help. In many countries, an important factor to foster data localization is to help law enforcement and national security agencies' access to data – but (foreign) government access to personal information was the reason why European Court of Justice dealt with the issue of international data transfers in the framework of their EU-U.S. Privacy Shield decision. Data localization is justified by the need to protect personal information, but the above circumstances explain why there is also fear that (domestic) government access to data through data localization undermines data privacy, and that is why some claim that data localization does not solve the problem of surveillance, but introduces new troubles of its own[1383], including negative political impacts "*by bringing information under governmental control*".[1384] From a data privacy perspective, it should be taken into consideration that general data protection principles like data minimization, data integrity and confidentiality may not be met if companies must establish and defend multiple versions of its systems across continents with additional hardware, additional vendors and additional staff. Data localization and data residency are complicated and costly, and may lead to further fragmentation, and that is perhaps why there does not seem to be a consistent approach even within the European Union: apart from the fact that GDPR's

[1381] Christopher Millard: Forced Localization of Cloud Services: Is Privacy the Real Driver? Paper provided for the 2015 forthcoming in IEEE Cloud Computing. Article published May 14, 2015, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605926. Retrieved October 22, 2021.

[1382] Chan-Mo Chung: Data localization: The causes, evolving international regimes and Korean practices, Journal of World Trade 2018, vol. 52, issue 2, pp. 187-208.

[1383] Anupam Chander: Is Data Localization a Solution for Schrems II? Article published September 2020, available at https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3318&context=facpub. Retrieved October 22, 2021.

[1384] Erica Fraser: Data Localisation and the Balkanisation of the Internet, SCRIPTed – Journal of Law, Technology & Society, vol. 13, issue 3, December 2016, available at https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/. Retrieved October 22, 2021.

official title explains that the regulation also is about the "free movement of data", the EU commission previously discussed to ban forced data localization.[1385]

III. Emerging U.S. legal landscape

As for the emerging U.S. legal landscape, the difference between the U.S.A. and Europe is that U.S. legislators have been very active in recent years when it comes to regulating AI: California seems to be leading in the area of data protection as the state worked on several major initiatives: the California Consumer Privacy Act (CCPA),[1386] and the California Privacy Rights Act (CPRA)[1387] are the most recent initiatives, and the Online Privacy Protection Act (CalOPPA)[1388] was the first state law in the nation to require commercial websites and online services to post a privacy policy; it went into effect already in 2004 and was amended in 2013 to require new privacy disclosures regarding tracking of online visits.[1389] In addition, California's Privacy Protection Agency which was created under CPRA held its first meeting and is prepared for upcoming rulemaking.[1390] The US privacy landscape became so dynamic that law firms started to provide weekly status information about the status of state privacy legislation.[1391] Several states introduced their own privacy bills with requirements that are somewhat similar to those set forth in the GDPR, for example Washington[1392] which grants consumers various rights such as access, portability, correction, deletion, and the right to object to the processing of their data in certain circumstances, or Virginia: the law requires opt-out for targeted advertising and profiling decisions that produce legal or similarly significant effects and mandatory Data Protection Impact Assessment for certain activities including profiling.[1393] Colorado[1394] also enacted privacy

[1385] Jennifer Baker: EU Commission aims to ban forced data localization. Article published October 24 2016, available at https://iapp.org/news/a/eu-commission-aims-to-ban-forced-data-localization/. Retrieved October 22, 2021.

[1386] Source: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Retrieved October 22, 2021.

[1387] The text of the California Consumer Privacy Act is available at https://www.caprivacy.org/cpra-text/. Retrieved October 22, 2021.

[1388] California Online Privacy Protection Act text available at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC. Retrieved October 22, 2021.

[1389] California's Consumer Federation provides background information on various relevant laws, including the Online Privacy Protection Act, available at https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/. Retrieved October 22, 2021.

[1390] Madeline Salinas: California Privacy Protection Agency Holds First Meeting. Article published June 24 2021, available at https://www.insideprivacy.com/ccpa/california-privacy-protection-agency-holds-first-meeting-preparing-for-upcoming-rulemaking/. Retrieved October 22, 2021.

[1391] David Stauss: Status of Proposed CCPA-Like State Privacy Legislation as of May 3, 2021. Article published May 2 2021, available at https://www.bytebacklaw.com/2021/05/status-of-proposed-ccpa-like-state-privacy-legislation-as-of-may-3-2021/. Retrieved October 22, 2021.

[1392] Background information on Washington's Privacy Act (WPA) can be found at https://www.consumerprivacyact.com/washington/. Retrieved October 22, 2021.

[1393] Jim Halpert, Lael Bellamy: What Virginia's Consumer Data Protection Act means for your privacy program. Article published March 8 2021, available at legislation that has special protections for sensitive data and adopted certain privacy-by-design principles,[1395] and New Jersey introduced a notable bill that reminds of GDPR by providing for a right for a consumer not to be subject to a decision based on solely automated decision making.[1396] However, these laws are addressed to consumers, meaning that either definitions are different or that the scope of these laws is different in comparison to GDPR or any other data protection laws that are concerned with the individual behind the data. This shows that historically, data protection in the U.S. was about consumer protection and vice versa, whereas in continental Europe, data protection initiatives were addressed to the public sector. While the emergence of privacy laws in the U.S. is generally welcomed, some describe recent developments as a "*disparate landscape in need of consolidation*."[1397] Apart from basic data protection legislation, there is consensus about the need for AI-specific rules,[1398] the White House dealt with the issue and provided guidance for the Regulation of AI applications[1399] which on the one hand, aims at promoting the development of trustworthy AI and encouraging public engagement, but on the other hand also intends to promote a "light-touch AI regulatory approach."[1400] In addition, the White House launched a National AI Initiative Office for federal AI coordination,[1401] and is moreover planning for the establishment of a National Security Commission on Artificial Intelligence.[1402] The U.S.A. are also working on a "Algorithmic Justice and Online Platform Transparency Act"[1403] which sets forth specific requirements for online platforms, ranging from transparency and documentation – including annual public reports and ad libraries – over prohibition of discrimination up to the establishment of a specific task force to investigate the

https://iapp.org/news/a/what-the-virginia-consumer-data-protection-act-means-for-your-privacy-program/#:~:text=Virginia%27s%20CDPA%20is%20a%20somewhat%20simplified%20version%20of,by%20overwhelming%20margin%20in%20fewer%20than%20two%20months. Retrieved October 22, 2021.

[1394] Source: https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf. Retrieved October 22, 2021.

[1395] Angelique Carson: Colorado Privacy Act (CPA): What is it? Article published June 11 2021, available at https://www.osano.com/articles/colorado-privacy-act-what-is-it. Retrieved October 22, 2021.

[1396] For example, the Colorado Privacy Act, Virginia's CDPA or the New Jersey Disclosure and Accountability Transparency Act, see Pollyanna Sanderson: Automated Decision Systems Legislation Update, presentation held on June 14 2021 during a Future of Privacy Forum meeting.

[1397] Jacob Nix, Pascal Bizarro: US Data Privacy Law: A Disparate Landscape in Need of Consolidation. Article published September 9 2020, available at https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/us-data-privacy-law-a-disparate-landscape-in-need-of-consolidation. Retrieved October 22, 2021.

[1398] Marta Delgado Echevarría et al: European Union – Regulating Artificial Intelligence: European Commission Launches Proposals. Article published April 30 2021, available at https://www.jonesday.com/en/insights/2021/04/regulating-artificial-intelligence-european-commission-launches-proposals?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration

[1399] Source: https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf. Retrieved October 22, 2021.

[1400] Katori Rameau, K.C. Halm: White House Issues Guidance for AI Regulation and "Non-Regulation". Article published January 22 2020, available at https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2020/01/white-house-ai-guidelines.

[1401] Source: https://trumpwhitehouse.archives.gov/briefings-statements/white-house-launches-national-artificial-intelligence-initiative-office/#:~:text=The%20Office%20is%20charged%20with%20overseeing%20and%20implementing,as%20with%20private%20sector%2C%20academia%2C%20and%20other%20stakeholders. Retrieved October 22, 2021.

[1402] Source: https://www.congress.gov/bill/115th-congress/house-bill/5356/. Retrieved October 22, 2021.

[1403] Source: https://www.congress.gov/bill/117th-congress/senate-bill/1896/text. Retrieved October 22, 2021.

discriminatory algorithmic processes employed in by online platforms.[1404] The country is also making efforts towards a comprehensive federal data protection legislation,[1405] and in recent years, various AI, algorithmic as well as ADM- and accountability-specific laws have been introduced at federal and state level, for example the Algorithmic Accountability Act,[1406] the Artificial Intelligence Act[1407], the AI in Government Act,[1408] the National Artificial Intelligence Initiative Act,[1409] the Protecting Americans from Dangerous Algorithms Act,[1410] the Artificial Intelligence Reporting Act,[1411] the Future of AI Act,[1412] the Advancing American AI Act,[1413] the Advancing AI Research Act,[1414] or the Mind Your Own Business Act.[1415]

H. Summary and conclusions

The examination of the historical context showed that it is important to distinguish various terms which are used interchangeably, namely, privacy and data protection, and to explain legislator objectives in recent decades. The history of (the right to) privacy and the fact that privacy and the respect for the private life are mentioned in a variety of international conventions also demonstrated that privacy is considered a fundamental right. As such, protective mechanisms have traditionally been directed against the state, and this was reflected in first-generation data protection laws since they addressed the public sector. The problem however is that there seems to be a shift of protections of fundamental rights to the private sector: some argue that, because GDPR allows for processing based on legitimate interests as well as compatible processing (secondary use of personal information), this may lead to a self-regulatory regime; ditto for self-assessments as foreseen under the new AI Regulation.

[1404] Pollyanna Sanderson: Automated Decision Systems Legislation Update, presentation held on June 14 2021 during a Future of Privacy Forum meeting.

[1405] Shiva Stella: Senate Releases Principles for Comprehensive Privacy Legislation. Article published November 18 2019, available at https://www.publicknowledge.org/press-release/senate-releases-principles-for-comprehensive-privacy-legislation/. Retrieved October 22, 2021.

[1406] Source: https://www.congress.gov/bill/116th-congress/senate-bill/1108. Retrieved October 22, 2021.

[1407] Benjamin Muller: The Artificial Intelligence Act – a quick explainer. Article publishedMay 4 2021, available at https://datainnovation.org/2021/05/the-artificial-intelligence-act-a-quick-explainer/. Retrieved October 22, 2021.

[1408] Source: https://www.congress.gov/bill/115th-congress/senate-bill/3502. Retrieved October 22, 2021.

[1409] Source: https://www.congress.gov/bill/116th-congress/house-bill/6216. Retrieved October 22, 2021.

[1410] Source: https://www.congress.gov/bill/117th-congress/house-bill/2154?q=%7B%22search%22%3A%5B%22algorithmic%22%5D%7D&s=1&r=2. Retrieved October 22, 2021.

[1411] Source: https://www.congress.gov/bill/115th-congress/house-bill/6090/. Retrieved October 22, 2021.

[1412] Source: https://www.congress.gov/bill/115th-congress/house-bill/4625. Retrieved October 22, 2021.

[1413] Source: https://www.congress.gov/bill/117th-congress/senate-bill/1353/text?q=%7B%22search%22%3A%5B%22data+OR+privacy%22%5D%7D&r=27&s=5. Retrieved October 22, 2021.

[1414] Source: https://www.congress.gov/bill/116th-congress/senate-bill/3891. Retrieved October 22, 2021.

[1415] Source: https://www.congress.gov/bill/117th-congress/senate-bill/1444/text?q=%7B%22search%22%3A%5B%22automated+decision-making%22%5D%7D&r=3&s=3. Retrieved October 22, 2021.

In this regard, the market power of certain companies within the so-called "Industry 4.0" has to be taken into consideration: One author's situational analysis is that "*Alphabet controls our search and much of our mobile experience, Apple controls the remainder of our mobile and much of our content experience, Amazon controls a large portion of our content experience and much of the Internet of Things, and Microsoft essentially sweeps up everything else*."[1416] As a result, a small number of companies may have the power to control a large part of our personal information, perhaps rather based on corporate terms and conditions and less on privacy laws, and the phenomenon became so significant that it has put the antitrust authorities on notice.

It can generally be said that data protection laws are on the rise. For example, large countries or important markets like Brazil or China adopted data protection laws, and the U.S.A. are a perfect example of an emerging legal landscape with numerous data privacy or data security (breach provision) laws and specific rules on the use of sensitive data like biometric or genetic information. The legal framework in the U.S.A. is very dynamic: California alone, to only name one example, introduced the following laws relating to privacy: the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), or the California Online Privacy Protection Act (CalOPPA). On the one hand, this should be welcomed, on the other hand, this adds to the complexity, which starts with seemingly simple issues like terminology, including translation issues.

In this context, it should also be considered that, for example, Brazil's LGPD has a territorial scope that extends outside of Brazil, meaning that as a result, global companies to which these laws apply must comply with a multitude of laws. This may lead to the so-called "Brussels-effect" which guides the way companies are doing business, because multinational organizations adjust their global operations to EU standards to be compliant.

As for the existing legal framework, another general problem is not only complexity, but also opposing legislative aspirations: a technical example is encryption which is desirable from a data protection perspective but may be legally prevented for reasons of crime prevention. This is both, a legislative and a provider trend as recent discussions around certain provider's filter functions show. A legal example is data localization: many countries around the globe already introduced data localization requirements, either for selected industries or for public service providers or for certain types of data (for example, government data, health records, or payment information).

Another factor to consider is the different approach various legislators take. The European approach is rights-based, the U.S.A. is harm-based, and China pursues a control-based approach, and different

[1416] Julia Black, Andrew Murray: Regulating AI and Machine Learning: Setting the regulatory agenda. European Journal of Law and Technology, vol. 10, issue 3, 2019. The article is available at https://ejlt.org/index.php/ejlt/article/view/722/980. Retrieved October 24, 2021.

jurisdictions focus on different things, for example the U.S. legal landscape is mostly concerned with customers, not all individuals (including employees).

Probably the greatest difference between the U.S. and the EU approach to data protection is that European law is permission-based, meaning that a legal basis is always required for the processing of personal data, whereas in the US, the contrary is true, because data can generally be processed unless a law explicitly prohibits such an activity. But considering how difficult the exercise of individual rights and privacy-self management in today's Big Tech "David vs. Goliath" data processing environment is, a harm-based approach may be more of a future-proof concept.

Data protection laws as we know them today have been introduced some decades ago, but the Internet (of things), the growing digitalization, new technologies and new phenomena like social media platforms, together with the growing connectivity of devices, and the overall exponential growth of (user, sensor, behavioral, etc.) data lead to the emergence of a well-known problem, the fact that the development of (appropriate) laws takes too much time: in this context, "cookies" are a good example – debates are still focused around the use of cookies, but fact is that regulators took a lot of time to come up with guidance and enforcement, and legislators took too much time with controversial discussions around accompanying legislation like the draft E-Privacy Regulation – when in fact there is already new technology which can replace cookies and provide for the same results.

As regards factual difficulties, errors may occur at any stage: owing to underlying datasets being outdated, incomplete, or incorrect, or due to wrong project design or wrong interpretation of results – this "relativity of results" is a human (awareness, training), not a technical problem. It nevertheless shows a very important factor to consider: the outcome of AI applications is based on statistical correlations, not causality, and this is quite often overlooked when AI is used.

The paper elaborated on existing legal definitions such as personal, anonymous, pseudonymous and identifiable as well as special categories of data, processing, automated decision-making and profiling or consent. Definitions are an important issue since the scope and application of laws depend on clarity as regards relevant definitions, and there are indeed challenges with definitions due to inconsistent terminology in various regulations and inconsistent use of terms within provisions, translation issues, potentially non-future-proof definitions, and the introduction of new terms in new relevant laws like the draft AI regulation.

It is moreover important to note that Big Tech players who process personal information at large scale define types of data in a way that is unknown to data protection laws. In their data processing agreements, they distinguish between data entered by users and data generated by systems or otherwise accessed, which shows that there is awareness about the de-facto predominance of indirect data collection. This explains that very often, there is little room left for the individual to control what happens to their data, and that questions viability of traditional concepts of data protection laws such as privacy self-management. Consequently, some authors argue to expand the development of privacy-enhancing and privacy-preserving technologies that need to leverage on device data.

Given the fact that the General Data Protection Regulation has a broad definition of personal data, some speak of the GDPR as "the law of everything"[1417] because literally all processing seems covered as everything may be regarded as personal data. Moreover, anonymization is technically hard to achieve or cannot be applied to certain data sets where "real data" is needed as opposed to "synthetic" or "dummy" data. Consequently, data protection laws may indeed govern most of what happens with (customer, employee) data within a business, leaving little room for the avoidance of the application of laws that govern personal information and allow for data subject rights.

The emergence of Big Data, automated decision-making and Artificial Intelligence describes data processing as we know it today and explained the foundations of these technologies as well as their dependency on the development of computer science, the needed speed of processing and infrastructure. Rather than elaborating on privacy principles such as purpose limitation, transparency or data and storage limitation, this paper focused on characteristics of Big Data and Artificial Intelligence to explain why there may be obvious collisions with basic privacy standards. The paper thus explained the main traits including the most relevant use cases, for example analytics and forecasting, fraud prevention as well as data-driven products and services. It covered the famous "Vs" of Big Data (volume, variety, velocity, veracity, variability, volatility, value) and describes various types of Artificial Intelligence such search and planning Algorithms, symbolic AI, Robotics, computer sensing and vision, Machine Learning and Deep Learning, Natural Language Processing, Knowledge Engineering or Neural Networks to name some.

A substantial part of the Thesis is dedicated to the analysis of relevant sources of law to provide an overview over the existing legal framework for processing of personal data and the protection of individuals' rights as well as privacy principles such as data minimization and purpose specification. At international level, the United Nations Universal Declaration of Human Rights, the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, the Council of Europe Data Protection Convention 108+, OECD's Privacy Guidelines as well as further

[1417] Nadezhda Purtova: The law of everything. Broad concept of personal data and future of EU data protection law. Article published in Law, Innovation and Technology 2018, vol. 10, issue 1, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355.

conventions and resolutions have been introduced. The fact that conventions deal with data protection and privacy matters shows the human rights dimension of data protection issues.

Regarding superior law, it should not be forgotten that legally binding global trade agreements also play a role in the context of data processing, particularly regarding to trans-border data flows: these agreements set forth certain standards, including norms of non-discrimination that require protections against unjustified data localization requirements.

From a data protection perspective, many immediately think of the General Data Protection Regulation as a major piece of legislation and despite the fact that the GDPR was a milestone in the history of data protection laws, it is by far not the only relevant regulation: At EU-level only, a variety of other regulations and directives have to be taken into consideration when processing of (personal) data, automated decision-making, profiling, Big Data or Artificial Intelligence are in question – be it from a security, database, know-how protection, compliance or product safety perspective, for example: the privacy and e-communications directive, the directive on trade secrets, the NIS-Directive, the Cyber-Security Act, the directive on the free flow of non-personal data, the directive on general product safety, the database directive as well as directives on equal treatment and against discrimination and equal opportunity in the employment context, and rules applicable to EU institutions and bodies or the police and justice sector.

There are numerous national data protection laws and laws with specific provisions pertaining to the processing of personal data, even within the European Union as the General Data Protection Regulation has dozens of “opening clauses” that either provide or allow for national rules: for certain areas (e.g. processing of personal data in the employment context, see GDPR Art. 88) or for certain types of data (e.g. processing of national identification numbers). Depending on the use case in question, further laws may be applicable such as consumer protection and e-commerce or competition laws for marketing activities or labor, equal opportunity and industrial constitution laws in the employment context. The same is true for products or “connected devices” with a particular focus on information and cyber-security provisions and rules that apply to the so-called “Internet of Things”.

In terms of existing rules and regulations, it is important to take note of the fact that already at present, various sector / industry specific (e.g. banking: high frequency algorithmic trading), or product specific (e.g. medical devices) as well as purpose (e.g. facial recognition, autonomous driving, autonomous weapons) and data specific (e.g. biometric data, genetic data, health information) laws exist which must be obeyed when Big Data applications and algorithmic systems are used. In shall furthermore be noted that some states within the U.S.A. either already introduced or are working on laws that specifically deal with algorithm-based data processing and automated decision-making, and several states introduced specific provisions for (the ban of) facial recognition technology. Facial recognition may lead to serious threats because it could be used for undesired (unlawful) data processing as the case of ClearView showed. In addition, this technology has the potential for discrimination and could also be used for surveillance purposes, and that is why many raised concerns from a human rights point of view.

In recent years, many countries introduced their own privacy bills with requirements that are similar to those set forth in the GDPR and which grant consumers various rights such as access, portability, correction, deletion, and the right to object to the processing of their data in certain circumstances; other laws requires opt-out for targeted advertising and profiling decisions that produce legal or similarly significant effects and foresee that mandatory data protection impact assessment must be carried out for certain processing activities including profiling. Documentation requirements and data subject rights often sound familiar, however, the scope is not the same as some laws are rather concerned with consumers than individuals, but that does not necessarily mean that the level of protection is lower: California introduced the “Do Not Sell Rule” which allows individuals to opt-out of the sales (including sharing) of their personal data – in contrast, the much-discussed "Do Not Track" browser option does not seem to have caught on yet.

It can therefore be said that the codification and regulation of systems and applications that use Artificial Intelligence is not in their infancy as there is already a variety of laws and guidelines that govern the use of AI. This is not surprising since such technology is already being used across the board, for example, in production (robotics), operations (forecasting), marketing (analytics), finance (scoring), healthcare (diagnostics), in “smart cities,” “smart homes,” and “smart devices” and as well as for (behavioral, online, location) tracking and targeting purposes.

GDPR is a European regulation that is applicable internationally, however, the envisaged harmonization of privacy laws was not achieved, not even within the EU: Differences in the interpretation as to the scope of data privacy laws and in particular data subject rights – the right to information and the right to copy are perfect examples – resulted in privacy being far less uniform than generally assumed. Fragmentation and lack of harmonization can be best explained in the field of marketing activities and employment law, both of which are areas of high importance to businesses: GDPR only mentions marketing in one of its Recitals but does not explicitly cover such activities; GDPR moreover has dozens of “opening clauses” with either allow or foresee for national provisions, even in such important areas like employee data protection. Therefore, depending on the case in question, companies must consider various regulations on top of data protection rules. In the area of marketing, that would be consumer protection, e-commerce or competition laws; in the area of employment, that would typically be co-determination or legislation concerning health at work – the recent COVID crisis has shown how significant the intersection of different areas of law can be.

GDPR enforcement is also a challenge: while we have seen several multi-million dollars fines, there has also been a series of fine failures with drastic reductions of penalties of up to 90 % which showed that imposing administrative fines under GDPR might not be easy, because administrative, procedural as well as commercial criminal laws must be taken into consideration as well.

In terms of GDPR-specific challenges and the question whether GDPR addresses processing with the help of Big Data, ADM and AI, it can generally be said that GDPR's fundamental principles like accountability, transparency, data accuracy and quality, fairness, purpose specification as well as its permission- and risk-based approach (accompanied by appropriate technical and organizational measures) together with a dedicated set of individual rights form a sound foundation for data privacy.

GDPR is also not silent on various topics that are highly relevant for Big Data, ADM and AI, e.g., consent, profiling, automated decision-making, data subject rights, admissible re-use of personal information, international data transfers, transparency, data security or special categories of personal information. But this is also an example of areas in which the framework might have failed: GDPR (definitions) are concerned with "original data", not "derived data", but that seems needed as the minority of data that is being processed in Big Data and AI applications has been collected directly form the individual. These circumstances raise further questions from a business and an individual's perspective, e.g., with regards to copyrights database rights and legal personhood of robots, or regarding the idea of data ownership.

GDPR itself has numerous ambiguities and uncertainties. On the one hand, data subject rights are strengthened but on the other hand, there is also an emphasis on legitimate interests. Compatible processing which is admissible under the conditions set forth in GDPR Art 6 IV is another example, and some fear that compatible processing may lead to unlimited processing.

There is also controversy about whether profiling under GDPR Art 22 shall be interpreted as a prohibition or a data subject right, and there is very little case law to explain GDPR Art 21, the "*right to object, on grounds relating to his or her particular situation*". The fact that the standard of GDPR Art. 22 is only applicable if the decision is "*based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*" sounds like a guarantee, but it also shows that there is a limit to this right. Fully automated means that there is no human intervention at all, but this can be circumvented fairly easy by implementing spot checks. It is also not always clear what has the quality of a decision (or similar legal effect): does that only apply to a final (job candidate selection, loan or housing application, etc.) decision or should this rather be regarded as a constant criterion for the design of Big Data and AI applications, and thus be applicable at every relevant processing phase. GDPR is perhaps not as far-reaching or future-proof in terms of data subject rights.

As already mentioned, some U.S. laws already introduced “Do Not Sell” as an individual right, and if that is taken seriously, then this is more than what GDPR Art. 12-18 and 19 want – not just a “*notification obligation regarding rectification or erasure of personal data or restriction of processing*” in the sense of an onward duty, but preventing that an individual’s personal information is provided to other (unknown, unlimited number of) entities and monetized. This approach underlines the awareness for the value of data, the importance of data sovereignty and the significance of today’s data-driven businesses which some describe as “surveillance capitalism.”[1418]

One of the most important observations is that some approaches have failed in practice, and that makes the viability of traditional data protection (i.e. rights based) concepts questionable: consent and privacy self-management does not seem to afford the desired individual protections, and it not the same like comprehensibility or replicability of individual decisions or the demand for making “true operators” known, which would be especially important as many controllers and processors may be involved in processing operations, but this is not what the front-end user of (online, mobile, etc.) applications gets to know.

Consent is another well-established concept in privacy, but consent can factually hardly work given the information mismatch, and psychologically, privacy self-management does not work given the inconsistency between peoples’ opinions on the relevance of privacy and their actual behavior which tells a different story.

The principle of accountability is a common thread running through data protection regulations, but the question is whether accountability as set forth in existing data privacy laws goes far enough to guarantee responsibility, liability, contestability, safety and fairness together with an approach to data processing that includes sound risk assessment and human oversight and human intervention if need be. That is why in summary, many believe that traditional rights-based concepts no longer fit the era of Artificial Intelligence.

In addition, it seems that certain mechanisms have simply not been used in practice, for example GDPR Art. 80, the representation of data subjects which allows the “*data subject shall have the right*

[1418] Shoshanna Zuboff: The Age of Surveillance Capitalism – The Fight for Human Future at the New Frontier of Power. Profile Books, 2019.

to mandate a not-for-profit body, organization or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law."

As a reaction to the above-mentioned issues, there have been controversial discussions on how to best address these matters: While some predict that new approaches are needed, others stress that existing legal framework shall be exploited, including well-established standards like joint controllership, which is particularly important as Big Data and AI applications in many cases involve more than just one controller, more than just one service provider, and more than just one site where data are processed and stored, which leads to the topic of international data transfers.

An important development in this regard is the invalidation of the "Privacy Shield" by the European Court of Justice in summer 2020. Big Data and AI are complex processing operations, and many of them are unimaginable without a multitude of vendors and multiple data handling and (cloud?) storage locations, which leads to further questions regarding alternative transfer mechanisms, data localization requirements or potential technical solutions such as encryption. Despite the confirmation of the validity of (renewed) Standard Contractual Clauses and regardless of the fact that numerous authorities came up with guidance on transfer impact assessments and the like, companies are left with a certain degree of uncertainty when it comes to considerations for international data transfers, because many questions are unanswered – be it with regards to possible derogations in accordance with GDPR Art. 49, or with regards to California, the home of many Tech Giants, having an adequate level of data protection (GDPR Art. 45 III refers to a third country or *territory*), or regarding possible technical solutions like encryption or data trustee models which, on the one hand, allow for data transfers, but on the other hand, avoid undesired access to personal information.

The factual problem is that some promising data trustee models have been discontinued, and the legal problem is that government access to personal information is neither novel nor unique to the U.S.A. It is a given in the U.S. and in the EU, the difference being that there is little public awareness of regulations like the E-evidence Regulation that allows for cross-border access to electronic evidence.
The situation for globally active corporations is further complicated by the fact that there are dozens of national laws that foresee local storage of personal information. But "*technically speaking, physical access to a server is neither a necessary nor a sufficient condition for access to information, and logical access is both necessary, and may be sufficient to provide access to data in an intelligible*

form, regardless of the geographic location.”[1419] Data residency requirements do not really do privacy a favor: principles like data minimization, data integrity and confidentiality may not be met if companies must establish and defend multiple versions of its systems across continents with additional hardware, additional vendors and additional staff having access to that data. In addition, legally binding global trade agreements in fact address the issue of international data transfers and stipulate protections against unjustified data localization requirements.

The Thesis explained what kind of risks may result out of the application of Big Data and AI systems, algorithmic processing or automated decision-making and profiling, and a common effect of Big Data, ADM and AI is the secondary use of personal information. Compatible re-use of personal data is admissible to the extent the conditions of GDPR Article 6 (4) are met, i.e. considering the nature of the data in question, the context in which the data were collected, the relationship between the purposes for which the data have been collected and the purposes of further processing, the impact of the envisaged data processing on the data subjects, and the safeguards applied by the controller. Since a major characteristic of many AI applications is a certain degree of autonomy with systems being able to perform in an unsupervised manner, it is questionable whether such data processing operations meet all these requirements or if that may lead to indefinite re-use of personal data which could also render purpose and storage limitation obsolete.

Furthermore, data aggregation and data maximization go hand in hand with most Big Data and AI applications, simply because large (training) datasets are needed for the majority of use cases. Big Data is about turning volume to value, but that may conflict with GDPR’s principle of data minimization, and it may pose a threat to individuals insofar as there is a risk of (re-)Identification: the more datasets grow, and the more data is attributed to a person, the easier it gets to identify the person behind the dataset, and various studies confirmed that actually not much information is needed to uniquely re-identify individuals. The usual practice of constant “enrichment” of datasets further adds to the risk of identification and profiling: if one and the same person is “constantly analyzed and scored” this may result in detailed profiles and (online) “identities” the person is not aware of.

Another problem of Big Data and AI applications is that, quite often, external (collateral) data are processed. The upload of address books to social media platforms is a simple example of this risk: whenever a user uploads his individual contacts to a social media platform, the platform receives a full set of contact information of other individuals, and these individuals may not have been informed nor did they consent to such data collection.

[1419] Christopher Millard: Forced Localization of Cloud Services: Is Privacy the Real Driver? Paper provided for the 2015 forthcoming in IEEE Cloud Computing. Article published May 14, 2015, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605926. Retrieved October 22, 2021.

Further potential risks of AI applications are opaqueness and lack of human oversight: a challenge with Artificial Intelligence is that quite often, important factors are unknown, e.g. details of the processing operations, and the “true operators” behind those algorithms in the sense of who exactly is responsible for which part of the processing. In many cases, input and output are known, but the workings in between are not, is also known as the “black box effect”. Some argue that there are three distinct types of opaqueness which can be distinguished: intentional opacity when the inner workings of the system are deliberately concealed, illiterate opacity when the inner workings are opaque since only those with expert knowledge understand how it works, and intrinsic opacity due to a fundamental mismatch between how humans and how algorithms understand the world. The ability of AI to act autonomously and in unforeseeable ways adds to the fear that certain types of AI systems may be considered a “Kafkaesque system of unreviewable decision-makers”, and that explains why human oversight may be at risk when algorithms are used for the processing of personal information.

Closely connected to the issue of oversight are question of responsibility and liability: while accountability is established as a privacy principle and rated as an important value in literally all publications, fewer texts deal with the fact that AI has the potential to challenge the traditional notions of legal responsibility (and legal personality). In this regard, the European Parliament and the European Commission provided various publications, for example on liability issues in respect of autonomous robots, liability (and safety) implications of Artificial Intelligence and the Internet of Things, or a report on liability for other emerging technologies. In their papers, the EC and EP explain their key findings with regards to new duties of care, strict and vicarious liability, the burden of proof as well as insurance issues.

From an individual’s perspective, the question would probably primarily be whom to turn to: a court or a regulator or a company, and if so, which one: from a GDPR perspective, there are controllers, processors and joint controllers, but the problem is that and more laws introduce more “players”: e.g. the DGA, mentions, amongst other things, “data holders” and “data users”, and looking at the categorization of relevant players within the draft AI regulation, the situation becomes even more complex as there are providers, manufacturers, distributors, importers – how should an average person without corresponding expertise be able to tell who is responsible for which part and under which conditions.

Big Data and AI applications in many cases raise further concerns, which is a situation literature describes as the information mismatch: companies must be transparent about the processing of personal data, but even GDPR itself sets limits to transparency obligations: Article 13 (2) lit. f limits the obligation to information about “*the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the* *logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*".

Details about the significance as well as envisaged consequences of the processing are relative insofar as dynamic processing may simply not allow to foresee all relevant consequences; details about the underlying logic are relative insofar as meaningful information is simply not the same as comprehensibility or reproducibility of decisions. Companies may moreover argue with trade and businesses secrets to avoid having to disclose underlying algorithms they use.

Another factor that adds to the mismatch is the dilemma of information asymmetry between users and (Internet, online) service providers, and the situation is worsened by the fact that users in many cases are not aware that seemingly "free services" may not really come without a service in return, which explains the famous quote that, "*if you are not paying for a service, you are the product*."[1420] The problem is that individuals unlike companies do not dispose of enough information to defend themselves "against being sorted in the wrong bucket".

The above circumstances underline the challenges with privacy self-management. Even if lack of transparency is not the problem, transparency as such is problematic since the ineffectiveness of transparency requirements seems to be proven by now: people are as badly informed as they are overtaxed with long and complex privacy notices; people routinely turn over their data for small benefits; people care much more about price-sensitive information than about data protection information; people are much more concerned about social privacy than about institutional privacy, and if people are about to decide about their privacy preferences, they tend to make their lives easy and accept all default settings instead of taking their time to really decide on relevant settings. Even worse, certain Apps take advantage of psychological (behavioral) patterns that can reinforce loss of user control, and legislation on such dark patterns is just in the process of being created.

Some authors describe the afore-mentioned challenges around information obligations as the transparency paradox. They compare interactions with Big Data platforms with a poker game "where one of the players has his hand open and the other keeps his cards close". The controversy around the use of cookies and the like showed that transparency and consent are difficult to achieve and that privacy self-management in many instances is only about a take-it-or-leave-it-approach, a mere click-mechanism.

[1420] Ben Kepes: Google Users - You're The Product, Not The Customer. Article published December 4 2013, available at https://www.forbes.com/sites/benkepes/2013/12/04/google-users-youre-the-product-not-the-customer/#:~:text=The%20old%20adage%20goes%20that%20if%20you%27re%20not,up%20advertising%20to%20users%20of%20these%20free%20products.

This leads to the next issue, the control paradox, i.e., the problem that affording more control to users does not help them to better protect their privacy. It seems that the opposite is true: affording more control to users does not necessarily lead to a better protection of their data – this may even induce them to reveal more information: if people feel that they have control over their data, they tend to provide more data about themselves. Related observations are known from other fields, for example in the framework of the introduction of the safety belt legislation as people felt more secure with safety belts and drove less carefully.

The control paradox is connected to another problem, the security paradox: Data protection and data security are inseparable, and that is why security measures such as access controls are principally indispensable. But any such measures require the processing of personal data such as log-in data, and the general risk is that the more data are processed, the larger the risks that data are somehow compromised. More and more often, users are required to provide a fingerprint in the framework of the authentication process, and that may lead to further risks: nowadays, many devices require the use of biometric data, but the problem is that, unlike a password, there is no reset process for a unique fingerprint, and what is worse, such data can be manipulated very easily, because access to a used object is sufficient to reproduce a fingerprint, and if fingerprints are a mandatory part of official ID-documents, then the individual concerned has a serious problem.

Another effect which is connected to the security paradox can be described as the trust paradox: a growing number of people are so used to relying on all kinds of Apps as their "single source of truth" that there does not seem to be any more room left for own decision making, and that has an impact on how they handle their data. Recently, similar findings were made in the framework of the introduction of "COVID apps": the mere fact that technology can track cases of infections does not replace other necessary measures to prevent infections.

AI can be used in novel ways, for example by exploiting human vulnerabilities (e.g. through the use of speech synthesis for impersonation), by exploiting existing software vulnerabilities (e.g. through automated hacking) or the vulnerabilities of AI systems (e.g., through data poisoning or by introducing training data that causes a learning system to make mistakes or by inputs designed to be misclassified by machine learning systems. The latter is a particularly important aspect because AI itself may be vulnerable as well – if AI systems can exceed human performance, they may also fail in ways that a human never would.

Another point to consider is the risk of malicious use of AI, because so far, much more attention has been paid to beneficial applications of AI than the ways in which Artificial Intelligence could be used maliciously. Some predict that the growing use of AI systems will change the landscape of threats, because adequate defenses to potential security threats from malicious uses of AI are not yet developed. A recent report surveyed potential security threats in the area of Artificial Intelligence and came to the conclusion that the use of AI will expand existing threats and change the typical character of threats, because AI may simply lower the costs of attacks since AI is scalable and can complete tasks that would ordinarily require human labor, intelligence and expertise.

The use of AI for malicious purposes could be especially effective, because it could be finely targeted, difficult to attribute, and thus likely to exploit vulnerabilities (e.g., by using speech synthesis for impersonation), and complete tasks that would be otherwise be impractical for humans (e.g. labor intensive attacks). In consequence, a new quality of malicious actors may emerge, which reinforces the conclusion some make that, certain types of AI should be treated as dual-use technology, which shall result in a corresponding (appropriate) legal framework as is the case for weapons, chemicals or medicinal products. There is good reason why data protection laws traditionally foresee that impact assessments or similar documentation is necessary as a first step when new technology is used, or when systems are deployed that allow for systematic / extensive / large-scale processing of personal information, or when the processing may involve high risks for the rights and freedoms of individuals or lead to decisions that may have significant (negative, legal) effects on individuals.

Since AI helps with the transformation of businesses, AI will consequently also have an impact on workforce. We have come to a point where not only monotonous tasks in production lines or computer-assisted customer care operations care can be automated by robots or chatbots. Complex operations can be automated as well, and even the legal profession may be severely impacted by this new kind of virtual workforce, because tasks like document classification, summarization, comparison, knowledge extraction, discovery and retrieval are more and more based on technology, and less on human work. Against this background, discussions around potential negative employment effects of AI commenced, including ideas like specific taxes on AI-performed tasks or the introduction of an unconditional basic income to secure livelihoods. At the same time however, some say that the lack of access to new technologies in less developed countries will further increase inequalities between individual populations and countries. The impact on AI on the digital economy was also raised by numerous international institutions who stress that AI shall, amongst other things, respect internationally recognized labor rights. Fact is that today, even getting a job starts with AI because resume screenings and background checks are very often being automated, and the draft AI Regulation addresses employment and recruitment issues and classifies AI applications used for such purpose / in this sector as high-risk applications.

Further risks that have been discussed in the context of Artificial Intelligence are the potential for discrimination for surveillance: the probabilistic nature of individual decision-making and profiling is highly desired from a business perspective, but their inherent opacity together with their potential for discrimination and discrimination is problematic from an individual's perspective, and that is why many believe that these two risks are probably the most important dangers from the point of view of those affected. There consequences of such risks are far-reaching: employers may turn down job candidates based on social media information without providing candidates with an opportunity to comment on their findings, and this explains the problem of information injustice and information inequality.

Some object to the use of AI applications in field of welfare, public administration and jurisprudence as this may either pave the way or strengthen existing injustices or even restrict the legal process, and consequently, limit access to justice.

Demonstrable bias in recidivism scoring systems or bias in healthcare are quite dramatic examples, and they show that AI risks affect individuals and society – also because AI may even threaten physical security, for example by using drones or by subverting or manipulating critical infrastructure.

The case of Cambridge Analytica demonstrated that the use of Artificial intelligence has a political dimension as well: Influencing voters is traditionally at the core of any campaign, but the problem is that there is little transparency and awareness of how sophisticated this technology is and how cleverly it can be used: AI could be used to create targeted propaganda or to manipulate photos (for morphing purposes) and videos (for deepfakes) and this way, pose a threat to democracy.

In the context of possible risks of Big Data and AI applications, many authors commented on the potential of Big Data and AI applications to conflict with a variety of basic privacy principles such as purpose limitation or fairness and transparency which seem to be rendered obsolete.

Others demonstrated that, even if privacy principles are applied, there is a risk of trade-offs between different data protection principles. Such tensions may arise between the principles of accuracy, fairness and privacy, for example: more data may lead to more accuracy, but at the expense of individual's privacy; if AI is tailored to avoid discrimination (if certain indicators are removed to that AI is fair), this may have an impact on accuracy; if AI is tested to see if it may be discriminatory, it needs to be tested by using data that is labeled by protected characteristics, but that may be restricted under privacy laws that govern the processing of special category data.

As regards a possible future framework for Big Data and AI, there have been numerous individual conceptions: Some authors claim that there is a general need for additional (specific) AI laws, for example for employee data protection, to facilitate the handling of research data or for the "Internet of

Things". Other initiatives deal with the idea of mandatory labeling, or a specific liability regime in accordance with product liability regulations which should cover all involved providers. Further recommendations for the future regulation of AI stress the importance of technical standardization or certifications, the need for external control mechanisms including the establishment of specific AI oversight bodies or compulsory public archives and the introduction of termination obligations in the event a system gets out of control up to the strict prohibition of certain technology such as facial recognition.

From an individual's perspective, some stress the need for enhanced redress mechanisms including rights of association action, the right to human intervention and the right to participation or the right not to be subject to a discriminatory decision and secret profiling. They moreover address enhanced transparency which would include explicability of data processing and replicability of individual decisions and making true operators known; they demand the use of anonymized and synthetic data shall be forced whenever possible and discuss the idea of having personal information replaced rather than having the processing restricted, because that might be a more effective way to avoid re-identification. There are also debates about data ownership to fight data monetization.

Given that the mass application of Big Data, AI and automated decision-making not only affects individuals, but society, many initiatives elaborated on embedding ethics into Big Data, ADM and AI, and focused on a human-centric approach that does not harm, but which serves society. However, this approach was criticized as some consider that ethics may be an escape from regulation.[1421]

In the context of the potential future legislation for algorithmic processing and decision-making as well as AI, it should moreover be noted that some legislative proposals which, at first glance, do not suggest having provisions on consumer and / or data protection, in fact have rules that are relevant from a data subject perspective: Transparency, security, documentation, evaluation and oversight requirements are topics that are relevant to data privacy and are covered by various regulations that govern online content, electronic communications, the Internet of Things or the (re-) use of public sector information. Several legislative proposals qualify in this regard, for example the proposal for a Regulation on electronic evidence in criminal matters or the proposal for a review of the Directive on the re-use of public sector information, the Machinery Regulation or the Digital Services and Digital Markets Act and the Data Governance Act.

The proposal for a Regulation on Artificial Intelligence immediately attracted a lot of attention and has received numerous comments: positive ones due documentation and evaluation requirements and

[1421] Ben Wagner: Ethics as an escape from regulation. From ethics-washing to ethics-shopping? In: Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds,): BEING PROFILED: COGITAS ERGO SUM. 10 Years of Profiling the European Citizen, 2018: Amsterdam University Press, 84-88.

owing to the establishment of a European AI Board and a public database; negative ones for unclear definitions, the missing right to compensation, numerous exceptions, and the "*missed opportunity to draw red lines for certain technologies*."[1422] But the proposal for a Regulation on privacy and electronic communications alone is probably the best example of how hard it is to assess the situation appropriately: There is controversy around the draft E-Privacy regulation for many years now, and it is possible that the same could happen to the draft AI regulation owing to the high business significance of this initiative. Therefore, at this stage, only an overview and outlook on potential developments in the legal landscape relevant to Big Data and AI applications can be given.

As a reaction to the emergence of Big Data and AI as an economic and societal given lead to a variety of initiatives that dealt with the issue of addressing risks of Big Data and AI. Recently, there has been a significant increase of initiatives that deal with the issue of addressing risks of Big Data, ADM and AI at international, intergovernmental, EU as well as local / national level. Numerous proposals address the matter from different perspectives, e.g., from a regulatory, governance, assessment, data subject rights perspective:

At international level, the paper OECD's AI principles as well as the G20, G7 and World Economic Forum recommendations on AI. Ditto for various initiatives and declarations the United Nations provided, for example, UNESCO, UNICRI, UNICEF or UN's Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.

As for guidance and recommendations at European level, the following initiatives are examined (non-exhaustive): the European Commission's White Paper on Artificial Intelligence, the Ethical Charter on the Use of AI in Judicial Systems, the Resolution on Civil Law Rules on Robotics, Council of Europe Recommendations as well as ethics guidelines for trustworthy AI – the latter is also a good example that the majority of these initiatives focus on ethics, including UNI Global Union's Principles for Ethical Artificial Intelligence or IEEE's Ethically Aligned Design.

The same is true for various expert guidelines, civil society and multistakeholder recommendations such as the Toronto and the Montreal Declaration or papers published by the Future of Life Institute and the Centre for Information Policy Leadership (non-exhaustive). There is also considerable intergovernmental cooperation with regards to Artificial Intelligence, e.g., OECD's Network of Experts on AI, UNESCO's Ad Hoc Expert Group, EU's High-level Expert Group on Artificial Intelligence or the Global Partnership on AI.

[1422] Friederike Reinhold, Angela Müller: AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence – A major step with major gaps. Article published April 22 2021, available at https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/. Retrieved October 22, 2021.

As regards to expert / multistakeholder / NGO guidelines, it can be said that these initiatives have in common that they intend to provide useful recommendations for the use of Artificial Intelligence, however, they vary insofar that some guidelines focus on the ethics and responsible use of AI including the future of work, whereas other recommendations are concerned with the classification of AI systems. Most of these papers underline the importance of awareness raising and emphasize the relevance of a human-centered approach to AI and the need for the protection of privacy and intimacy, as well as human control and oversight.

Notwithstanding differences as regards strategy and methods, these initiatives show certain parallels which could be summarized as follows: a new kind of transparency that exceeds existing standards and ranges from the explicability and replicability of decisions, failure transparency as well as making “true operators known” to public consultation and/or public registries for high-risk AI use cases.

Some of these guidelines discuss a new kind of accountability which shall include “all players” in the data value chain (onward responsibility) and suggest specific audits for AI applications, further independent oversight bodies and public safety obligations.

The papers furthermore deal with new requirements such as mandatory human rights impact assessments and termination obligations in the event a system gets out of control. Some of the statements recommend advanced individual rights such as general the right to human intervention and determination as well as enhanced access and redress mechanisms, and others discuss the introduction of further principles such as non-discrimination and inclusion, equality and diversity that should be applied whenever algorithmic processing is in question.

These initiatives also address judicial and societal implications of AI applications and elaborate on how to best ensure fair trial and access to justice and welfare how to best protect the freedom of expression, assembly and association, and the right to work in an era of growing automatization and digitalization.

Finally, some papers propose the strict prohibition of certain AI uses, for example secret profiling and unitary scoring or facial recognition. In contrast, other opinions stress the relevance and application of existing principles and (enforcement) mechanisms like the fairness, accountability, transparency, data quality, accuracy and provenance, privacy by design and by default, joint controllership, the need for (explicit) consent or technical and organizational requirements which constitute substantial part of most data privacy and data security laws.

There are also interesting alternative approaches to issues that arise with the use of Algorithms and Artificial Intelligence such as the call for a Hippocratic oath for data scientists or initiatives that deal with the question how privacy bills should (not) be written: these authors question the concept of rights-based governance where individual rights function as the primary mechanism for governing the collection and processing of personal data since that puts the burden of privacy controls on the individual rather than the controller as such a conventional approach might not be appropriate in an era of more and more "surveillance-based business models".

The "AI arms race" has also resulted in numerous national AI initiatives and strategies around the globe, all pursuing the same goal – to become a leader in Artificial Intelligence: the U.S.A. is home to world-famous Big Tech companies and innovation; the fact that numerous laws that specifically deal with AI such as the Artificial Intelligence Act, the Algorithmic Accountability Act, the AI in Government Act, the Future of AI Act, the Artificial Intelligence Reporting Act, the National Artificial Intelligence Initiative Act, the Advancing AI Research Act, the Growing Artificial Intelligence Through Research Act show the nation's strong wish to shape the American AI policy.

China is also heavily engaged in AI, the nation released an "Artificial Intelligence Development Plan" and established an AI Governance Expert Committee as well as AI-focused industrial parks. Similar developments can be observed in many countries, throughout various jurisdictions, and business sectors.

A noteworthy development in this context is that the UK, which has well-established tech landscape and is traditionally strong in the area of research, announced that it intends to take advantage by the opportunity afforded by the UK's exit from the European Union to reform the UK's data protection regime, including plans to revisit the nation's AI strategy: this might have implications for data protection as there are discussions around softening the conditions around (re-)use of personal data and considerations if data protection legislation and the ICO is the right forum and regulator for determining fairness in profiling and automated decision-making.

In summary, a common feature of many international, intergovernmental, multistakeholder, civil society initiatives and expert guidelines is that they focus on established principles like accountability, purpose specification, collection and use limitation as well as data quality, security, but also stress the need for enhanced transparency and individual participation which they claim shall be taken more seriously and enforced correspondingly. However, the nuances within call for "enhanced transparency" and "individual participation" goes beyond existing standards, and these two demands show that what is at stake here is the desire for further development of existing conditions which would result in new standards. The right to participation is more than the right to information, and if "enhanced transparency" includes the need for public registries for (audited) AI apps, this is also more than a mere public-facing privacy notice with a brief explanation of the underlying logic.

An analysis of propositions relating to AI applications shows that the majority of proposals suggest that any future AI regulations or AI principles shall take the following into consideration: accountability and responsibility, human control of technology, safety and security, transparency and explicability, fairness, non-discrimination as well as privacy and the promotion of human values, which contains the following (main principles within each theme):[1423]

Privacy: Privacy, Privacy by Design, Consent, Control over Use of Data, Ability to Restrict Processing, Right to Rectification, Right to Erasure, Recommendation for Data Protection Laws.

Accountability: Accountability, Evaluation and Auditing Requirement, Impact Assessment, Verifiability and Replicability, Liability and Legal Responsibility, Remedy for Automated Decision, Ability to Appeal, Creation of a Monitoring Body, Recommendation for New Regulations, Environmental Responsibility.

Transparency and Explainability: Explainability, Transparency, Open-Source Data and Algorithms, Notification when Interacting with an AI and when AI Makes a Decision about an Individual, Regular Reporting Requirement, Right to Information, Open Procurement (for Government).

Fairness and Non-discrimination: Non-discrimination and the Prevention of Bias, Fairness, Inclusiveness in Design and Impact, Representative and high-quality Data, Equality.

Human Control of Technology: Human Control of Technology, Human Review of Automated Decision, Ability to Opt out of Automated Decision.

Professional Responsibility: Multistakeholder Collaboration, Responsible Design, Consideration of Long-Term Effects, Accuracy, Scientific Integrity.

Promotion of Human Values: Leveraged to Benefit Society, Human Values and Human Flourishing, Access to Technology.

Safety and Security: Security, Safety and Reliability, Predictability, Security by Design.

[1423] Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy, Madhulika Srikumar: Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. Berkman Klein Center Research Publication No. 2020-1 published February 14 2020, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482. Retrieved October 17, 2021.

The following conclusions which also form the main hypotheses underlying this work, can be drawn: It can first be determined that privacy self-management as a rights-based concept failed, for a variety of reasons, for example considering that data subject rights do not lead to the desired protections, taking into consideration that valid consent is difficult to imagine given the existing information asymmetries, owing to admissible or secondary use of personal information, or due to transparency obligations being restricted.

Second, transparency needs to be further developed, moving from mere notice-level summary-format information which addresses individuals in the direction of meaningful information on underlying algorithms for all data subjects concerned as well as public registries allowing the public to access relevant information such as details on risk evaluations, mitigation measures and information on sub-processors. This may increase the chances for the needed social debate for this important technology that has the potential to shape our lives, and it could also allow to better exercise individual's rights and foster individual engagement, which is a factor that should not be underestimated as a single activity has brought down an entire data transfer mechanism. The success of such initiatives can be compared to the functioning of the fourth pillar of the state which, in addition to the executive, legislative and judicial branches, can influence developments through reporting and public discussion.

This idea forms the transition to the next conclusion and leads to the third main hypothesis, which is that new controls and constraints are needed that are based on public debate and include new values which are not only judged from an individual's perspective but consider the societal perspective since issues AI's dual use character, its capability for surveillance and the potential impact on human rights and democracy as well as digital workforce aspects show that there is an important intersection between individuals rights and societal values. Frances Haugen's leaks on Meta practices such as design decisions that may influence the spread of misinformation or have a negative impact on users' mental health which caused lawmakers to invite her to testify[1424] show both, that public discussion is needed to allow for better insight into how AI can be used, and that self-regulation does not work.[1425] While it is comprehensible that industry may prefer a deregulated landscape when it comes to using novel technology, because it is argued that regulation stifles innovation, "*legislative history in the course of industrial revolutions and across various sectors, be it transportation, chemical engineering, communications, aviation or biotechnology and digitization has shown that voluntary codes or self-regulation may simply not work, and that regulatory discussions should not primarily focus on specific*

[1424] Ryan Browne: Facebook whistleblower behind major leak is going to testify in Europe
Article published October 12 2021, available at https://www.cnbc.com/2021/10/12/facebook-whistleblower-behind-major-leak-is-going-to-testify-in-europe.html. Retrieved January 22 2022.

[1425] MEP Christel Schaldemose is quoted by Euronews in their October 5, 2021 news entry: Frances Haugen whistleblower leaks show Facebook cannot regulate itself, MEPs say. Article available at https://www.euronews.com/next/2021/10/05/frances-haugen-whistleblower-leaks-show-facebook-cannot-regulate-itself-meps-say. Retrieved January 22 2022.

harms or individual risks but also take the systemic and structural risk of Artificial Intelligence into consideration.[1426] Therefore, voluntary codes and ethics standards may not be sufficient to mitigate the risks posed by Big Data, automated decision-making and Artificial Intelligence because AI applications may have an impact on human rights, and legislation alone is required to protect human rights. A starting point in this regard could be mandatory certifications, and public registries – steps which are already foreseen in some draft recommendations for the future regulation of Artificial Intelligence. There is a need for clear statements on red lines which includes bans on certain use cases such as private facial recognition databases and facial recognition surveillance by public authorities as well as social scoring to rate citizens' behavior, because such uses of Big Data and AI may have an impact on fundamental rights such as freedom of expression,[1427] freedom of assembly and association,[1428] liberty, security[1429] and fair trial,[1430] physical, psychological and moral integrity,[1431] as well as prohibition of discrimination.[1432] Even though the United Nations recently failed to ban "*slaughter-bots*" which some call an epic failure[1433] because algorithmic errors in this context do not cause simple IT bugs that need to be fixed, but could lead to the elimination of whole cities,[1434] the fact that the European Parliament[1435] and the Council of Europe Committee on Artificial Intelligence[1436] addressed these issues gives cause to hope.

[1426] Julia Black, Andrew Murray: Regulating AI and Machine Learning: Setting the Regulatory Agenda, European Journal of Law and Technology, vol 10, issue 3, 2019. An online version of the paper is available at https://ejlt.org/index.php/ejlt/article/view/722/980. Retrieved October 22, 2021.

[1427] See UDHR Art. 19 and ECHR Art. 10.

[1428] See UDHR Art. 20 and ECHR Art. 11.

[1429] See UDHR Art. 3 and ECHR Art. 6.

[1430] See UDHR Art. 10 and ECHR Art. 47.

[1431] See UDHR Art. 3 and ECHR Art. 3.

[1432] See UDHR Art. 19 and ECHR Art. 21.

[1433] Sam Shead: UN talks to ban 'slaughter-bots' collapsed – here's why that matters. Article published December 22 2021, available at https://www.cnbc.com/2021/12/22/un-talks-to-ban-slaughterbots-collapsed-heres-why-that-matters.html. Retrieved January 22, 2022.

[1434] It is reported that robots already killed humans: https://undocs.org/S/2021/229. Retrieved January 22, 2022.

[1435] Source: https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html. Retrieved October 23, 2021.

[1436] Source: https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da. Retrieved October 23, 2021.

Bibliography

Martin Abrams: Time to break the privacy legislative paradigm – IAF Model Legislation. Article published June 3 2021, available at https://informationaccountability.org/2021/06/time-to-break-the-privacy-legislative-paradigm-iaf-model-legislation/.

AccessNow: Europe's approach to artificial intelligence: How AI strategy is evolving. Report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf.

Max Adamek, Julian Räder: DSGVO-Verstöße und das OWiG. Article published August 20 2021, and is available at https://haerting.de/wissen/dsgvo-verstoesse-und-das-owig/#:~:text=Gem.%20%C2%A7%2030%20Abs.%201%20Nr.%205%20OWiG,handelt%20und%20eine%20Straftat%20oder%20Ordnungswidrigkeit%20begangen%20hat.

AI Now Institute: 2019 Report. Report published in December 2019, available at https://ainowinstitute.org/AI_Now_2019_Report.pdf.

Kenneth Anderson, Matthew Waxman: Law and Ethics for Autonomous Weapon Systems: Why a ban won't work and how the laws of war can, American University Washington College of Law Research Paper No. 2013-11. The article is available at http://ssrn.com/abstract=2250126.

Julia Angwin, Jeff Larson, Surya Mattu, Lauren Kirchner: Machine Bias: There's software used across the country to predict future criminals. Article for ProPublica published May 23 2016, available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Sebastian Bader, Pascal Hitzler: Dimensions of Neural-symbolic Integration – a structured survey. Article published November 10 2005, available at https://arxiv.org/pdf/cs/0511042.pdf.

Jennifer Baker: EU Commission aims to ban forced data localization. Article published October 24 2016, available at https://iapp.org/news/a/eu-commission-aims-to-ban-forced-data-localization/.

Jennifer Baker: California Dreamin': Is a Single State EU Data Protection Deal on the Cards? Article published published January 20 2020, available at https://www.cpomagazine.com/data-protection/california-dreamin-is-a-single-state-eu-data-protection-deal-on-the-cards/.

Jennifer Baker: EU Parliament debates: Could California be considered 'adequate' on its own? Article published January 9 2020, available at https://iapp.org/news/a/eu-parliament-debates-could-california-be-considered-adequate-on-its-own/.

Baker McKenzie: GDPR National Legislation Survey. Report published January 2018, available at https://www.bakermckenzie.com/-/media/minisites/tmt/files/gdpr_national_legislation_survey.pdf?la=en.

Husam Barham: Achieving competitive advantage through big data – a literature review. Conference paper for the 2017 International Conference on Management of Engineering and Technology (PICMET) at Portland, Oregon, USA. Conference paper available at https://www.researchgate.net/publication/318351614_Achieving_Competitive_Advantage_Through_Big_Data_A_Literature_Review.

John Barnett: Will AI Revolution Lead to Mass Unemployment? What artificial intelligence might mean for your job and industry. Article published April 25 2017, available at https://www.business.com/articles/john-barnett-artificial-intelligence-job-market/#:~:text=Well%2C%20the%20real%20answer%20lies%20somewhere%20in%20between.,will%20result%20in%20huge%20losses%20and%20then%20layoffs.

Susanne Barth, Menno de Jong: The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior: a systematic literature review. Journal of Telematics and Informatics, vol. 34, issue 7, pp. 1038-1058.

Masooda N Bashir, Carol Hayes, April Lambert, Jay P Kesan: Online privacy and informed consent: The dilemma of information asymmetry, Proceedings of the Association for Information Science and Technology 2015, vol. 52, issue 1, pp. 1-10.

Helmut Bäumler, Albert von Mutius: Datenschutzgesetze der dritten Generation: Texte und Materialien zur Modernisierung des Datenschutzrechts, Luchterhand Verlang Munich 1999.

Lee Bell: Machine learning versus AI: what's the difference? Article published December 1 2016, available at https://www.wired.co.uk/article/machine-learning-ai-explained.

Alexander Bekker: Twenty Big Data Use Cases. Article published March 6 2018, available at https://www.experfy.com/blog/twenty-big-data-use-cases.

Steven Bellovin, Preetam Dutta, Nathan Reiting: Privacy and Synthetic Datasets, Stanford Technological Law Review 2019, vol. 22, issue 1.

David Bender: GDPR harmonization: Reality or myth? Article published June 7, 2018 on IAPP’s website, available at https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/.

Brahim Benichou, Jan De Bruyne, Thomas Gils, Ellen Wauters: Regulating AI in the European Union: Seven Key Takeaways. Article published February 25 2020, available at https://ai-laws.org/2020/02/regulating-ai-in-the-european-union-seven-key-takeaways/.

Bettina Berendt, Sören Preibusch: Toward accountable discrimination-aware data mining- the importance of keeping the human in the loop, Big Data. 2017, vol. 5, Nr. 2, pp. 135-152.

Rohith Bhaskar: 5G: Why is it the next big thing? Article published February 22 2021, available at https://www.moneycontrol.com/news/technology/5g-why-is-it-the-next-big-thing-6555881.html.

Priyankar Bhunia: Plans for cloud-first strategy and national AI framework revealed at 29th MSC Malaysia Implementation Council Meeting. Article published October 28 2017, available at https://opengovasia.com/plans-for-cloud-first-strategy-and-national-ai-framework-revealed-at-29th-msc-malaysia-implementation-council-meeting/.

Tas Bindi: Amazon, Google, Facebook, IBM, and Microsoft form AI non-profit. Article published September 29 2016, available at https://www.zdnet.com/article/amazon-google-facebook-ibm-and-microsoft-form-ai-non-profit/.

Reuben Binns, Valeria Gallo: Trade-offs. Article published published July 25 2019, available at https://ico.org.uk/about-the-ico/news-and-events/ai-blog-trade-offs/.

Julia Black, Andrew Murray: Regulating AI and Machine Learning: Setting theRegulatory Agenda, European Journal of Law and Technology, vol 10, issue 3, 2019.

James Blackman: Operational intelligence, three ways – descriptive, predictive and prescriptive. Article published December 11 2018, available at https://enterpriseiotinsights.com/20181211/channels/fundamentals/descriptive-predictive-prescriptive-analytics.

Keily Blair, James Hall, Christian Schröder, Heather Sussman, Shannon Yarovsky: The new EU approach to the regulation of Artificial Intelligence. Article published May 10 2021, available at https://www.jdsupra.com/legalnews/the-new-eu-approach-to-the-regulation-4438826/.

Ruth Boardman, Louise Hutt, Antonia Boyce: Article 49 derogations – summary table with examples. Article published May 12 2021, available at https://iapp.org/media/pdf/resource_center/article_49_derogations_summary_table_with_examples_iapp.pdf.

Igor Bobriakov: Top 10 Data Science Use Cases in Retail. Article published July 22 2018, available at https://medium.com/activewizards-machine-learning-company/top-10-data-science-use-cases-in-retail-6483accc6042.

Ariel Bogle: Australian Federal Police officers trialled controversial facial recognition tool Clearview AI. Article published April 15 2020, available at https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894.

Jens-Matthias Bohli, Christoph Sorge,Osman Ugus: A Privacy Model for Smart Metering, 2010 IEEE International Conference on Communications Workshops, Capetown, 2010, pp. 1-5.

Doug Bolton: The rise of artificial intelligence could put millions of human workers out of jobs - could a basic income be a solution? Article published February 19 2016, available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/basic-income-artificial-intelligence-ai-robots-automation-moshe-vardi-a6884086.html.

Frederik Zuiderveen Borgesius, Joost Poort: Online Price Discrimination and EU Data Privacy Law, Journal of Consumer Policy Vol. 40, issue 3, pp. 347–366.

Diana Borsa, Bilal Piot, Rémi Munos, Olivier Pietquin: Observational Learning by Reinforcement Learning. Article published June 20, 2017, available at https://arxiv.org/abs/1706.06617.

Anu Bradford: The Brussels Effect - How the European Union Rules the World, Oxford University Press 2020.

Laura Brandimarte, Alessandro Acquisti, George Loewenstein: Misplaced Confidences – Privacy and the Control Paradox. Article published August 9 2012, available at http://www.futureofprivacy.org/wpcontent/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf.

Russell Brandom: New Toronto Declaration calls on algorithms to respect human rights. Article published May 16 2018, available at https://www.theverge.com/2018/5/16/17361356/toronto-declaration-machine-learning-algorithmic-discrimination-rightscon.

Sebastian Bretthauer in: Louisa Specht/Reto Manz: Handbuch europäisches und deutsches Datenschutzrecht. C.H. Beck publishing Munich 2019.

Ryan Browne: Facebook whistleblower behind major leak is going to testify in Europe Article published October 12 2021, available at https://www.cnbc.com/2021/10/12/facebook-whistleblower-behind-major-leak-is-going-to-testify-in-europe.html.

Miles Brundage et al: The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Article published February 2018, available at https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217.

Gabriele Buchholtz, Rainer Stentzel in: Gierschmann, Schlender, Stentzel, Veil: Kommentar zur Datenschutzgrundverordnung, Bundesanzeiger Verlag publishing, Cologne 2017.

Benedikt Buchner, Jürgen Kühling in Kühling/Buchner: Kommentar zur DSGVO, C.H. Beck publishing Munich 2016.
Matthew Buckwell: EU Commission Proposes to Update the NIS/Cybersecurity Directive Only Two Years After Implementation. Article published January 2021, available at https://www.twobirds.com/en/news/articles/2021/global/eu-commission-proposes-to-update-the-nis-cybersecurity-directive-only-two-years-after-implementation.

Jens Bücking: Datenschutzgrundverordnung, NIS-Richtlinie der EU und das IT-Sicherheitsgesetz – ein neues, einheitliches Datensicherheits-/Datenschutzrecht für Europa. Working Paper published January 10 2018, available at https://www.sep.de/fileadmin/user_upload/Compliance/SEPsesam_Compliance_de_web.pdf.

Alexander Bugl: TMG and TKG to become TTDSG at December 1 2021. Article published August 25 2021, available at https://buglundkollegen.de/tmg-and-tkg-become-to-ttdsg-at-december-1-2021/#:~:text=TMG%20and%20TKG%20become%20to%20TTDSG%20at%20December,law%2C%20the%20Telecommunications%20Telemedia%20Data%20Protection%20Act%20%28TTDSG%29.

Tony Bunyan for Statewatch: The “point of no return” - Interoperability morphs into the creation of a Big Brother centralized EU state database including all existing and future Justice and Home Affairs databases. Paper published July 2018, available at https://www.statewatch.org/media/documents/analyses/no-332-eu-interop-morphs-into-central-database-revised.pdf.

Herbert Burkert: Governance of Global Networks in the Light of Differing Local Values, Nomos publishing, Baden-Baden 2000.

Maria Cristina Caldarola, Joachim Schrey: Big Data und Recht, C.H. Beck publishing Munich 2019.

Ryan Calo: The boundaries of privacy harm, Indiana Law Journal 2011, vol. 86, no. 3.

Libbie Canter, Rebecca Yergin: Newly Effective Florida Law Imposing Criminal Sanctions Adds to Developing Nationwide Patchwork of State Genetic Privacy Laws. Article published October 6 2021, available at https://www.insideprivacy.com/health-privacy/newly-effective-florida-law-imposing-criminal-sanctions-adds-to-developing-nationwide-patchwork-of-state-genetic-privacy-laws/.

Bruno Capone: Intrusion Detection based on Deep Learning. Article published October 16 2020, available at https://www.aitech.vision/en/2020/10/16/intrusion-detection-based-on-deep-learning/.

Angelique Carson: Colorado Privacy Act (CPA): What is it? Article published June 11 2021, available at https://www.osano.com/articles/colorado-privacy-act-what-is-it.

Fred Cate, Viktor Mayer-Schönberger: Notice and consent in a world of Big Data, International Data Privacy Law 2013, vol. 3, no. 2.

Ann Cavoukian, Jeff Jonas: Privacy by design in the age of big data. Article published June 8 2012, available at https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf.
Center for Information Policy Leadership: Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. Paper published December 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

Laurens Cerulus: Europe to crack down on surveillance software exports. Article published October 15 2020, available at https://www.politico.eu/article/europe-to-curtail-spyware-exports-to-authoritarian-countries/.

Anupam Chander: Is Data Localization a Solution for Schrems II? Article published September 2020, available at https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3318&context=facpub.
Nagesh Singh Chauhan: Introduction to artificial neural networks. Article published October 13, 2019, available at https://towardsdatascience.com/introduction-to-artificial-neural-networks-ann-1aea15775ef9.

Nancy Cheever, Larry Rosenblatt, Mark Carrier, Amber Chavez: Out of sight is not out of mind: The impact of restricting wireless mobile device use on anxiety levels among low, moderate and high users. Computers in Human Behavior 2014, vol. 37, pp. 290-297.

Saheli Choudhury: Malicious use of A.I. could turn self-driving cars and drones into weapons, top researchers warn. Article published February 21 2018, available at https://www.cnbc.com/2018/02/21/malicious-use-of-ai-by-hackers-could-pose-security-risks-threats.html.

Kamal Chouhbi: Hippocratic Oath for Data Scientists – the ethical checklist that every data scientist must follow. Article published October 6 2020, available at https://towardsdatascience.com/hippocratic-oath-for-data-scientists-407d2db15a78.

Theodore Christakis, Mathis Becuywe: Pre-market requirements, prior authorisation and Lex Specialis – novelties and logic in the facial recognition-related provisions of the draft AI Regulation. Article published May 4 2021, available at https://europeanlawblog.eu/2021/05/04/pre-market-requirements-prior-authorisation-and-lex-specialis-novelties-and-logic-in-the-facial-recognition-related-provisions-of-the-draft-ai-regulation/.

Chan-Mo Chung: Data localization: The causes, evolving international regimes and Korean practices, Journal of World Trade 2018, vol. 52, issue 2, pp. 187-208.

Peter Church: EU - Status of the proposed ePrivacy Regulation: Tighter cookie rules and more. Article published June 6 2017, available at https://www.linklaters.com/de-de/insights/publications/tmt-news/tmt-news---june-2017/eu---status-of-the-proposed-eprivacy-regulation-tighter-cookie-rules-and-more.

Danielle Keats Citron, Daniel Solove: Privacy harms, published February 2021 at George Washington Law School Public Law and Legal Theory Paper No. 2021-11.
Sam Clark: Draft SCC clash with Irish law reaches European Commission. Article published February 25 2021, available at https://globaldatareview.com/data-privacy/draft-scc-clash-irish-law-reaches-european-commission.

Diletta De Cicco, Charles-Albert Helleputte: The EU Artificial Intelligence Act. Article published May 2021, available at https://www.steptoeinternationalcomplianceblog.com/files/2021/05/AI_Infographic-1.pdf.

Ignacio Cofone: Google v. Spain: a right to be forgotten? Chicago-Kent Journal of International and Comparative Law 2015, vol. 15, no. 1, 2015, pp. 1-11.

Julie Cohen: How (not) to write a Privacy Law – disrupting surveillance-based business models requires government innovation. Article published March 23 2021, available at https://knightcolumbia.org/content/how-not-to-write-a-privacy-law.

Andrew Cormack: E-Privacy Regulation – one step closer. Article published February 12 2021, available at https://regulatorydevelopments.jiscinvolve.org/wp/2021/02/12/eprivacy-regulation-one-step-closer/.

Liam Critchey: Storing Information and Data with DNA. Article published August 11 2020, available at https://www.electropages.com/blog/2020/08/storing-information-and-data-dna.

Bennett Cyphers: Google's FLoC Is a Terrible Idea. Article published March 3 2021, available at https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea.

Ingo Dachwitz, Alexander Fanta: EU-Staaten wollen Verlagen einen Blankoscheck für Online-Tracking gewähren. The article provides background information on the draft ePrivacy regulation. Article published November 18 2019, available at https://netzpolitik.org/2019/eu-staaten-wollen-verlagen-einen-blankoscheck-fuer-online-tracking-gewaehren/.

Indranil Das: How To Implement Expert System in Artificial Intelligence? Article published September 18 2019, available at https://www.edureka.co/blog/expert-system-in-artificial-intelligence/#ExpertSystemInArtificialIntelligence.

Datameer: Top Five High-Impact Use Cases for Big Data Analytics. E-book published 2016, available at http://orcp.hustoj.com/wp-content/uploads/2016/01/eBook-Top-Five-High-Impact-UseCases-for-Big-Data-Analytics.pdf.

Ben Davis: 13 examples of dark patterns in ecommerce checkouts. Article published on April 6 2017, available at https://econsultancy.com/13-examples-of-dark-patterns-in-ecommerce-checkouts/.

Thomas Declerck: New EU Cybersecurity Strategy: European Commission Accelerates Push for EU to Lead in Cybersecurity Regulation. Article published December 24 2020, available at https://www.jdsupra.com/legalnews/new-eu-cybersecurity-strategy-european-47823/.

Deven Desai, Christos Makridis: We should have known SolarWinds would be a target. Article published January 6 2021, available at https://www.cfr.org/blog/we-should-have-known-solarwinds-would-be-target.

Ben Dickson: Why the difference between AI and machine learning matters. Article published October 8 2018, available at https://bdtechtalks.com/2018/10/08/artificial-intelligence-vs-machine-learning/.

Renee Dopplick: New Statement on Algorithmic Transparency and Accountability by ACM U.S. Public Policy Council. Article published January 14 2017, available at https://techpolicy.acm.org/2017/01/new-statement-on-algorithmic-transparency-and-accountability-by-acm-u-s-public-policy-council/.

Stephan Dreyer, Wolfgang Schulz: Was bringt die Datenschutzgrundverordnung für automatisierte Entscheidungssysteme? Bertelsmann Stiftung Publishing Gütersloh 2018.

Mike Dutch: A Data Protection Taxonomy, paper for the Storage Networking Industry Association. Article published June 2010, available at https://www.snia.org/sites/default/files/A_Data_Protection_Taxonomy_V51.pdf.

Marta Delgado Echevarría et al: European Union – Regulating Artificial Intelligence: European Commission Launches Proposals. Article published April 30 2021, available at https://www.jonesday.com/en/insights/2021/04/regulating-artificial-intelligence-european-commission-launches-proposals?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration.

Karsten Egetoft: Data-Driven Analytics: Practical Use Cases For Financial Services. Article published January 29 2019, available at https://www.digitalistmag.com/customer-experience/2019/01/29/data-driven-analytics-practical-use-cases-for-financial-services-06195123/.

Stefanie Eschholz, Jonathan Djabbarpour: Big Data und Scoring in der Finanzbranche. Dossier published January 2015, available at http://www.abida.de/sites/default/files/06%20Scoring.pdf.

Marcus Evans, Lara White, Sahar Bhaimia: UK Government sets out proposals to shake up UK data protection law. Article published September 28 2021, available at https://www.dataprotectionreport.com/2021/09/uk-government-sets-out-proposals-to-shake-up-uk-data-protection-laws/.

Marcus Evans, Peter McBurney, Michael Sinclair: The UK National AI Strategy: Regulation, Data Protection and IPR in the Mix. Article published September 27 2021, available at https://www.insidetechlaw.com/blog/the-uk-national-ai-strategy-regulation-data-protection-and-ipr-in-the-mix.

Daniel Fagella: Will There Be Another Artificial Intelligence Winter? Article published January 2 2019, available at https://emerj.com/ai-executive-guides/will-there-be-another-artificial-intelligence-winter-probably-not/.

Alexander Fanta: E-Privacy-Verordnung: EU-Staaten verwässern digitales Briefgeheimnis. Article published February 10 2021, available at https://netzpolitik.org/2021/eprivacy-verordnung-eu-staaten-verwaessern-digitales-briefgeheimnis/.

Alexander Fanta: France, Spain push for new EU data retention law. Article published March 5, 2021, available at https://netzpolitik.org/2021/urgently-needed-france-spain-push-for-new-eu-data-retention-law/.

Stephan Faris: The Hackers of Damascus. Article published November 14 2012, available at http://www.businessweek.com/articles/2012-11-15/the-hackers-of-damascus.

Joe Fay: Vatican signs up IBM and Microsoft as AI ethics apostles. Article published March 2 2020, available at https://devclass.com/2020/03/02/vatican-signs-up-ibm-and-microsoft-as-ai-ethics-apostles/.

Müge Fazlioglu; Transparency and the GDPR: Practical guidance and interpretive assistance from the Article 29 Working Party. Article published December 14 2017, available at https://iapp.org/news/a/transparency-and-the-gdpr-practical-guidance-and-interpretive-assistance-from-the-article-29-working-party/.

Lukas Feiler: Die 69 Öffnungsklauseln der DSGVO - Regelungsspielräume der nationalen Gesetzgeber. Presentation held on June 1 2017, available at http://www.lukasfeiler.com/presentations/Feiler_Die_69_Oeffnungsklauseln_der%20DS-GVO.pdf.

Lukas Feiler, Wouter Seinen: BCRs as a robust alternative to Privacy Shield and SCCs. Article published July 23 2020, available at https://iapp.org/news/a/binding-corporate-rules-as-a-robust-alternative-to-privacy-shield-and-sccs/.

Michael Fekete: ISO/IEC 27018 – new code of practice promotes privacy protection in the cloud, 2014. Article published October 20 2014, available at https://www.lexology.com/library/detail.aspx?g=ff6d5e13-1f3e-4539-887e-20dfc12eb8fd.

Greg Ferenstein: The birth and death of privacy: 3000 years of history told in 46 images. Article published November 25 2015, available at https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e#.8tcuzmf86.

Veleria Ferraris, Francesca Bosco, Elena D’Angelo: The impact on profiling on fundamental rights. Article published December 22 2013, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366753.

Jessica Fjeld et al: Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. Berkman Klein Center Research Publication No. 2020-1. Article published February 14 2020, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482.

Keith Foote; A Brief History of Big Data. Article published December 14 2017, available at https://www.dataversity.net/brief-history-big-data/#.

Nikolaus Forgo et al.: The principle of purpose limitation in Big Data in: Marcelo Corales, Mark Fernwick, Nikolaus Forgo (eds.): New Technology, Big Data and the Law, Springer Publishing 2017.

Vanessa Franssen: The European Commission’s E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement? Article published October 2018, available at http://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/.

Seth Frantzman: Israel and UAE defense companies partner on Artificial Intelligence. Article published April 21 2021, available at https://nationalinterest.org/blog/buzz/israel-and-uae-defense-companies-partner-artificial-intelligence-183274.

Erica Fraser: Data Localisation and the Balkanisation of the Internet, SCRIPTed – Journal of Law, Technology & Society 2016, vol. 13, issue 3.

Eike Michael Frenzel in Paal/Pauly: Kommentar zur Datenschutzgrundverordnung, Bundesdatenschutzgesetz, second edition 2018, C.H. Beck publishing Munich 2018.

Gloria Gonzalez Fuster, Serge Gutwirth, Eriak Ellyne: Profiling in the European Union – a high-risk practice, Inex Policy Brief No. 10, published June 2010, available at https://www.ceps.eu/system/files/book/2010/06/INEX%20PB10%20Fuster%20et%20al.%20on%20Profiling%20in%20the%20EU%20e-version.pdf.

FTC Report: Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues. Report published 2016, available at https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report.

Catherine Gallagher: 25 stunning advances in artificial intelligence. Article published June 23 2019, available at https://stacker.com/stories/3336/25-stunning-advances-artificial-intelligence.

John Garrett: EU data protection code to replace US/EU data rules. Article published September 16 2020, available at https://www.iteuropa.com/news/eu-data-protection-code-replace-useu-data-rules#:~:text=The%20EU%20Cloud%20Code%20of%20Conduct%20General%20Assembly,personal%20data%20to%20third%20countries%20around%20the%20world.

Francesca Gaudino: International Data Transfer Solutions under GDPR. Article published April 19 2020, available at https://globalcompliancenews.com/international-data-transfer-solutions-under-gdpr-23032020/.

Raphael Gellert: Understanding data protection as risk regulation, Journal of Internet Law 2015.

Bill Gertz: Social credit score: China set to roll out “Orwellian” mass surveillance tool. Article published December 9 2019, available at https://www.washingtontimes.com/news/2019/dec/9/social-credit-system-china-mass-surveillance-tool/.

David Gewirtz: Volume, velocity, and variety - understanding the three V's of big data. Article published March 21 2018, available at https://www.zdnet.com/article/volume-velocity-and-variety-understanding-the-three-vs-of-big-data/.

Sibylle Gierschmann: Was bringt deutschen Unternehmen die DSGVO – mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD 2016, pp. 51-54.

Global Legal Group: The International Comparative Legal Guide to data protection, 5th edition 2018, available at https://iapp.org/media/pdf/resource_center/Legal_Guide_To_Data_Protection_2018.pdf.

Global Partners Digital: National Artificial Intelligence Strategies and Human Rights: Paper published April 15 2020, available at https://www.gp-digital.org/publication/national-artificial-intelligence-strategies-and-human-rights-a-review/.

Peter Gola: Bundesdatenschutzgesetz C.H. Beck Publishing Munich 2012

Ian Goodfellow et al.: Generative Adversarial Networks, Proceedings of the International Conference on Neural Information Processing Systems (NIPS 2014), pp. 2672–2680, available at https://papers.nips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf.

Adam Gorlick: Researchers say voters swayed by candidates who share their looks, Stanford University report published October 22 2008, available at https://news.stanford.edu/news/2008/october22/morph-102208.html.

Jean-Etienne Goubet: AI Ethics – beware of AI ethics washing. Article published September 24 2019, available at https://www.genesys.com/blog/post/ai-ethics-beware-of-ai-ethics-washing.

Rachana Gupta: China making big strides in artificial intelligence. Article published September 6 2019, available at http://www.china.org.cn/opinion/2019-09/06/content_75178964.htm.

Serge Gutwirth, Ronald Leenes, Paul de Hert: Data Protection on the Move – Current Developments in ICT and Privacy / Data Protection, Springer Science + Media Publishing Dordrecht, 2016.

Paul de Hert, Serge Gutwirth: Regulating profiling in a democratic constitutional state, in: Profiling the European citizen, Springer Publishing 2008.

Paul de Hert, Vagelis Papakonstantinou: The new police and criminal justice data protection directive: A first analysis, New Journal of European Criminal Law 2016, vol. 7, issue 1, pp. 7-19.

Jim Halpert, Lael Bellamy: What Virginia's Consumer Data Protection Act means for your privacy program.. Article published March 8 2021, available at https://iapp.org/news/a/what-the-virginia-consumer-data-protection-act-means-for-your-privacy-program/#:~:text=Virginia%27s%20CDPA%20is%20a%20somewhat%20simplified%20version%20of,by%20overwhelming%20margin%20in%20fewer%20than%20two%20months.

Meghan Han: China Aims to Get the Jump on AI Standardization. Article published January 25 2018, available at https://syncedreview.com/2018/01/25/china-aims-to-get-the-jump-on-ai-standardization/#:~:text=China%20has%20just%20released%20its%20%E2%80%9CArtificial%20Intelligence%20Standardization,Standardization%20Management%20Committee%20Second%20Ministry%20of%20Industry%20%28%E5%9B%BD%E5%AE%B6%E6%A0%87%E5%87%86%E5%8C%96%E7%AE%A1%E7%90%86%E5%A7%94%E5%91%98%E4%BC%9A%E5%B7%A5%E4%B8%9A%E4%BA%8C%E9%83%A8%29.

Niko Härting: Internetrecht, Dr. Otto Schmidt Publishing Cologne 2014

Niko Härting: Datenschutzgrundverordnung, Dr. Otto Schmidt Publishing, Cologne 2016.

Niko Härting: Kopplungsverbot nach der DSGVO – erste Sichtung der Literatur, itrb-Rechtsberater 2019, Sonderheft zur DSGVO.

Niko Härting: DSGVO – gibt es Regelungen für anonyme Daten Article published May 3 2016, available at https://www.cr-online.de/blog/2016/05/03/dsgvo-gibt-es-regelungen-fuer-anonyme-daten/.

Niko Härting: Mit der DSGVO zum "Golden Handshake" – von der Sprengkraft des "Rechts auf Kopie". Article published March 29 2019, available at https://www.cr-online.de/blog/2019/03/29/mit-der-dsgvo-zum-golden-handshake-von-der-sprengkraft-des-rechts-auf-kopie/.

Niko Härting: Wann ist eine Datenverarbeitung eigentlich „erforderlich"? Article published February 1 2019, available at https://www.cr-online.de/blog/2019/02/01/wann-ist-eine-datenverarbeitung-eigentlich-erforderlich/.

Niko Härting: Post von der Datenschutzbehörde – Risiken des Wohlverhaltens: Was ist zu beachten, wenn eine Datenschutzbehörde Auskünfte verlangt? Article published November 8 2018, available at https://www.cr-online.de/blog/2018/11/08/post-von-der-datenschutzbehoerde-risiken-des-wohlverhaltens/.

Joerg Heidrich: Datenschutzbehörden erklären den Einsatz von Microsoft 365 für rechtswidrig. Article published October 23 2020, available at https://www.heise.de/news/Datenschutzbehoerden-erklaeren-den-Einsatz-von-Microsoft-365-fuer-rechtswidrig-4931745.html.

Melissa Heikkila for POLITICO: AI: Decoded: US states move to ban facial recognition - AI and structural racism. Article published May 12 2021, available at https://www.politico.eu/newsletter/ai-decoded/politico-ai-decoded-ai-gov-us-states-move-to-ban-facial-recognition-ai-and-structural-racism/.

Thomas Helbing: Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, KuR 2015.

John Henley, Robert Booth: Welfare surveillance system violates human rights, Dutch court rules. Article published February 5 2020, available at https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules.

Luke Henriques-Gomes: The automated system leaving welfare recipients cut off with nowhere to turn. Article published October 16 2019, available at https://www.theguardian.com/technology/2019/oct/16/automated-messages-welfare-australia-system?etcc_med=newsletter&etcc_cmp=nl_algoethik_13834&etcc_plc=aufmacher&etcc_grp=

Nicloas Herrmann: ePrivacy-Verordnung in der Krise – Die Suche nach einem Plan B. Article published November 25, 2019, available at https://www.datenschutzbeauftragter-info.de/eprivacy-verordnung-in-der-krise-die-suche-nach-einem-plan-b/.

Daniel Heymann: DSGVO und UWG – Wettbewerbsrecht und Datenschutz. Article published July 26 2019, available at https://www.petersenhardrahtpruggmayer.de/de/news/dsgvo-und-uwg-wettbewerbsrecht-und-datenschutz/

Debbie Heywood: The EC draft Data Governance Act – an altruistic approach to data. Article published January 29 2021, available at https://www.taylorwessing.com/en/insights-and-events/insights/2021/01/the-ec-draft-data-governance-act---an-altruistic-approach-to-data#:~:text=The%20DGA%20applies%20to%20a%20very%20broad%20range,the%20form%20of%20sound%2C%20visual%20or%20audiovisual%20recording%22

Seiko Hidaka: EU's possible Data Act: What can we anticipate from the Inception Impact Assessment and the Consultation? Article published July 5 2021, available at https://www.dataprotectionreport.com/2021/07/eus-possible-data-act-what-can-we-anticipate-from-the-inception-impact-assessment-and-the-consultation/.

Mireille Hildebrandt: Slaves to Big Data. Or Are we? Keynote during the 9th Annual Conference on Internet, Law & Politics on June 25, 2013 in Barcelona, available at http://works.bepress.com/mireille_hildebrandt/52.

Thomas Hoeren: Big Data und Recht, C.H. Beck publishing Munich 2014.

Thomas Hoeren, Reiner Münker: Die EU-Richtlinie für den Schutz von Geschäftsgeheimnissen und ihre Umsetzung unter besonderer Berücksichtigung der Produzentenhaftung, Wettbewerb in Recht und Praxis, vol. 2, 2018 pp. 150-155, available at https://www.itm.nrw/wp-content/uploads/Die-EU-Richtlinie.pdf

House of Lords Select Committee on Artificial Intelligence Report of Session 2017–19: HL Paper 100 - AI in the UK: ready, willing and able? Report published April 2018, available at https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf.

Jamie Humphreys, Edward Turtle: European Parliament publishes its proposals for new AI laws. Article published October 28 2020, available at https://products.cooley.com/2020/10/28/regulating-ai-eu-proposes-legal-framework-for-artificial-intelligence/

Scott Ikeda: Big Tech Companies May Face Blizzard of New Probes in EU as CJEU Ruling Clears Path for Data Protection Authorities. Article published June 28 2021, available at https://www.cpomagazine.com/data-protection/big-tech-companies-may-face-blizzard-of-new-probes-in-eu-as-cjeu-ruling-clears-path-for-data-protection-authorities/#:~:text=The%20new%20CJEU%20ruling%20gives%20the%20data%20protection,protection%20authorities%20will%20need%20to%20meet%20certain%20conditions.

Eleni Ilkoua, Maria Koutrakia provide background information on Symbolic AI in their 2020 paper: Symbolic vs. Sub-symbolic AI Methods: Friends or Enemies? Proceedings of the CIKM 2020 Workshops, October 19-20, Galway, Ireland, available at http://ceur-ws.org/Vol-2699/paper06.pdf.

International Network of Privacy Professionals: A brief history of data protection: How did it all start? Aarticle published June 1 2018, available at https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/.

International Working Group on Data Protection in Telecommunications: Working Paper on Big Data and Privacy principles under pressure in the age of Big Data analytics. Paper published May 2014, available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2014/06052014_en.pdf.

Krzysztof Izdebski: Comment on AI Regulation Proposal. EU Database on High-risk AI Systems. Article publishedApril 28 2021, available at https://epf.org.pl/en/2021/04/28/comment-on-ai-regulation-proposal-eu-database-on-high-risk-ai-systems/.

Trisha Jalan: European Commission proposes Data Act 2021 to increase data sharing between businesses and governments. Article published February 21 2020, available at https://www.medianama.com/2020/02/223-european-commission-data-sharing/.

Jan-Keno Janssen, Sylvester Tremmel: Die Psycho-Tricks der App-Entwickler. Article published October 15 2019, available at https://www.heise.de/ct/artikel/Die-Psycho-Tricks-der-App-Entwickler-4547123.html?seite=all.

Wiel Janssen: Seat-belt wearing and driving behavior – an instrumented-vehicle study. Accident Analysis and Prevention 1994, vol. 26, no. 2, pp. 261-268. A summary of the study is available at https://www.ncbi.nlm.nih.gov/pubmed/8198694?dopt=Abstract.

Manu Siddharth Jha: Want to Win an Election? Use AI And Machine Learning. Article published April 23 2020, available at https://www.mygreatlearning.com/blog/how-ai-and-machine-learning-can-win-elections/#:~:text=Artificial%20Intelligence%20for%20the%20Benefit%20of%20the%20Voter,help%20them%20make%20up%20their%20minds%20about%20candidates.

Jeff Jonas: Master Data Management vs. Sensemaking. Article published November 11 2011, available at http://jeffjonas.typepad.com/jeff_jonas/2011/11/master-data-management-mdm-vs-sensemaking.html.

Odia Kagan: Latin American and Spanish DPAs Issue Joint Statement on Data Processing and Artificial Intelligence. Article published October 24 2019, available at https://dataprivacy.foxrothschild.com/2019/10/articles/general-privacy-data-security-news-developments/latin-american-and-spanish-dpas-issue-joint-statement-on-data-processing-and-ai/.

Odia Kagan: FTC Filling Role of De Facto US Privacy Regulator. Article published March 7 2019, available at https://dataprivacy.foxrothschild.com/2019/03/articles/general-privacy-data-security-news-developments/ftc-filling-role-of-de-facto-u-s-privacy-regulator/.

Lawrence Kalman: The GDPR and NIS Directive – a new age of accountability, security and trust?, presentation held during the 2017 OWASP summit, available at https://www.owasp.org/images/b/b9/Olswang_slides_-_GDPR_and_NIS_Directive_-_accountability_security_and_trust_-_25_Jan_2017.pdf.

Gregg Keizer: WWII's Colossus computer cracks codes once again. Article published November 15 2007, available at https://www.computerworld.com/article/2540136/wwii-s-colossus-computer-cracks-codes-once-again.html.

Éanna Kelly: Israel sets out to become the next major artificial intelligence player. Article published July 2 2019, available at https://sciencebusiness.net/news/israel-sets-out-become-next-major-artificial-intelligence-player.

Ben Kepes: Google Users - You're The Product, Not The Customer. Article published December 4 2013, available at https://www.forbes.com/sites/benkepes/2013/12/04/google-users-youre-the-product-not-the-customer/#:~:text=The%20old%20adage%20goes%20that%20if%20you%27re%20not,up%20advertising%20to%20users%20of%20these%20free%20products.

Arjun Kharpal: China is building a giant $2.1 billion research park dedicated to developing A.I. Article published January 3 2018, available at https://www.cnbc.com/2018/01/03/china-is-building-a-giant-2-point-1-billion-ai-research-park.html.

Laura Kim, John Graubert: Dark Patterns: What They Are and What You Should Know About Them. Article published July 9, 2019, available at https://www.insideprivacy.com/consumer-protection/dark-patterns-what-they-are-and-what-you-should-know-about-them/.

Donald Klümper, Peter Rosen and Kevin Mossholder: Social Networking Websites, Personality Ratings and the Organizational Context – More than Meets the Eye?, Journal of Applied Social Psychology, vol. 42, issue 5, pp.1143-1172.

Daniel Knight: Personal Computer History from 1975 to 1984. Article published June 26 2014, available at https://lowendmac.com/2014/personal-computer-history-the-first-25-years/.

Will Knight: Clearview AI Has New Tools to Identify You in Photos. Article published April 10 2021, available at https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/.

Nicole Kobie: The complicated truth about China's social credit system. Article published June 7, 2019, available at https://www.wired.co.uk/article/china-social-credit-system-explained.

Jamens Kobielus: The Enterprise Data Warehouse – defined, refined, evolving with the times. Article published April 8 2008, available at https://go.forrester.com/blogs/08-04-08-the_enterprise_data_warehouse_edw_defined_refined_evolving_with_the_times/.

Helmut Köhler: Die Umsetzung der Richtlinie über unlautere Geschäftspraktiken in Deutschland – eine kritische Analyse, Gewerblicher Rechtsschutz und Urheberrecht 2012, pp. 1073-1079.

Juliane Kokott, Christoph Sobotta: The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, vol. 3, issue 4, pp. 222-228, available at https://academic.oup.com/idpl/article/3/4/222/727206.

Merel Koning: EU companies selling surveillance tools to China’s human rights abusers. Article published September 21 2020, available at https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers/.

Udo Kornmeier, Anne Baranowski: Eigentum an Daten – Zugang statt Zuordnung, Der Betriebsberater 2019, pp. 1219-1225.

Thomas Kranig, Andreas Sachs, Markus Gierschmann: Datenschutz-Compliance nach der DSGVO – Handlungshilfe für Verantwortliche inclusive Prüffragen für Aufsichtsbehörden, Bundesanzeiger Ltd. publishing Cologne, 2017.

George Krasadakisd: Artificial Intelligence: The Impact on Employment and the Workforce. How is AI replacing jobs? Which roles and industries will be most impacted? How can societies get prepared? Article published January 2018, available at https://medium.com/innovation-machine/artificial-intelligence-3c6d80072416.

Torsten Kraul, Max von Schönfeld, Marvin Bartels: Europäische Datenstrategie: EU-Kommission veröffentlicht Folgenabschätzung zum Data Act. Article published June 24 2021, available at https://www.noerr.com/de/newsroom/news/europaische-datenstrategie-eu-kommission-veroffentlicht-folgenabschatzung-zum-data-act?etcc_cmp=Noerr_news+072021&etcc_med=Newsletter.

Stefan Krempl: E-Privacy-Verordnung: EU-Rat für Vorratsdatenspeicherung und Cookie-Walls. Article published February 11, 2021, available at https://www.heise.de/news/E-Privacy-Verordnung-EU-Rat-fuer-Vorratsdatenspeicherung-und-Cookie-Walls-5051963.html.

Stefan Krempl: CCC-Tüftler hackt Merkels Iris und von der Leyens Fingerabdruck. Article published December 28, 2014, available at https://www.heise.de/security/meldung/31C3-CCC-Tueftler-hackt-Merkels-Iris-und-von-der-Leyens-Fingerabdruck-2506929.html.

Mihalis Kritikos: What if algorithms could abide by ethical principles? EPRS briefing paper, Paper published November 2018, available at https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/624267/EPRS_ATA(2018)624267_EN.pdf.

Mihalis Kritikos: Artificial Intelligence ante portas: legal and ethical reflections, EPRS briefing. Paper published March 2019, available at https://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-artificial-intelligence-ante-portas.pdf.

Quinten Kroes, Joost van Eymeren: EPR vis-à-vis GDPR: A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation. Report prepared by Brinkhof Advokaten for the Centre for Information Policy Leadership in July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-brinkhof_epr_study.pdf.

Jürgen Kühling: Die Europäisierung des Datenschutzrechts – Gefährdung deutscher Grundrechtsstandards? C.H. Beck Publishing Munich 2014.

Jürgen Kühling, Florian Sackmann: Irrweg Dateneigentum, Zeitschrift für Datenschutz 2020, pp. 24-30.

Christopher Kuner, Fred Cate, Christopher Millard and Dan Svantesson: The Challenge of Big Data for Data Protection, International Data Privacy Law 2012, vol. 2, no. 2, pp. 48-52.

Christopher Kuner: The European Union and the search for an international data protection framework, Groningen Journal of International Law, vol. 2 (2) 2014, pp. 55-71.

Matt Kusner, Joshua Loftus, Chris Russell, Ricardo Silva: Counterfactual Fairness, presented and published at the 31st Conference on Neural Information Processing Systems, available at https://papers.nips.cc/paper/6995-counterfactual-fairness.pdf.

Doug Laney: 3D Data Management – controlling Data Volume, Velocity, and Variety. Article published February 2001, available at http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Katarzyna Lasinska: Encryption Policy Issues in the EU. Article published May 25 2018, available at https://www.globalpolicywatch.com/2018/05/encryption-policy-issues-in-the-eu/.

Mike Latonero: Governing Artificial Intelligence: upholding human rights & dignity. Paper for Data & Society issued 2018, available at https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf.

Heidi Ledford: Millions of black people affected by racial bias in health-care algorithms. Article published October 24 2019 (updated October 26 2019), available at https://www.nature.com/articles/d41586-019-03228-6.

Phil Lee: Why Apple's "Consent for IDFA" announcement is a game changer for online and mobile privacy. Article published on June 24, 2020, available at https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/why-apples-consent-idfa-announcement-is-a-game-changer.

Lars Lensdorf, Robert Henrici, Moritz Hüsch, Nicholas Shepherd: A New Day for GDPR Damages Claims in Germany? Article published February 25 2021, available at https://www.insideprivacy.com/data-privacy/a-new-day-for-gdpr-damages-claims-in-germany/.

Brenda Leong of the Future of Privacy Forum called “The spectrum of Artificial Intelligence”. The infographic was published December 14 2020, and is available at https://fpf.org/blog/the-spectrum-of-artificial-intelligence-an-infographic-tool/.

Abner Li: Google names external advisory council to guide artificial intelligence usage. Article published March 26 2019, available at https://9to5google.com/guides/google-ai-principles/#:~:text=Google%20AI%20Google%20AI%20Principles.%20Back%20in%20June%2C,implemented%20to%20ensure%20that%20all%20guidelines%20are%20enforced.

Natasha Lomas: Sweden’s data watchdog slaps police for unlawful use of Clearview AI. Article published February 12 2021, available at https://techcrunch.com/2021/02/12/swedens-data-watchdog-slaps-police-for-unlawful-use-of-clearview-ai/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAALgmrj2j7lIqtPjUw9cgbbjI_LwuKoMDVdLqwxaBB4vNzCgFK7Pbz7Ez_PA0oQOMd7Csz70S7acDJmzPURaBLxCvcCrHG9kAiK1112tsVuo1yTd_vtJ3XMiwQYkT2_yofnTUP6pgIpte0masI6OagPfoQ91ZjZA16T2v7bBqJRwp

William Long, Francesca Blythe, Lauren Cuyvers, Monika Zdzieborska: EU Commission Issues Draft AI Regulation. Article published April 23 2021, available at https://datamatters.sidley.com/eu-commission-issues-draft-ai-regulation.

Stephanie Lopes: Key insights from the leaked EU Data Governance Act. Article published November 6 2020, available at https://digitalbusiness.law/2020/11/key-insights-from-the-leaked-eu-data-governance-act/.

Sebastian Louven, Malte Engeler: Copyright Directive – does the best effort principle comply with GDPR? Article published March 23 2019, available at https://www.telemedicus.info/article/3402-Copyright-Directive-Does-the-best-effort-principle-comply-with-GDPR.html%EF%BB%BF.

Nikita Lukianets: A (more) visual guide to the proposed EU Artificial Intelligence Act. Article published May 3 2021, available https://futurium.ec.europa.eu/en/european-ai-alliance/open-discussion/more-visual-guide-proposed-eu-artificial-intelligence-act.

Orla Lynskey: Criminal justice profiling and EU data protection law: precarious protection from predictive policing, International Journal of Law in Context, vol. 15, issue 2, pp. 162-176.

Kim Lyons: Google Pixel 6 leak teases Magic Eraser feature, plus five years of Android security updates. Article published October 9 2021, available at https://www.theverge.com/2021/10/9/22718007/google-pixel-6-leak-teases-magic-eraser-camera-five-years-android-security-updates.

Mark MacCarthy, Kenneth Propp: The EU’s White Paper on AI: A Thoughtful and Balanced Way Forward. Article published March 5 2020, available at https://www.lawfareblog.com/eus-white-paper-ai-thoughtful-and-balanced-way-forward

Tambiama Madiega: EU guidelines on ethics in artificial intelligence – EP briefing paper, available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf.

Mark Mao et al: Data Privacy – the Current Legal Landscape. Article published February 2016, available at https://iapp.org/media/pdf/resource_center/TS_CurrentLegalLandscape_February_2016.pdf.

Bernard Marr: How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. Article published May 21, 2018, available at https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#2152235f60ba.

Mario Martini: Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz in: Hill/Martini/Wagner: Die digitale Lebenswelt gestalten, Baden-Baden 2015, pp. 99-169.

Emma Martinho-Truswell, Constanza Gomez Mont: Mexico leads Latin America as one of the first ten countries in the world to launch an artificial intelligence strategy. Article published May 24 2018, available at https://www.oxfordinsights.com/insights/2018/5/24/mexico-leads-latin-america-as-one-of-the-first-ten-countries-in-the-world-to-launch-an-artificial-intelligence-strategy.

Mario Martini: Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz in: Hill/Martini/Wagner: Die digitale Lebenswelt gestalten, Baden-Baden 2015, pp. 99-169.
Molly Martinson: Work in progress – substantial revisions recommended to the European Commission’s draft new Standard Contractual Clauses. Article published January 28 2021, available at https://practicalprivacy.wyrick.com/blog/work-in-progress-substantial-revisions-recommended-to-the-european-commissions-draft-new-standard-contractual-clauses.

Kristen Mathews, Courtney Bowman: The California Consumer Privacy Act of 2018. Article published July 13, 2018, available at https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.

Viktor Mayer-Schönberger: Generational Development of Data Protection in Europe, in: Philip E. Agre, Marc Rotenberg (eds.): Technology and Privacy: The New Landscape, Massachusetts Institute of Technology Press 1998, Cambridge and London, pp. 219-241.

Viktor Mayer-Schönberger, Ernst Brandl, Hans Kristoferitsch: Datenschutzgesetz, Linde Verlag Wien 3. Edition 2014, p. 6.

Karen McCullagh: Protecting privacy through control of personal data processing – a flawed approach, International Review of Law, Computers and Technology 2009, vol. 23, no. 1, pp. 23-29.

Cassandra McNeill: Veracity – the most important “V” of Big Data. Article published August 29 2019, available at https://www.gutcheckit.com/blog/veracity-big-data-v/.

Maya Medeiros: A legal framework for artificial intelligence. Article published November 20 2019, available at https://www.socialmedialawbulletin.com/2019/11/a-legal-framework-for-artificial-intelligence/.

Isak Mendoza, Lee A. Bygrave: The right not to be subject to automated decisions based on profiling, University of Oslo, Legal Studies, Research Paper Series No. 2017-20, available at https://ssrn.com/abstract=2964855.

Rachel Metz: Researchers can now use AI and a photo to make fake videos of anyone. Article published May 24 2019, available at https://edition.cnn.com/2019/05/24/tech/deepfake-ai-one-photo/index.html.

Christopher Millard: Forced Localization of Cloud Services: Is Privacy the Real Driver? Paper provided for the 2015 forthcoming in IEEE Cloud Computing. Article published May 14, 2015, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605926.

Oliver Miller: A conversation with ELIZA, the electronic therapist. Article published August 1 2012, available at https://thoughtcatalog.com/oliver-miller/2012/08/a-conversation-with-eliza/.

Jay Modrall: EU proposes new Artificial Intelligence Regulation. Article published April 16 2021, available at https://www.nortonrosefulbright.com/en/knowledge/publications/fdfc4c27/eu-to-propose-new-artificial-intelligence-regulation.

Lokke Moerel: Big Data protection – how to make the draft EU future proof. Tilburg University press, Tilburg 2014, available at https://pure.uvt.nl/ws/portalfiles/portal/2837675/oratie_Lokke_Moerel.pdf.

Lokke Moerel, Corien Prins: On the death of purpose limitation. Article published June 2 2015, available at https://iapp.org/news/a/on-the-death-of-purpose-limitation/.

Aleksandra Mojsilovic: Introducing AI Explainability 360. Article published August 8 2019, available at https://www.ibm.com/blogs/research/2019/08/ai-explainability-360/#:~:text=AI%20Explainability%20360%20complements%20the%20ground-breaking%20algorithms%20developed,were%20built%20or%20in%20which%20environment%20they%20run.
Alex Moltzau: The French National Strategy on Artificial Intelligence. Article published January 15 2020, available at https://towardsdatascience.com/the-french-national-strategy-on-artificial-intelligence-c8c8fcfdace1

Renato Leite Monteiro: GDPR matchup – Brazil's General Data Protection Law. Article published October 4 2018, available at https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/.

Renato Leite Monteiro: The new Brazilian General Data Protection Law - a detailed analysis. Article published August 15 2018, available at https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/.

Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh, Alex Pentland: Unique in the shopping mall: On the reidentifiability of credit card metadata, Science 2015, vol. 347, issue 6221, pp. 536-539.

Ulf Morgenstern: 5. MaRisk-Novelle in Kraft getreten – deutliche Herausforderungen für Kreditinstitute. Article published December 20 2017, available at https://bankinghub.de/banking/steuerung/5-marisk-novelle-kraft-getreten.

Benjamin Muller: The Artificial Intelligence Act – a quick explainer. Article published on May 4 2021, available at https://datainnovation.org/2021/05/the-artificial-intelligence-act-a-quick-explainer/.

Catelijne Muller: The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law, report for the Council of Europe Ad Hoc Committee on Artificial Intelligence. Report published June 24 2020, available at https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da.

Michele Nati, Cert Ahlin: Data Portability 2.0 is yet to come. Article published September 17, 2018, available at https://medium.com/mydata/data-portability-2-0-is-yet-to-come-1c438c2a96c1.

Laurens Nauds: The Right not to be Subject to Automated Decision-Making: The role of explicit consent. Article published in 2016 available at https://www.law.kuleuven.be/citip/blog/the-right-not-to-be-subject-to-automated-decision-making-the-role-of-explicit-consent/.

Nils Nilsson, The Quest for Artificial Intelligence: A History of Ideas and Achievements, Cambridge University Press 2010, Cambridge (UK).

Debby Nirwan: Using Forward-search algorithms to solve AI Planning Problems. Article published September 19 2020, available at https://ai.plainenglish.io/using-forward-search-algorithms-to-solve-ai-planning-problems-361ad4910239.

Jacob Nix, Pascal Bizarro: US Data Privacy Law: A Disparate Landscape in Need of Consolidation. Article published September 9 2020, available at https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/us-data-privacy-law-a-disparate-landscape-in-need-of-consolidation.

Jacob Nix, Pascal Bizarro: US Data Privacy Law: A Disparate Landscape in Need of Consolidation. Article published September 9 2020, available at https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/us-data-privacy-law-a-disparate-landscape-in-need-of-consolidation.

Cynthia O'Donoghue, Asel Ibraimova: ICO announces it is working on bespoke UK set of Standard Contractual Clauses. Article published 5 May 2021, available at https://www.technologylawdispatch.com/2021/05/privacy-data-protection/ico-announces-it-is-working-on-bespoke-uk-set-of-standard-contractual-clauses/.

Cynthia O'Donoghue, Andreas Splittgerber, Asel Ibraimova: European Commission issues New Standard Clauses for data transfers outside the EEA: Act within 18 months. Article published June 4 2021, available at https://www.technologylawdispatch.com/2021/06/global-data-transfers/european-commission-issues-new-standard-clauses-for-data-transfers-outside-the-eea-act-within-18-months/.

Mie Oehlenschlager: First European Ethical Charter on AI in Judicial Systems. Article published on January 16, 2019, available at https://dataethics.eu/first-european-ethical-charter-on-ai-in-judicial-systems/.

Maureen Ohlhausen for the Federal Trade Commission: Painting the Privacy Landscape: Informational Injury in FTC privacy and data security cases. Article published September 19 2017 and is available at https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.

Begüm Yavuzdoğan Okumuş, Direnç Bada: Turkish Data Localization Rules In Effect For Social Media Companies. Article published October 14 2020, available at https://gun.av.tr/insights/articles/turkish-data-localization-rules-in-effect-for-social-media-companies?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration

Arlindo Oliveira: Biotechnology, Big Data and Artificial Intelligence. Biotechnology Journal 2019, vol. 14, issue 8. The article is also available at https://doi.org/10.1002/biot.201800613.

Samed Olukoya: Think20 Says Artificial Intelligence (AI) Based Learning Technologies Can Overcome Current Educational Challenges. Article published August 25 2020, available at https://investorsking.com/2020/08/25/think20-says-artificial-intelligence-ai-based-learning-technologies-can-overcome-current-educational-hallenges/.

Maya Oppenheim for the Independent: Amazon scraps 'sexist AI' recruitment tool. Article published October 11 201X, available at https://www.independent.co.uk/life-style/gadgets-and-tech/amazon-ai-sexist-recruitment-tool-algorithm-a8579161.html.

Meir Orbach: Israel launches national AI program, but lack of budget threatens its implementation. Article published December 22 2020, available at https://www.calcalistech.com/ctech/articles/0,7340,L-3883355,00.html.

Jim O'Reilly: Data Protection in the Public Cloud. Article published March 15 2018, available at https://www.networkcomputing.com/data-centers/data-protection-public-cloud-6-steps.

Cailean Osborne: The European Commission's Artificial Intelligence Act highlights the need for an effective AI assurance ecosystem. Article for the Centre for Data Ethics and Innovation. Article published May 11 2021, available at https://cdei.blog.gov.uk/2021/05/11/the-european-commissions-artificial-intelligence-act-highlights-the-need-for-an-effective-ai-assurance-ecosystem/.

Jayshree Pandya: The dual-use dilemma of Artificial Intelligence. Article published January 7 2019, available at https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/.

Arockia Panimalar, Varnekha Shree, Veneshia Kathrine who describe the evolution of the vectors in their 2017 article: The 17 V's of Big Data, International Research Journal of Engineering and Technology 2017, Vol. 4, Issue 9, pp. 329-333, available at https://www.irjet.net/archives/V4/i9/IRJET-V4I957.pdf.

Vagelis Papakonstantinou, Paul de Hert: Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI. Article published April 1 2021, available at https://lsts.research.vub.be/en/20210401.
Salvatore Parise, Bela Iyer, Dan Vesset: Four strategies to capture and create value from big data. Article published in Ivey Business Journal, July/August issue 2012, available at http://www.iveybusinessjournal.com/topics/strategy/four-strategies-to-capture-and-create-value-from-big-data#.Uwm-L4XHjWh.

Oliver Patel, Nathan Lea: EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows, published in May 2020 by the UCL European Institute. Article published May 2020, available at https://www.ucl.ac.uk/european-institute/sites/european-institute/files/privacy_shield_brexit_and_the_future_of_transatlantic_data_flows_1.pdf.

Andy Peart: Homage to John McCarthy, the Father of Artificial Intelligence. Article published October 29 2020, available at https://www.artificial-solutions.com/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence.

Lisa Peets, Marty Hansen, Sam Jungyun Choi, Nicholas Shepherd, Anna Oberschelp de Meneses: European Commission Presents Strategies for Data and AI. Article published February 20, 2020, available at https://www.covingtondigitalhealth.com/2020/02/european-commissions-white-paper-on-artificial-intelligence-part-2-of-4/.

Ceyhun Pehlivan, Peter Church:EU: The ePrivacy Regulation - Let the trilogue begin! Article published February 12 2021, available at https://www.linklaters.com/en/insights/blogs/digilinks/2021/february/eu---the-eprivacy-regulation---let-the-trilogue-begin.

Dieter Petereit: Google wird seine Tracking-Alternative FLoC zunächst nicht in Europa einführen. Der Suchmaschinenriese will erst die rechtliche Basis klären. DSGVO-Verstöße können schließlich sehr teuer werden. Article published March 24 2021, available at https://t3n.de/news/huch-dsgvo-googles-floc-scheitert-1369031/.

Carlo Piltz: How German Data Protection Authorities interpret the GDPR. Article published July 5 2017, available at https://www.delegedata.de/2017/07/how-german-data-protection-authorities-interpret-the-gdpr/.

Carlo Piltz: Bundeskartellamt erlasst Untersagungsverfügung gegen Facebook – Warum das Vorgehen der Behörde datenschutzrechtlich kritisch betrachtet werden muss. Article published February 7 2019, available at https://www.delegedata.de/2019/02/bundeskartellamt-erlasst-untersagungsverfuegung-gegen-facebook-warum-das-vorgehen-der-behoerde-datenschutzrechtlich-kritisch-betrachtet-werden-muss/.

Carlo Piltz: Oberster Gerichtshof in Österreich zur Kopplung der Einwilligung nach der DSGVO – grundsätzlich unzulässig? Article published November 13 2018, available at https://www.delegedata.de/2018/11/oberster-gerichtshof-in-oesterreich-zur-kopplung-der-einwilligung-nach-der-dsgvo-grundsaetzlich-unzulaessig/.

Kai-Uwe Plath: Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen des TMG und TKG, Otto Schmidt Publishing Cologne 2016

Vincent Mannacourt: Have a GDPR complaint? Skip the regulator and take it to court. Article published August 30 2020, available at https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/.

Meaghan Powell, Lesley Sutton: AI regulation: the push for Australian standards. Article published July 29 2019, available at https://www.gtlaw.com.au/insights/ai-regulation-push-australian-standards.

Duane Pozza and Jacquelynn Ruff: The next phase of AI regulation in the US and abroad. Article published July 19, 2019, available at https://www.wileyconnect.com/home/2019/7/19/the-next-phase-of-ai-regulation-in-the-us-and-abroad.

Dag Prawitz: Tacit Knowlege - an Impediment for AI? in: Göranzon et al.: Artifical Intelligence, Culture and Language: On Education and Work. The Springer Series on Artificial Intelligence and Society. Springer Verlag Berlin Heidelberg 1990, available at https://doi.org/10.1007/978-1-4471-1729-2_7.

Gil Press: A Very Short History of Artificial Intelligence. Article published December 30 2016, available https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/.

Price Waterhouse Coopers: Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Report published in August 2019, available at https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile.

Olivier Proust: What future for the transfers of personal data? Article published January 18 2022, available at https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/what-future-for-the-transfers-of-personal-data.

Kanan Purkayastha: Challenges from malicious use of AI. Article published May 18 2020, available at https://www.observerbd.com/news.php?id=257035.

Nadezhda Purtova: Between the GDPR and the Police Directive: navigating through the maze of information sharing in public–private partnerships, International Data Privacy Law, vol. 8, issue 1, 2018, pp. 52–68, available at https://doi.org/10.1093/idpl/ipx021.

Nadezhda Purtova: The law of everything. Broad concept of personal data and future of EU data protection law. Article published in Law, Innovation and Technology 2018, vol. 10, issue 1, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355.

Michael Radwin: Knowledge Engineering demystified, expert paper for the Future of Privacy Forum issued February 8 2021.

Katori Rameau, K.C. Halm: White House Issues Guidance for AI Regulation and "Non-Regulation". Article published January 22 2020, available at https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2020/01/white-house-ai-guidelines.

Friederike Reinhold, Angela Müller: AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence – A major step with major gaps. Article published April 22 2021. AlgorithmWatch's response is available at https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/.

Neil Richards, Jonathan King: Three Paradoxes of Big Data, Stanford Law Review Online 2013, Vol. 66:41. Article published September 3 2013, available at http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big-data.

Sarah Rippy: Virginia passes the Consumer Data Protection Act. Article published March 3 2021, available at https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.

Steven Roosa, Daniel Rosenzweig: iOS 15: New Privacy Features Industry Should Note. Article published October 7 2021, available at https://www.ntanalyzer.com/blog/ios-15-new-privacy-features-industry-should-note/

Ira Rubinstein: Big Data: The End of Privacy or a New Beginning? International Data Privacy Law 2013, vol. 3, no. 2, pp. 77-81.

Madeline Salinas: California Privacy Protection Agency Holds First Meeting. Article published June 24 2021 for Covington & Burling LLP, available at https://www.insideprivacy.com/ccpa/california-privacy-protection-agency-holds-first-meeting-preparing-for-upcoming-rulemaking/.

Pollyanna Sanderson: Automated Decision Systems Legislation Update, presentation held on June 14 2021 during a Future of Privacy Forum meeting.

Marianno Delli Santi: ePrivacy Regulation – an open letter from 30 civil society organizations: our letter to the European Parliament asking them to stand up against online tracking. Article published April 14 2021, available at https://www.openrightsgroup.org/publications/eprivacy-regulation-an-open-letter-from-30-civil-society-organisations/.

Martin Schallbruch: E-Evidence – Outsourcing von Grundrechtsschutz. Article published in the CR-blog in May 2018, available at https://www.cr-online.de/blog/2018/05/10/e-evidence-outsourcing-von-grundrechtsschutz-teil-3/.

Allison Schiff: Google Will not run FLoC origin tests in Europe due to GDPR concerns. Article published March 23 2021, available at https://www.adexchanger.com/platforms/google-will-not-run-floc-origin-tests-in-europe-due-to-gdpr-concerns/.

Jens Peter Schmidt: European Commission proposes world’s first ever regulatory framework on Artificial Intelligence. Article published March 23 2021, available at https://www.noerr.com/en/newsroom/news/european-commission-proposes-worlds-first-ever-regulatory-framework-on-artificial-intelligence-ai.

Ursula Schmidt-Erfurth, Amir Sadeghipour, Bianca Gerendas , Sebastian Waldstein, Hrvoje Bogunović: Artificial intelligence in retina. Article published August 1 2018, available at https://pubmed.ncbi.nlm.nih.gov/30076935/.

Christoph Schmon: Our EU Policy Principles: Platform Liability. Article published July 9 2020, available at https://www.eff.org/deeplinks/2020/07/effs-eu-policy-principles-platform-liability-and-monitoring.

Christoph Schmon, Karen Gullo: Euopean’s Commission proposed Digital Services Act, got several things right, but improvements are necessary to put users in control. Article published December 15 2020, available https://www.eff.org/deeplinks/2020/12/european-commissions-proposed-regulations-require-platforms-let-users-appeal.

Andreas Schneider: Datenschutzgrundverordnung, presentation held in his role as representative of the Saxon Data Protection Commissioner at the KISA Forum on February 18 2018, available at https://www.kisa.it/de/datei/anzeigen/id/19667,3/datenschutzgrundverordnung.pdf.

Hans Peter Schüler: Cloud Privacy Service zur DSGVO-konformen Nutzung von Microsoft 365. Article published September 6 2021, available at https://www.heise.de/hintergrund/Cloud-Privacy-Service-zur-DSGVO-konformen-Nutzung-von-Microsoft-365-6171165.html.

Peter Gola: Kommentar zur DSGVO, C.H. Beck publishing Munich 2018.

Christiane Schulzki-Haddouti: Scharfe E-Privacy-Verordnung verabschiedet: Mehr Datenschutz, klares Nein zu Hintertüre. Article published October 26 2017, available at https://www.heise.de/newsticker/meldung/Analyse-EU-Kommission-verschlimmbessert-Entwurf-zur-E-Privacy-Verordnung-3594716.html.

Christiane Schulzki-Haddouti: Datenschutz-Verstöße werden sehr selten sanktioniert. Article published April 4 2016, available at https://www.datenschutzbeauftragter-online.de/datenschutz-verstoesse-werden-sehr-selten-sanktioniert/9536/.

John Selby: Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? International Journal of Law and Information Technology, vol. 25, issue 3, pp. 213–232, available at https://doi.org/10.1093/ijlit/eax010.

Tom Shafer: The 42 V's of Big Data and Data Science. Article published April 1 2017, available at https://www.elderresearch.com/blog/42-v-of-big-data.

Lori Sherer: Data Scientists, Take a Hippocratic Oath: While the ethics of analytical tools can be tricky to parse, five basic principles can help data scientists address the challenge. Article published June 13 2018, available at https://www.bain.com/insights/data-scientists-take-a-hippocratic-oath-forbes/#.

Connor Shorten: Machine Learning vs. Deep Learning. Article published on September 7, 2018, available at https://towardsdatascience.com/machine-learning-vs-deep-learning-62137a1c9842.

Spiros Simitis: Bundesdatenschutzgesetz, Nomos Publishing Baden Baden 2014.

Meagan Simpson: Canada, France Governments Announce Declaration of the International Panel on AI. Article published May 16 2019, available at http://canada.ai/posts/canada-france-governments-announce-declaration-of-the-international-panel-on-ai.

Tom Simonite: Should Data Scientists Adhere to a Hippocratic Oath? Article published on August 2 2018, available at https://www.wired.com/story/should-data-scientists-adhere-to-a-hippocratic-oath/.

Ranjeet Singh: The Rise and Fall of Symbolic AI. Article published September 14 2019, available at https://towardsdatascience.com/rise-and-fall-of-symbolic-ai-6b7abd2420f2.

Bill Siwicki: Is synthetic data the key to healthcare clinical and business intelligence? Article published February 21 2020, available at https://www.healthcareitnews.com/news/synthetic-data-key-healthcare-clinical-and-business-intelligence.

Stu Sjouwerman: Seven Reasons For Cybercrime's Meteoric Growth. Article published December 23 2019, available at https://www.forbes.com/sites/forbestechcouncil/2019/12/23/seven-reasons-for-cybercrimes-meteoric-growth/#:~:text=Cybercrime%20has%20been%20on%20the%20rise%20for%20years.,more%20criminals%20are%20leveraging%20the%20internet%20to%20steal.

Daniel Solove: Understanding Privacy, Harvard University Press 2008.

Daniel Solove: The digital person: Technology and Privacy in the Information Age, NYU Press 2004.

Daniel Solove: Conceptualizing Privacy, California Law Review Vol. 90, No. 4, pp. 1132-1140, available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview.

Daniel Solove: Introduction: Privacy self-management and the consent dilemma, Harward Law Review 2013, vol. 126:1880, pp. 1886-1903.

Dennis Späth: Artificial Intelligence is transforming the workforce as we know it. Article published March 18, 2019, available at https://workplaceinsight.net/artificial-intelligence-is-transforming-the-workforce-as-we-know-it/.
Andy Splittgerber: German Cookie Law enters into force on December 1, 2021. Article published May 21 2021, available at https://viewpoints.reedsmith.com/post/102gyp8/german-cookie-law-enters-into-force-on-dec-1-2021.

David Stauss: Status of Proposed CCPA-Like State Privacy Legislation as of May 3, 2021. Article published May 2 2021, available at https://www.bytebacklaw.com/2021/05/status-of-proposed-ccpa-like-state-privacy-legislation-as-of-may-3-2021/.

Shiva Stella: Senate Releases Principles for Comprehensive Privacy Legislation. Article published on November 18 2019, available at https://www.publicknowledge.org/press-release/senate-releases-principles-for-comprehensive-privacy-legislation/.

Rainer Stentzel: Das Grundrecht auf ...? Auf der Suche nach dem Schutzgut des Datenschutzes in der Europäischen Union, PingG (Privacy in Germany), issue 5, pp. 185-191, available at https://www.pingdigital.de/ce/das-grundrecht-auf/detail.html.

Richard Steppe: Online price discrimination and personal data: A General Data Protection Regulation perspective, Computer Law & Security Review 2017, vol. 33, issue 6, pp. 768-785, available at https://www.sciencedirect.com/science/article/abs/pii/S0267364917301656.

Sean Stephenson, Paul Lalonde: The Limits of Data Localization Laws. Article published August 9 2019, available at http://www.dentonsdata.com/the-limits-of-data-localization-laws-trade-investment-and-data/.

Richard Stirling, Hannah Miller, Emma Martinho-Truswell: Oxford Institute Government AI Readiness Index, Article published in 2017, available at https://www.oxfordinsights.com/government-ai-readiness-index?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_recent_activity_details_all%3BeJ%2FPpiq8RzyLuLPtyf%2FYoA%3D%3D.

Samuel Stolton: After Clearview AI scandal, Commission ‘in close contact’ with EU data authorities. Article published February 12 2020, available at https://www.euractiv.com/section/digital/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/.

Nancy Tai: Dimensions of Big Data. Article published July 27 2018, available at http://www.klarity-analytics.com/2015/07/27/dimensions-of-big-data/

Steven Tanimoto: The elements of Artificial Intelligence, Computer Science Press 2010.

Omer Tene: Privacy: For the Rich or for the Poor? Concurring Opinions. Article published July 26 2012, available at http://www.concurringopinions.com/archives/2012/07/privacy-for-the-rich-or-for-the-poor.html.

Omer Tene, Jules Polonetsky: Privacy in the age of big data – a time for big decisions, Stanford Law Review 2012, vol. 64:63.

Omer Tene, Jules Polonetsky: Big data for all – privacy and user control in the age of analytics, Northwestern Journal of Technology and Intellectual Property, vol. 11, issue 5, pp. 239, available at https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip.

Omer Tene: Privacy: For the Rich or for the Poor? Concurring Opinions. Article published July 26 2012, available at http://www.concurringopinions.com/archives/2012/07/privacy-for-the-rich-or-for-the-poor.html.

Lydia de la Torre: GDPR matchup – The California Consumer Privacy Act. Article published July 31 2018, available at https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/.
Valerie Thomas on behalf of the Regulatory Institute: Report on Artificial Intelligence part I: the existing regulatory landscape. Report published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/.

Jetty Tielemans: A look at what's in the EU's newly proposed regulation on AI. Article published April 21 2021, available at https://iapp.org/news/a/a-look-at-whats-in-the-eus-newly-proposed-regulation-on-ai/.

Jetty Tielemanns, Müzge Fazlioglu: ePrivacy Regulation - Q&A on select topics. Article published May 25 2021, available at https://iapp.org/news/a/eprivacy-regulation-qa-on-select-topics/.

Victor Timon, Helen Hart: EU plans changes to e-commerce and competition law. Article published June 10 2020, available at https://www.lewissilkin.com/en/insights/eu-plans-changes-to-e-commerce-and-competition-law.

The Alan Turing Institute: AI, ethics and the law: what challenges and what opportunities. Article published January 18 2018, available at https://aticdn.s3-eu-west-1.amazonaws.com/2018/03/140318-Ai-ethics-and-the-law-public-panel-report.pdf.

Marc van Lieshout: The Value of Personal Data. In: Jan Camenisch, Simone Fischer-Hubner, Marit Hansen (eds). Privacy and Identity Management for the Future Internet in the Age of Globalisation, Springer Publishing 2015.

Tanguy Van Overstraeten, Julie De Meyer: Belgium: Council of State approves US data transfer. Article published September 16 2021, available at https://www.linklaters.com/th-th/insights/blogs/digilinks/2021/september/belgium-council-of-state-approves-us-data-transfer.

Kristof Van Quathem: New Draft ePrivacy Regulation Released. Article published on October 14, 2019, available at https://www.insideprivacy.com/international/european-union/new-draft-eprivacy-regulation-released/.

Winfried Veil: 21 Thesen zum Irrweg der DSGVO. Article published May 23 2018, available at https://www.cr-online.de/blog/2018/05/23/21-thesen-zum-irrweg-der-ds-gvo/#anker4.

Winfried Veil: Accountability – Wie weit reicht die Rechenschaftspflicht der DSGVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, Zeitschrift für Datenschutz vol. 1 2018, pp. 9-16.

Winfried Veil: Die Schutzgutmisere des Datenschutzrechts (Teil I). Article published February 6 2019, available at https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/.

Winfried Veil: Die Schutzgutmisere des Datenschutzrechts (Teil II). Article published February 6 2019 in Computer und Recht (CR-online.de Blog), available at https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/

Winfried Veil: Zum Schutzgut der DSGVO – eine naive Wortlautanalyse. Article published April 22 2021, available at https://www.cr-online.de/blog/2021/04/22/zum-schutzgut-der-ds-gvo-eine-naive-wortlautanalyse/.

Winfried Veil: Accountability – Wie weit reicht die Rechenschaftspflicht der DSGVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, Zeitschrift für Datenschutz 2018, vol. 1, pp. 9-16.

Cedric Villani: For a meaningful Artificial Intelligence – towards a French and European strategy. Article published March 2018, available at https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf.

John Villasenor: Products liability law as a way to address AI harms. Article published October 31, 2019, available at https://www.brookings.edu/research/products-liability-law-as-a-way-to-address-ai-harms/.

Benjamin Vitaris: Data Residency: Meaning, Laws, & Requirements. Article published July 30 2020, available at https://permission.io/blog/data-residency/.

Sandra Wachter, Brent Mittelstadt, Luciano Floridi: Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR, International Data Privacy Law 2017, vol. 7, issue 2, pp. 76–99.

Heidi Waem, Simon Verschaeve: What's left of the GDPR's one-stop-shop? CJEU clarifies the competences of non-lead data protection authorities. Article published July 5 2021, available at https://blogs.dlapiper.com/privacymatters/eu-whats-left-of-the-gdprs-one-stop-shop-cjeu-clarifies-the-competences-of-non-lead-data-protection-authorities/?utm_source=mailpoet&utm_medium=email&utm_campaign=privacy-matters-newsletter.

Ben Wagner: Ethics as an escape from regulation. From ethics-washing to ethics-shopping? In: Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds): BEING PROFILED : COGITAS ERGO SUM. 10 Years of Profiling the European Citizen, 2018: Amsterdam University Press, 84-88.

Gang Wang: Tech Talk: Intuit's AI-Powered Tax Knowledge Engine Boosts Filers' Confidence. Article published March 6 2019, available at https://www.intuit.com/blog/social-responsibility/tech-talk-intuits-ai-powered-tax-knowledge-engine-boosts-filers-confidence/?q=knowledge+engineering++taxation&qs=n&form=QBRE&sp=-1&pq=knowledge+engineering+taxation&sc=0-30&sk=&cvid=C86F17EA921A4662B0AEE8187B558298.

Samuel Warren, Louis Brandeis: The Right to Privacy, Harvard Law Review, vol. 4, No. 5. 1890, pp. 193-220.

Weizenbaum Institut: Statement on the Proposed Digital Content Directive. The statement was published July 4 2018, available at https://www.weizenbaum-institut.de/index.php?id=107&tx_news_pi1%5Baction%5D=&tx_news_pi1%5Bcontroller%5D=&tx_news_pi1%5Bnews%5D=36&L=5&cHash=416e3183f5ac501a1777c33e947ff6ae.

Alan Westin: Social and political dimensions of privacy. Journal of Social Issues vol 59, No. 2, pp. 431-434, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.455.4866&rep=rep1&type=pdf.

Lara White, Fiona Bundy-Clarke: Tentative further steps towards an agreed ePrivacy Regulation. Article for the law firm of Norton Rose Fulbright published February 15 2021, available at https://www.dataprotectionreport.com/2021/02/tentative-further-steps-towards-an-agreed-eprivacy-regulation/.

James Wilson, Paul Daugherty, Chase Davenport: The future of AI will be about less data, not more. Article published January 14 2019, available at https://hbr.org/2019/01/the-future-of-ai-will-be-about-less-data-not-more.

Alan Winfield: Ethical standards in robotics and AI, Nature Electronics 2019, vol. 2, available at https://doi.org/10.1038/s41928-019-0213-6.
Eva Witzleb, Pascal Schumacher: Datenschutz vs. Kartellrecht - Die nächste Runde. Article published May 6 2021, available at https://www.noerr.com/de/newsroom/news/datenschutz-vs-kartellrecht.

David Wright, Paul de Hert, Serge Gutwirth: Are the OECD guidelines at 30 showing their age? Communications of the ACM, vol. 54, issue 2, February 2011, pp. 119-127.

Wenjun Wu, TiejunHuang, KeGong: Ethical Principles and Governance Technology Development of AI in China, Engineering vol. 6, issue 3, March 2020, pp. 302-309.

Joanna You, Louis Berney: Guangzhou International Institute of AI launched in Nansha. Article published December 15 2017, available at https://www.lifeofguangzhou.com/whatsNew/content.do?contextId=6987&frontParentCatalogId=199&frontCatalogId=200.

Tal Zarsky: The Trouble with algorithmic decisions: An analytic roadmap to examine efficiency and fairness in automated and opaque decision making, Science, Technology, & Human Values 2016, vol. 41 (1), pp. 118-132.

Marek Zubik, Jan Podkowik, Robert Rybski: European Constitutional Courts towards Data Retention Laws, Law, Governance and Technology Series, Springer Nature Switzerland AG 2021.

Shoshanna Zuboff: The Age of Surveillance Capitalism – The Fight for Human Future at the New Frontier of Power. Profile Books, 2019.

Katharina Zweig, Sarah Fischer, Konrad Lischka: Wo Maschinen irren können – Verantwortlichkeiten und Fehlerquellen in Prozessen algorithmischer Entscheidungsfindung, Bertelsmann Stiftung Publishing Gütersloh 2018.

Stanford University: One Hundred Year Study on Artificial Intelligence (AI100). Report published 2015, available at https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf.