Prof. Dr. Lilian Mitrou

University of the Aegean

DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES

IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

Prof. Dr. Lilian Mitrou

DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES - IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

A. ARTIFICIAL INTELLIGENCE: A NEW LANDSCAPE OR A NEW ERA?

1. Introduction: artificial intelligence and cognitive services as every-day reality?
2. Artificial intelligence and machine learning: framing and understanding the notions

2.1. What is Artificial Intelligence?

2.2. What is Machine Learning?

3. The Technological Environment: AI, Big Data and Internet of Things

B. ARTIFICIAL INTELLIGENCE AND PERSONAL DATA

1. AI and processing of personal data
2. AI and the General Data Protection Regulation
   - 2.1. AI -proof definitions?
   - 2.2. The scope of application
3. Lawfulness and Fairness of processing - AI, consent and legitimate interests
4. AI, Fairness and Discrimination
5. AI and the Data Processing /Protection Principles
   - 5.1. The purpose limitation principle
   - 5.2. AI, Proportionality and Data Minimization Principle
   - 5.3. AI and the Accuracy Principle
6. AI and Transparency
7. Accountability and Risk Assessment
8. AI and the Data Subject: Profiling and the Rights to Human Intervention and Explanation

C. AI, ETHICS AND FUNDAMENTAL RIGHTS

1. Does GDPR deal sufficiently with AI?
2. Data Protection friendly AI by design?
3. Of Fundamental Rights and AI Ethics

DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES.

IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ? [1]

A. Artificial intelligence: a new landscape or a new era?

1. Introduction: artificial intelligence and cognitive services as every-day reality?

Seven decades after Alan Turing's "intelligent machines"[2], what we conceive as Artificial Intelligence is anything but science fiction. On the contrary: after several cycles of boom and bust we record recently a surge of interest in machine learning, algorithmic decision making and offering of cognitive services[3]. Significant advancement has been achieved in particular with regard to the processing of large amounts of information, the analysis and prediction of human behavior and characteristics, and in related fields such as robotics, computer vision and autonomous systems. To a great extent the rapid evolution of Artificial Intelligence is to be attributed to the exponential growth of "datafication" [4]. In the two first decades of 21st century the confluence of machine learning and the large datasets results to an increased number of products and services, in public and private sector, in any kind of application[5].

---

[1] This study has been commissioned by Microsoft in 2018. The views and opinions expressed in this study are those of the author and do not necessarily reflect the policy or position of Microsoft.

[2] See Alan Turing 1950. Computing Machinery and Intelligence, 49 Mind, pp. 433– 460.

[3] C. Cath, S. Wachter, B. Mittelstadt, M. Tadde, L. Floridi, Artificial Intelligence and the 'Good Society': the US, EU, and UK approach, Science and Engineering Ethics, Volume 24, Issue 2 (2018), pp 505–528.

[4] See Mayer-Schönberger, V. and Cukier, K. 2013. Big Data. A Revolution That Will Transform How We Live, Work and Think, p. 78.

[5] European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems, March 2018, p. 6.

What is making Artificial Intelligence the major trigger for the "Fourth Industrial Revolution"[6] is not only, though primarily, the ever more sophisticated technological potential and the availability and processability of vast amount of data but also the fact that AI is no more "the domain of a few nerdy specialists working mainly in academia, financial services or large marketing departments"[7]. The AI research is shifting from being driven by academic curiosity to being driven by economic and social demands[8]. The AI developments can be found across the full range of business activities. AI is becoming a reality. In their everyday professional and private life people are dealing increasingly with AI artefacts.[9] Without human intervention or control, smart systems are able to conduct dialogues with users, respond to their needs and requests and make suggestions to them[10]. Moreover, they are reaching the "average user"[11] through the

[6] M. Brkan, Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond Electronic copy available at: https://ssrn.com/abstract=3124901. The Council of Europe Consultative Committee recognises that "as occurred in the past with cloud computing, Big Data and IoT, there is a clear tendency of some vendors to magnify the possibilities of AI and the term has become a buzzword in contexts that do not strictly involve this technology. However, there is a basis of truth in this attention to AI concerning the peculiar technological environment that makes it possible today to achieve results that could only be dreamt of in the past". See Report on Artificial Intelligence, September 2018, p. 5. However commentators warn about regarding AI as the new "Hype". See S. H. Reimer and C. Wegener, Künstliche Intelligenz: Vorsicht Hype! Datenschutz und Datensicherheit 10/2018, p. 599f.

[7] See S. Finlay, Artificial Intelligence and Machine Learning for Business, Third edition 2018, p. 3.

[8] See Yunhe Pan, who mentions that the new goals and problems in intelligent cities, medicine, transportation, logistics, manufacturing, and smart products, as well as driverless automobiles and smartphones, all require AI development, in Heading toward Artificial Intelligence 2.0, Engineering 2 (2016), p. 410.

[9] Voice recognition models are now capable of responding correctly to all sorts of user requests in the most diverse situations while image recognition programs are able to recognise figures – and autonomous cars will become a reality in the streets in the coming years.

[10] See European Group on Ethics in Science and New Technologies Artificial Intelligence, Robotics and 'Autonomous' Systems with references to speech recognition interfaces and recommender systems of online platforms, such as Siri, Alexa and Cortana.

[11] Amazon's Echo, Apple's Siri and Google Translate are just three well known software products.

accessibility of cheap, enormous computational power and connectivity that create a new context.

"Algorithms and AI have come to represent new mythologies of our time", as the CNIL, the French Data Protection Authority emphasizes[12]. If "General AI" still sounds more as an expectation or a distant fear[13] , artificial intelligence is supporting human expertise and action in many domains. If machine learning processes are deployed in contexts varying from fraud prevention to the development of autonomous vehicles (self-driven cars), at the same time low cost, scalable AI tools and services are accessible practically to anyone: voice generating features in smartphones, personal assistants, facial and pattern recognition.[14]

AI is "traditionally" related with utopian or -mostly- dystopian narratives …""of a world that surreptitiously adjusts the environment to the needs and desires of its users "[15] or…vice versa. In their work titled "Slave to the algorithm", Edwards and Veale point out that algorithms increasingly regulate our lives, as they enable or support decisions that they are vital of our welfare and freedoms[16].

Does AI affect the fundamental rights and freedoms of a person and in which way …? At this point we would like to indicate

[12] CNIL, COMMENT PERMETTRE À L'HOMME DE GARDER LA MAIN ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, Decembre 2017, p. 14.

[13] As mentioned by the Datatilsynet (the Norwegian DPA), "General AI refers to systems that are as versatile as humans when it comes to learning and problem solving. But it will probably be several decades before it is achieved". See Datatilsynet, Artificial Intelligence and Privacy – Report January 2018, p. 5.

[14] C. Kuner, D. J. B. Svantesson, F.H. Cate, O. Lynskey and C. Millard, Machine learning with personal data: is data protection law smart enough to meet the challenge? International Data Privacy Law, 2017, Vol. 7, No. 1, pp. 1-2.

[15] M. Hildebrandt, Law as Information in the Era of Data-Driven Agency, THE MODERN LAW REVIEW , Volume 79 January 2016 No. 1,pp 1-30, 4

[16] See L. Edwardš and M. Veale, Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for. Duke Law and Technology Review, 16 (1) 2017, pp. 1-65, 19.

a) the fact that offering and making use of such cognitive services presupposes, generates and/or results to the processing of personal data[17]. Algorithms cannot accurately learn from their environment without large amounts of personal data. Departing from the assumption that "the more data the better the result", the demand for data is steadily growing. In more clear terms: personal information is the fuel and the (by)product of AI applications.
b) the fact that such systems are designed to anticipate outcomes about the behaviour, the preferences, the conduct of a person. Profiling and classification algorithms determine how individuals and groups are assessed and managed while recommendation systems give users directions about when and how to exercise, what to buy, which route to take or even who to contact[18].
c) the "opacity" of these tools. As indicated by the European Group on Ethics in Science and New Technologies, "it is unfortunate that some of the most powerful among these cognitive tools are also the most opaque"[19].

Putting everything online and interconnecting anything "everyware"[20] enables persistent monitoring and surreptitious adaptation[21]. Many AI products and services are adaptive tailoring their responses to the behaviour of individual

[17]As underlined in the COMEST Report , there are two kinds of algorithms that can be distinguished: deterministic algorithms, that control the predictive behaviour of deterministic robots; and AI or stochastic algorithms, with learning abilities that form the heart of cognitive robots. AI-based, cognitive robots learn from past experiences and calibrate their algorithms themselves, so their behaviour will not be perfectly predictable, and will likely become an issue worthy of serious ethical attention and reflection. UNESCO-World Commission on the Ethics of Scientific Knowledge and Technology (COMEST), Report on Robotics Ethics, Paris 2014, p.4.

[18] B. D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter and L. Floridi, The ethics of algorithms: Mapping the debate, Big Data & Society July–December 2016, pp. 1–21, 1.

[19] European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems, March 2018, p. 6.

[20] A. Greenfield, Everyware. The dawning age of ubiquitous computing (Berkeley: New Riders, 2006), p. 272.

[21] M. Hildebrandt, Law as Information in the Era of Data-Driven Agency, p. 4.

users. By identifying the content a user likes, they evolve and adapt their recommendations to users' usual preferences.

AI in its interplay with Big Data, ambient intelligence, ubiquitous computing and cloud augments the existing major, qualitative and quantitative shift with regard to the processing of personal information: never there has been so much data collected about so many individuals, stored in so many places and analysed and used[22]. The increasing availability of bandwidth for data transfer, data storage and computational resources, the interconnection and fusion of data and knowledge have changed profoundly the information environment.

In this perspective AI poses fundamental questions concerning its ethical, social and legal impact thus setting new challenges to privacy and data protection. Since 2016, many reports but also legislative initiatives appeared to consider and address the impact of artificial intelligence on society and law[23]. Does AI accelerate the erosion of data protection[24] and related fundamental rights or is there room for mitigating risks and preventing the adverse consequences of an "amplified" AI?

[22] COMEST, Report on Robotics Ethics, Paris 2014, p. 6ff.

[23] These include the European Commission's proposals for the EU to develop civil law rules on the use of robots and artificial intelligence, the European Parliament's Committee on Legal Affairs, the White House Office of Science and Technology Policy (OSTP), the UK House of Lords Select Committee's call for evidence, the UK government's report on growing the artificial intelligence industry. For the analysis of these reports see M. Butterworth, The ICO and artificial intelligence: The role of fairness in the GDPR framework, computer law & security review 34 (2018) 257–268, pp. 257ff. Also C. Cath, S. Wachter, B. Mittelstadt, M. Taddeo, L. Floridi, Artificial Intelligence and the 'Good Society': the US, EU, and UK approach, Sci Eng Ethics (2018) 24:505–528, 508ff.

[24] S. Simitis has warned of the erosion of data protection as a result oft a rash technological development , See Die Erosion des Datenschutzes – Von der Abstumpfung der alten Regelungen und den Schwierigkeiten, neue Instrumente zu entwickeln, σε B. Sokol (Hrsg.), Neue Instrumente im Datenschutz, Düsseldorf 1999, p. 5 ff.

2. Artificial Intelligence and Machine Learning: framing and understanding the notions

Undoubtedly, there is a confusion or at least a lack of precision in the terms used.[25] While reflecting on the impact of artificial intelligence on fundamental rights and freedoms it is indispensable to build a clear idea of the notions and functions involved. Of importance is also to integrate these terms and notions in a holistic technological context in which the processing of personal data evolves in a continuously transforming way: cloud computing, ubiquitous computing, Internet of (every)thing(s) and Big Data Analysis.

2.1.`What is Artificial Intelligence?

The generic, traditional definition of artificial intelligence to be found in the Oxford English Dictionary emphasizes on the tasks performed by computer systems that normally require intelligence "if done by men[26]/humans[27]", enumerating indicatively visual perception, speech recognition, decision-making, and translation between languages[28]. The technical definitions rely more on the idea of the "intelligent" machine, which - as flexible rational agent - perceives its environment and takes actions that maximize its chance of success at an arbitrary goal"[29]. AI combines the properties of digital technologies in general (including

[25] CNIL points out the differences between the austere notion of artificial intelligence in scientific circles and the mainstream understanding of the term. See COMMENT PERMETTRE À L'HOMME DE GARDER LA MAIN ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, Décembre 2017, Report p. 14 .

[26] J. Minsky, Steps Toward Artificial Intelligence, PROCEEDINGS OF THE IRE, 1961, p. 8.

[27] J. Copeland, 'What is Artificial Intelligence?' (AlanTuring.net, May 2000) <http://www.alanturing.net/turing_archive/pages/reference%20articles/what%20is%20ai.html

[28] https://en.oxforddictionaries.com/definition/artificial_intelligence

[29] Russell S. and Norvig P. (2003), Artificial Intelligence: A Modern Approach (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, p. 23

scalability through copying of programs and speeding up their execution) with properties commonly thought to be unique to humans (competence)[30].

The ability to predict and anticipate possible future events on the basis of the analysis of data to model some aspect of the world is proposed as definition to codify and /or indicate not only the features but also the expectations from AI [31]. This aspect is expressed in a very clear way in the US report on AI[32] , which defines AI as a technology that — when used thoughtfully — can help to augment human capabilities, instead of replacing them, laying out an image labelled as "good AI society"[33]. In this approach AI is regarded as a replication of human analytical and/or decision-making capabilities[34]. AI mechanisms can perform various "functions of human intelligence: reasoning, problem solving, pattern recognition, perception, cognition, understanding, and learning''[35]. AI platforms and artefacts may support human decision making especially by probabilistic reasoning and discerning patterns in data[36].

We should notice that all or most of the AI applications currently in use are what we consider as "Narrow AI" that refers to specific application areas, such as playing strategic games, language translation, self-driving vehicles, and image

[30] See Miles Brundage, Scaling Up Humanity: The Case for Conditional Optimism about Artificial Intelligence, in European Parliament – European Parliamentary Research Service, Should we fear Artificial Intelligence? March 2018, p. 13.

[31] UK Government Office for Science. Artificial intelligence: opportunities and implications for the future of decision making, 2015, p. 5.

[32] White House Office of Science and Technology Policy (OSTP), Preparing for the Future of Artificial Intelligence, October 2016.

[33] Executive Office of the President National Science and Technology Council Committee on Technology (2016).

[34] S. Finlay, Artificial Intelligence and Machine Learning for Business, Third Edition 2018, pp. 19f.

[35] Kaori Ishi, Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects, AI & Soc (published online 31 August 2017), p. 18.

[36] See Microsoft, The Future Computed, Artificial Intelligence and its role in society. Published by Microsoft Corporation Redmond, Washington. U.S.A. 2018 (Foreword by Brad Smith and Harry Shum), 2018. p. 35f.

recognition thus contributing to areas such as commercial activities, research and healthcare. However, "true artificial intelligence" is about much more than just pattern recognition and prediction. General AI , namely is a system that can learn and act in a similar way as a person and exhibit intelligent behavior across the full range of cognitive tasks and a wide range of environments and problems[37] . AI is not likely to be achieved for the time being or even in the next decades, although many emphasize that the main feature of AI is exactly its unpredictability.

To assess the legal issues posed with regard to privacy and data protection necessitates also the understanding of the public perception of artificial intelligence. The main shift consists in the transition from something exceptional to something normal: the visitor of the planet in 1961 would have found "only a few machines (mostly "general-purpose" computers, programmed for the moment to behave according to some specification) doing things that might claim any real intellectual status"[38]. In their Document on Artificial Intelligence, Robotics, Privacy and Data Protection, the Data Protection and Privacy Commissioners pointed out the reflection on the public understanding of artificial intelligence provided by Wikipedia: in this perspective the subjective borderline around what constitutes "artificial intelligence" tends to shrink over time, as certain capabilities (such as optical character recognition) considered artificial intelligence are not regarded as artificial intelligence anymore as they become "a mundane routine technology"[39].

[37] See Executive Office of the President, Washington 2016, pp. 7–8.

[38] M. Minsky, Steps Toward Artificial Intelligence, PROCEEDINGS OF THE IRE, 1961, p. 8.

[39] See Artificial Intelligence, Robotics, Privacy and Data Protection – Room Document for the 38th International Conference of Data Protection and Privacy Commissioners, October 2016,p. 19.

2.2. What is Machine Learning?

As underlined by M. Hildebrandt, most of the infrastructure that gives rise to an "onlife world"[40] is supported by new techniques of artificial intelligence, notably by those of machine learning. Indeed, machine learning is one of the growing approaches by which AI is achieved[41], while many people use the terms AI and machine learning interchangeably.

The term machine learning is used to define " any methodology and set of techniques that finds novel patterns and knowledge in data and generates models that can be used for effective predictions about the data"[42] . Having the "ability to learn without being explicitly programmed", machine learning programs and techniques automatically improve with experience[43]. This encompasses the design, analysis, development and implementation of methods enabling a machine to operate via a systematic process, and to accomplish difficult tasks. It is to note that the algorithm[44] has the capacity to define or modify decision-making rules to handle new inputs.

---

[40] What Hildebrandt suggests as "onlife world" is "the new everyday where anything offline is turned online, while the infrastructures that supposedly make life easy, business more effective and society less vulnerable are saturated with artificial, data-driven agency". Mireille Hildebrandt, Law as Information in the Era of Data-Driven Agency, The Modern Law Review 79 (2016), pp. 1-30, p. 2.

[41] D. Kamarinou, C. Millard, and J. Singh, Machine Learning with Personal Data , Queen Mary University of London, School of Law Legal Studies Research Paper 247/2016, pp. 23f.

[42] See M. Van Otterlo, (2013) A machine learning view on profiling. In: Hildebrandt M and de Vries K (eds) Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology. Abingdon: Routledge, pp. 41–64, p. 46.

[43] See Tom M Mitchell, Machine Learning (McGraw-Hill Science/Engineering/Math, 1997) XV. As underlined by Information Commissioner's Office (UK), it's the ability of the algorithms to change their output based on experience that gives machine learning its power. See ICO, Big data, artificial intelligence, machine learning and data protection, par. 96.

[44] In the strict sense of the term, an algorithm is the description of a finite and unambiguous sequence of steps (or instructions) for producing results (output) from initial data (input). CNIL mentions "a recipe [as example of] an algorithm…., as a dish can be made from its ingredients."_. (CNIL, COMMENT PERMETTRE À L'HOMME DE GARDER LA MAIN ? p.). As example of a simply to understand algorithm the Fundamental Rights Agency mentions the list of persons is to be sorted according to their age. "The computer

Artificial intelligence grounded in machine learning concerns algorithms which have specifically been designed so that their behaviour can evolve over time, based on their input data. Machine learning algorithms are a whole new class of algorithms: we notice a steadily progress "from a programming world to a learning world"[45]. Classical algorithms are deterministic, their operating criteria are clearly defined by the people wishing to run them. Machine learning constitutes a disruption from conventional algorithms. Machine learning algorithms are probabilistic: their output is always changing depending on the learning basis they were given, which itself changes in step with their use. In particular, the development of deep learning technologies allows algorithms to solve complex operations leading to potential decisions[46].

Do algorithms regulate our lives? Operations, decisions and choices are increasingly delegated to algorithms, which may advise, if not decide, about how data should be interpreted. Machine learning is strictly related to prediction. The patterns relate to the relationships between (past) behaviours and outcomes thus enabling prediction about future behaviour. Algorithms are designed to anticipate outcomes, such as whether an individual or firm will repay a loan or jump bail. They are used to take or support decisions vital to people's life with regard to finance, housing, employment, education or- even – justice[47].

The introduction of machine learning into market processes drives the increasing personalization of contractual conditions and products offered to consumers. Search engines or news websites using personalisation and filtering

takes the ages of people on the list (input) and produces the new ranking of the list (output)". See European Union Agency for Fundamental Rights, #BigData: Discrimination in data-supported decision making, 2018, p. 4.

[45] Jean-Philippe Desbiolles, Public debate launch, CNIL, 23 January 2017.

[46] See 40th International Conference of Data Protection and Privacy Commissioners DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE (Tuesday 23rd October 2018, Brussels). The Commissioners underline however that this development makes such processes more opaque.

[47] See L. Edwards and M. Veale (2017) Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law and Technology Review, 16 (1). pp. 1-65, 19.

algorithms continue to mediate which and how information is accessed. Profiling and classification algorithms determine how individuals and groups are shaped and managed[48] .

Algorithmic systems are becoming familiar in both private and public aspects of life: How we understand our environment and react to it or interact with it is increasingly mediated by algorithms: recommendation systems give users directions about when and how to exercise, what to buy, which route to take, and who to contact[49]. Recommendation and filtering systems compare and group users to provide personalised content[50].

Moreover, AI applications serve as personal assistants: Nowadays AI capabilities include vision, speech, language and search. Learning (from and feeding by) the interests and the needs of the users, AI applications follow them at every turn, by extracting information, personalizing content, reminding rendezvous, advertising a new film and providing answers[51] to every day questions[52]. Systems are designed to see, hear, speak, understand, and interpret people's needs by using natural methods of communication[53]. AI platforms and artefacts may support human decision making especially by probabilistic reasoning and discerning patterns in data[54]. Computer vision, speech and knowledge recognition are made available to everyone to create AI-based systems

[48] See L. Floridi, Big data and their epistemological challenge. Philosophy & Technology 25(4) 2012, pp. 435–437.

[49] This is the case with AI-supported voice-generating features in smartphones such as Siri and/ or " personal assistants" such as Alexa.

[50] See B. A. Barnet, Idiomedia: The rise of personalized, aggregated content. Continuum 23(1) 2009, pp. 93–99.

[51] Questions answering to questions formulated either in a specific or an open-ended way.

[52] See Conrad Sebastian Künstliche Intelligenz – Die Risiken für den Datenschutz, Datenschutz und Datensicherheit 12/2017, p. 741.

[53] For example, Emotion APIs can analyze faces to detect feelings and personalize app's responses while Text Analytics APIs can detect sentiments from user's text.

[54] See Microsoft, The Future Computed, p. 35 .

and build their own AI-based solutions[55]. Offering services, tools and infrastructure to enable developers and organisations to integrate AI into their services and applications seems to be the next step[56]. These capabilities, especially those that are customizable, support (better) decisions and enable business/organization processes adapted to specific needs[57].

Either as "assisted" or "augmented" or "autonomous"[58] AI may augment human decision making. Artificial intelligence can not only "help to assist or replace humans with smart technology in difficult, dirty, dull or dangerous work"[59]. It promises to eradicate, or at least reduce, human bias in decision-making processes[60]. Machine learning promises also to reduce uncertainty[61] : from matching people on dating sites, to detection of credit card fraud or identification of criminal suspects predictive machine learning models provide insight into the likelihood, or odds, of each outcome.

---

[55] Microsoft for example uses and offers image processing algorithms to identify, capture and moderate pictures or face APIs or detect human faces and/or organize images into groups based on similarity.

[56] This is the case of Cognitive Services, defined a collection of Representational State Transfer (RESTful) intelligent application program interfaces (APIs) that allow systems to see, hear, speak, understand, and interpret people's needs by using natural methods of communication. These services are addressed to developers to add intelligent features—such as emotion and sentiment detection, vision and speech recognition, knowledge, search, and language understanding—into their applications.

[57] Microsoft, The Future Computed – Artificial Intelligence and its role in society, 2018, p. 42.

[58] Systems that can learn to perform tasks without human direction or without supervision.

[59] European Group on Ethics in Science and New Technologies, Artificial Intelligence, Robotics and 'Autonomous' Systems, 2018, p. 6.

[60] See J. Kleinberg, Himabindu Lakkaraju, J. Leskovec, J. Ludwig. Sendhil Mullainathan, Human Decisions and Machine Predictions, The Quarterly Journal of Economics, Volume 133, Issue 1, 1 February 2018, pp. 237–293.

[61] Microsoft regards AI tools as valuable "because, as researchers in cognitive psychology have established, human decision making is often imperfect", The Future Computed p. 35.

3. The Technological Environment: AI, Big Data and Internet of Things

AI is not developed in isolation. It forms part of a –technological – environment of enabling technologies[62] , while its relevance arise in a broader socio-economic context. It is the confluence of these technologies that makes AI the driver of the – next ? – (r)evolution.

AI is reinforced by specific developments and trends[63]: a) the availability and accessibility of enormous - and often cheap - computational power and infrastructure, b) the ever-increasing availability of large datasets from various domains, c) the evolution of more sophisticated statistical and probabilistic methods, d) the tendency to transform ever more places into IT –driven or IT-friendly environments. Developments and trends that amount progressively to the so called "datafication"[64], the process whereby life-processes must be converted into streams of data inputs for computer-based processing, feeding expectations, concerns and fears. At the same time processes, devices and places are becoming more or less (slowly or) rapidly no more – only "digital" - but - moreover - "intelligent"[65] or "smart"[66].

AI is fueled by a wide range of technological drivers: mobile connectivity, cloud infrastructure, the proliferation of sensors, advances in processing power, machine-learning software and storage[67]. Machine learning takes advantage of

---

[62] B. C. Stahl and D. Wright are referring to "enabling technologies", i.e. technologies that generate and collect data and act on the world and interact with humans. See B. C. Stahl and D. Wright, AI ETHICS- IEEE Security & Privacy (Special Issue) May/June 2018, p. 27.

[63] See C. Cath, S. Wachter, B. Mittelstadt, M. Taddeo, L. Floridi, Artificial Intelligence and the 'Good Society': the US, EU, and UK approach, Sci Eng Ethics (2018) 24, pp. 505–528, 508.

[64] Nick Couldry and Jun Yu, Deconstructing datafication's brave new world, New media & society 2018, pp. 1-19.

[65] Intelligent manufacturing, intelligent agriculture, intelligent medicine.

[66] Smartphones, smart homes, smart vehicles, smart cities.

[67] See PWC, Leveraging the upcoming disruptions from AI and IoT How Artificial Intelligence will enable the full promise of the Internet-of-Things, 2017, p. 8.

the scalable processing of vast sets of data enabled by the widespread and low cost availability of the cloud and its effectively unlimited resources. In the last years Cloud providers started offering cloud-supported machine learning services and tools, with a significant focus on predictive analytics[68]. However, AI goes on growing especially through Big Data[69] and the general Internet of Things.

AI can cope with the analysis of big data in its varying shapes, sizes and forms[70]. The French DPA, CNIL notes that AI and Big Data are indissociable[71]. In fact, the relation between AI and big data is bi-directional: Artificial intelligence, through machine learning, needs a vast amount of data to learn data in the realm of big data considerations. At the same time big data uses artificial intelligence techniques to extract value from big datasets[72].

AI can unlock the value of big data analytics [73]. In their combination, AI and Big they become "part of business as usual for many organisations in the public

---

[68] The underlying technologies are increasingly accessible to data controllers, with major cloud computing providers including Amazon, IBM, Google, and Microsoft offering low-cost, scalable, cloud-supported machine learning services and tools, Amazon Machine Learning <https://aws.amazon.com/machine-learning/> Google Cloud Prediction API Documentation <https://cloud.google.com/prediction/docs/> Microsoft Azure, Machine Learning <https://azure.microsoft.com/en-gb/services/machine-learning/>. More about in Christopher Kuner et al., Machine learning with personal data: is data protection law smart enough to meet the challenge?

[69] As underlined by the Executive Office of the President, the "current wave of progress and enthusiasm for AI began around 2010, driven by the availability of Big Data, which provided raw material for dramatically improved machine learning approaches and algorithms; which in turn relied on the capabilities of more powerful computers". See Executive Office of the President, National Science and Technology Council, Committee on Technology (2016) Preparing for the future of artificial intelligence. https://obamawhitehouse.

[70] ICO, Big data, artificial intelligence, machine learning and data protection, p. 7.

[71] CNIL, Comment Permettre à l'homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, Décembre 2017, p. 18.

[72] 38th International Conference of Data Protection and Privacy Commissioners, Artificial intelligence, Robotics , Privacy and Data Protection, October 2016, p. 4 .

[73] Characterised by the "three Vs": high-volume, high-velocity and high-variety information assets, demanding cost-effective, innovative forms of information processing for enhanced insight and decision making. See Gartner IT glossary Big data. http://www.gartner.com/it-glossary/big-data

and private sectors"[74]. This is supported by the development of tools to manage and analyse data, and growing awareness of the opportunities it creates for business benefits but also for research and development.

A decisive factor is the exponential growth and availability of data, including data collected and produced by the Internet of Things[75]. Together with Big Data IoT symbolizes the dramatic evolution of technologies[76]. The Internet of Things (IoT) closely linked to the notion of "ubiquitous computing" relies on the extensive processing of data through the network of sensors that communicate and exchange data in an unassertive and seamless way. It seems that also in this case there is a kind of bi-directional relation: To achieve its full potential, the IoT needs to be combined with Artificial Intelligence (AI)and at the same time the impact of AI on every aspect of life will be multiplied and more sophisticated by its combination with the Internet of Things.

[74] Information Commissioner Office (ICO), Big data, artificial intelligence, machine learning and data protection, 2017, p. 9.

[75] The Internet of Things relates to an infrastructure in which millions or billions of sensors embedded in common, everyday devices –"things" as such, or things linked to other objects or individuals –are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities. Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, p. 4.

[76] See Kaori Ishii, Comparative Legal Study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects, AI & Soc 2017.

B. ARTIFICIAL INTELLIGENCE AND PERSONAL DATA

1. AI and processing of personal data

Even if not all AI applications involve the processing of personal information, machine learning and AI software have multiple and valuable use in processing personal data[77]. Profiling, performed in the context of Big Data and machine learning, gains a new qualitive and quantitative dimension. Machine learning multiplies mining capabilities and helps discovering valuable knowledge from large state or commercial databases containing equipment maintenance records, loan applications, financial transactions or even medical records and make predictions or suggestions based thereon. As such systems, depending on their nature and architecture, need a lot of data about the persons/ users, they extract increasingly more data about them[78]. Personal data and Artificial Intelligence are "a two -way street": personal data feeds AI and AI produces more inferred data[79].

Tendencies already identified in the context of Big Data do apply with enhanced implications for data processing and protection when combined with AI. These tendencies refer mainly to:

a) the collection of "all data" or "as much data as possible" to be able to further learn and analyse. The Norwegian Data Protection Authority puts specific

[77] M. Butterworth, The ICO and artificial intelligence: The role of fairness in the GDPR framework, Computer Law and Security Review 34 (2018), pp. 257-268, 258.

[78] So the use of Specified Cognitive Services Data are provided to Microsoft by (or on behalf of) the Customer through the use of the cognitive services, such as Bing Search Services or Microsoft Translator. This data is used both for providing cognitive services and (as training data) to improve products and services.

[79] Giovanni Buttarelli, Privacy in an age of hyperconnectivity, Keynote speech to the Privacy and Security Conference 2016 Rust am Neusiedler See, 7 November 2016. "Personal data have increasingly become both the source and the target of AI applications", as expressed in the Council of Europe Consultative Committee Report on Artificial Intelligence and Data Protection, Strasbourg 17 September 2018.

emphasis to the greater demand of data[80]. In this context we should consider also that collected, analysed, used or produced / generated are also "new types of data"[81] .

b) that re-purposing or multi-purposing of data[82], that is generated from a specific context and/or activity but may be used and analysed for an initially unknown and wide range of purposes. AI enables harvesting and harnessing of vast amount of data and its -oft repurposed – further use. This is also fueled by the so called "unpredictability of outcomes", which makes some authors to consider that Big Data analytics powered by machine learning are at odds with the purpose limitation principle of data protection[83] .

Devices are becoming slightly but steadily precious "supporters": handling banal and repetitive tasks by the use/help of AI releases resources, energy and time. Receiving services such as translators, Bing Speech APIs, Face APIs , smart devices allow their owners to explore congested cyber information landscapes. Concreter, by collecting the available information, filtering it, and presenting relevant data to their owners, devices operate in a way that embeds and simultaneously enhances the cognitive process and models of a human brain[84]. Data processing based on AI and especially with regard to cognitive services entails the features of data processing as prerequisite and/or outcome of

[80] It seems that the Datatilsynet does not share the frequently heard "typical mantra" that the more the data we can feed into the model, the better the result. See Datatilsylnet, Artificial Intelligence and Privacy -Report, 2018, p. 11. Also ICO, who regards the "tendency to collect all data" as one of the main aspects of big data analytics using artificial intelligence with implications for data protection. See Report, p. 9.

[81] Such as data related to "speaking style" or "sentiment analysis".

[82] For the issues raised with regard to the purpose limitation principle.

[83] Nadezhda Purtova (2018) The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, 10:1, pp. 40-81, 56.

[84] Conti, Passarella and Das are referring to personal devices as the "avatars of their respective users" in M. Conti, A. Passarella, S. K. Das, The Internet of People(IoP) :A new wave in pervasive mobile computing, in Pervasive and Mobile Computing, 41 (2017), p. 1-27.

applications but it surpasses this dimension, both by predicting and influencing the forming of personal will and decision making.

Especially in smart environments it is the hyper-connected active user who creates and diffuses huge quantities of – not rarely very personal and pervasive – information about her. As emphasized by the UK Information Commissioner, the proliferation of internet connected devices and tracking of online activity means a large amount of personal data is generated automatically, rather than consciously provided by the individual [85]. The interaction of our devices with applications and devices of other uses generates new and multiply useful, if not exploitable information. Glancy highlights how data from autonomous vehicles could convey sensitive information about where the user is and what he or she is doing, as well as a comprehensive log of places the user visited and will visit in the future[86].

The potential use of information needed/required for using AI services or generated thereof may raise concerns of tracking and profiling, which constitute in the final analysis an inherent element of such services. Profiling is a matter of pattern recognition, which is comparable to categorisation, generalisation and stereotyping[87]. Profiling involves collecting data (recording, storing and tracking) and searching it for identifying patterns (with the assistance of data mining algorithms)[88]. Information about an individual is mined in order to determine

[85] ICO, Report, p. 12.

[86] This is the case where "the location where the vehicle is regularly parked overnight (e.g. in a high-income neighborhood) could be used to profile the likely user (e.g. as wealthy) and to predict the user's actions (e.g. likely to shop at high-end shops)". Furthermore "the present location of an autonomous vehicle user [and] that person's past travel patterns", but also "his or her future travel plans". See D. Glancy, Privacy in Autonomous Vehicles (2012) 52 Santa Clara L. Rev., pp. 1171, 1186.

[87] Performing profiling necessitates large quantities of digitised data from observation of the behaviour and characteristics of individuals, determination of the probability relations (correlations) between certain behaviours/characteristics and other behaviours or characteristics and inference, based on certain behavioural variables or observable characteristics of an individual identified in general terms, of new characteristics or past, present or future behavioural variables. See Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever, Antoinette Rouvroy, Application of Convention 108 to the profiling mechanism. Some ideas for the future work of the consultative committee (T-PD).

[88] ENISA. Privacy, Accountability and Trust– Challenges and Opportunities, 2011, p. 16.

whether she fits a previously established profile and make decisions about individuals and/ or groups[89]. Concerns about impacts of profiling, which is usually performed without the consent, or even the knowledge of the person affected, relate to the fact that through profiling and data mining, data that could be considered as insignificant or trivial may be proved sensitive providing intimate knowledge about, e.g., life style or health risk[90]. These concerns are fed also by the decreasing amount of human involvement to profiling, which increasingly is carried out by "machines"[91].

AI may affect privacy in various aspects: with regard to informational privacy, including surveillance privacy, interests but also to autonomy of a person. Informational privacy responds to the requirement that everyone should be in control of the information concerning her so as to formulate conceptions of self, values, preferences, goals and to be protect her life choices from public control[92], social disgrace or objectification. Intimidation effects which could have a negative impact on the exercise of fundamental rights[93].

Informational privacy concerns the capacity of an individual to control information about herself. It offers safeguards to preserve an underlying capacity

[89] For instance, flagging someone as a potential terrorist, or denying someone a loan. See Bart W. Schermer, The limits of privacy in automated profiling and data mining, Computer Law and Security Review 27 (2011), pp. 45-52, 50.

[90] See J. Čas, Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions. In: Gutwirth S., Poullet Y., De Hert P., Leenes R. (eds) Computers, Privacy and Data Protection: an Element of Choice. Springer, Dordrecht, (2011), pp. 139-169, 144.

[91] See D. Kamarinou, C. Millard, and J. Singh, Machine Learning with Personal Data, Queen Mary University of London, School of Law Legal Studies Research Paper 247/2016, p. 6.

[92] Glancy points out that comprehensive personal information collection could be used not only to profile and predict but also possibly to manipulate the behaviour of autonomous vehicle drivers (to stay away from the seedy side of town or to avoid attending a Trade Union meeting). See D. Glancy, Privacy in Autonomous Vehicles, (2012) 52 Santa Clara L. Rev. 1171, p. 1186.

[93] See the landmark Census Judgment of the German Federal Constitutional Court (1983). Bundesverfassungsgericht, Volkszählungsurteil Entscheidung von 15.12.1983 (BVerfGE 65, 1).

for autonomous decision - and choice-making[94], a value/right that constitutes an inherent characteristic of identity building, dignity and freedom. As emphasized by Hildebrandt and Gutwirth, a major problem identified with regard to AI supported profiling technologies is not only that they question the personal autonomy but, moreover, that they influence a person's sense of self[95].

The issues referring to the interference to the (right to) privacy and data protection arise in a quite compelling way. As analysed, data gained via AI applications and services may provide new insights and future projections about a person thus interfering with the right to personality and her (informational) self-determination[96]. The core issue is if individuals are able to retain control over their personal data. A preliminary question, reflecting a major concern with regard to the impact of AI on informational privacy is whether there should be limits to what AI systems can suggest to a person, based on a construction of the person's own conception of their identity[97].

Whether for "training purposes" or as part of their deployment, AI involves the processing of personal information, subject to the regulatory framework, if (it) exists. Without doubt, AI systems are subject to data protection laws and their respective requirements. The (broad range of) law governs AI in a twofold aspect: while designing and creating best practices for key aspects of a -legally and socially acceptable – development AI systems and while applying such systems, regardless of data processing being /is the goal or the result of the use of AI.

---

[94] See L. Mitrou, The Commodification of the Individual in the Internet Era: Informational Self-determination or "Self-alienation"? in Proceedings of 8th International Conference of Computer Ethics Philosophical Enquiry (CEPE 2009), INSEIT, Athens 2009, pp. 466-485.

[95] See M. Hildebrandt and S. Gutwirth, Profiling the European citizen: cross-disciplinary perspectives. Springer, New York (2008), p. 66. Also Norberto Nuno Gomes de Andrade, Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights, in Simone Fischer-Hübner Penny Duquenoy Marit Hansen RonaldLeenes GeZhang(Eds.), Privacy and Identity Management for Life, Springer 2011, p. 102 ff.

[96] See Conrad Sebastian, Künstliche Intelligenz – Die Risiken für den Datenschutz, Datenschutz und Datensicherheit 12/2017, pp. 740-744, 742.

[97] European Group on Ethics in Science and New Technologies, Artificial Intelligence, Robotics and 'Autonomous' Systems, p. 11.

Respecting privacy and data protection laws is not simply a matter of (demonstrating) compliance with the legal framework. The acceptance and consequently the use of AI services is highly depending on the trust of the users who have to be confident that their informational privacy is protected[98]. If users regard these services as possible threat to their informational privacy they will refrain from their use, although there has been little market resistance to the adoption of - the comparable? - mobile phone technology[99].

Is the current legal framework AI-proof ? Are the data protection and privacy rules and principles adequate to deal with the challenges of AI or do we need to elaborate new principles to work alongside the advances of AI technology[100] ? Is the current legal environment clear enough to allow or "guide the people building, using and applying AI systems"[101]?

2. AI and the General Data Protection Regulation

Privacy and data protection law seems to be the key area of law dealing with the effects of machines on society[102]. The birth of data protection in Europe, especially the Data Protection Directive 95/46/EC was linked to the impressive developments of the 70s[103]. Already from the time of the adoption of the Directive, the middle of the 90s, the rapid expansion of Internet usage and the appearance of many online services set new challenges for regulators. Next to the benefits of

[98] MICROSOFT, The Future Computed, p. 66.

[99] See Lisa Collingwood, Privacy implications and liability issues of autonomous vehicles, Information & Communications Technology Law, 26:1 (2017), 32-45 .

[100] See Lisa Collingwood, Privacy implications and liability issues of autonomous vehicles, pp. 32ff.

[101] MICROSOFT-THE FUTURE COMPUTED, p. 56.

[102] M. Butterworth, The ICO and artificial intelligence: The role of fairness in the GDPR framework, p. 258.

[103]See S. Simitis, Kommentar zum Bundesdatenschutzgesetz (2014) p. 82 ff, 134 ff.

digital technologies, the reality of collecting, processing, storing, and using data changed has brought new, quite unknown risks[104].

The vigorous data protection framework was regarded as outdated and cumbersome within an t an Internet (indeed, Web 2.0) environment, that is "more vulnerable than most people had assumed"[105]. Evolving technology and the ubiquitous nature of computing have created countless problems for the protection of personal data, as they jeopardize fundamental principles of "traditional" data protection law, such as the purpose specification/ limitation principle or the notice and consent model[106]. The adaptation of the legal principles to the convergence of "real and digitized" worlds into a seamless space for individuals, a convergence facilitated by the ever-increasing number of bridges created by both the innovative use of existing technologies and the development of new and emerging technologies, was the challenge to be faced by the European legislators[107].

The conception of GDPR aimed at responding to the risk of increasing loss of relevance and effectiveness of the 3rd generation legislation[108]. More than a simple revision of the Data Protection Directive and less than a regulatory

[104] See Burri, M., & Schär, R. (2016). The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. Journal of Information Policy, 6, pp. 479-511.

[105] Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, 2013.

[106] See A. Mantelero, The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. Computer Law & Security Review 30(6) 2014, pp. 643-660, 645.

[107] See L. Mitrou, Privacy Challenges and Perspectives in Europe in M. Bottis (ed.) An Information Law for the 21st Century (Proceedings of Third International Seminar on Information Law), Athens 2011, pp. 220-236. Buttarelli emphasized that this situation created legal uncertainties that may undermine trust and harm the development of the Information Society. See G. Buttarelli (Assistant European Data Protection Supervisor), "Internet of things: ubiquitous monitoring in space and time", European Privacy and Data Protection Commissioners' Conference Prague 2010.

[108] See Kiss A and Szoke G., Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation In: Gutwirth S, Leenes R, de Hert P (eds.) Reforming European Data Protection Law, Springer, Netherlands, pp. 311ff.

paradigm shift, the Regulation attempts to keep path with technological and socio-economic changes while guaranteeing the persons' fundamental rights and enabling the control over their data. Is this a mere declaration of good purposes or is the GDPR another regulatory text, whose "sustainability" may be contested already at the start of its entry into implementation in May 2018? Is GDPR applicable to AI? Can the use of cognitive services be effectively regulated by the new regulatory framework it as far as it concerns the use of personal data?

GDPR does not specifically address AI. Although the difficulties and complexities of digital environments have been taken into account by the designing of the data protection regulatory strategy, the regulatory choice in GDPR consists more in what we perceive as "technology – independent legislation". Refraining from technology-specific terminology and provisions seems to be a conscious choice to be attributed to the "technological neutrality approach"[109] .

Technology independent rules are regarded as a means to stand firm with technological turbulences[110] . Technology obviously develops more quickly that the law: even within the 5-years period between the Commission's proposal and the adoption of GDPR technology or at least the spectrum and the extent of its uses have changed substantially : the explosion of mobile apps or the introduction/ offer of cognitive services and the Internet of Things are perhaps the more apparent examples.

Emphasis is put not on the technology used for data processing but on the effects to be regulated, on the risks and impacts on fundamental rights that are to be faced. Technology neutrality concept emerged as a regulatory principle, a canon, where states are proceeded to promulgate technology impartiality.[111] The

[109] With GDPR the European legislators adhere explicitly to the technological neutrality approach as Recital 15 cites that the protection of natural persons should be technologically neutral and should not depend on the techniques used.

[110] Bert-Jaap Koops, Should ICT Regulation be Technology-Neutral? Starting points for ICT regulation. Deconstructing prevalent policy one-liners, IT & LAW SERIES, Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens (eds.), Vol. 9, , The Hague: T.M.C. Asser Press, 2006, pp. 77-108.

[111] As stated in a Commission's Communication in 1999, technological neutrality means that 'legislation should define the objectives to be achieved, and should neither impose,

technological neutrality of law requires that the latter generates the same effects irrespective of the technological environment in which these norms apply[112], a policy that presupposes, however, that the legislators have in mind and take into consideration both the issues posed by current technologies and the future trends.

Adopting technology-neutral provisions seems to be the path to deal with the unforeseeability of the technological developments and consequently ensure that the law is sustainable to respond successfully to such - unpredictable - developments over a sufficiently long period. The GDPR has not adopted a "sunset clause", which would provide by default that the law will expire after a certain period, unless it will be extended[113]. Principally, the rules and principles of GDPR, such as the notion of identifiability of the data subject, are flexible enough to cover future technological changes and confer lasting protection. However, we should not ignore the risk that the vagueness that characterizes some terms and notions may over the years result in large divergences in interpretation of the law and - consequently- legal uncertainty[114].

The GDPR applies both in the phase of AI development and with regard to its use for analyzing and decision making about individuals. GDPR contains

---

nor discriminate in favor of, the use of a particular type of technology to achieve those objectives". Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Towards a new Framework for Electronic Communications Infrastructure and Associated Services: the 1999 Communications Review COM (1999) 539 final, p. 14.

112 See M. Hildebrandt and L. Tielemans, Data protection by design and technology neutral law, Computer Law & Security Review Volume 29, Issue 5 (2013), pp. 509-521, 510.

113 Article 97 of GDPR provides for the competence of the European Commission to submit by 25 May 2020 and every four years thereafter a report to the European Parliament and to the Council. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

114 R. Ali points out that technological neutrality of the law may result in regulations whose meaning is so vague that its application to the technology is often a matter of guesswork. Technological Neutrality, Lex Electronica, vol. 14 n°2 (Automne / Fall 2009), p. 9.

important rights for users relating to any processing of their personal data as well as obligations of processors which will shape the way AI will be developed and applied[115]. Especially relevant for the AI-environment are the provisions concerning the scope of application, the legal grounds, the data protection principles and automated decision-making.

2.1. AI -proof definitions?

First of all, it should be noted that the definitions of the core notions of GDPR, i.e. personal data and data processing are formulated in a broad, flexible and adaptable way so that they may be applied to technological context of AI[116]. The definition of personal data has been aligned with the online reality. The definition contains not only that a person may be identified "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" (as included already in the Directive 95/46/EC Article 2a): The "online identifier"[117] has been

[115] See P. Niemitz, Constitutional Democracy and Technology in the age of Artificial Intelligence. Accepted for publication in Royal Society Philosophical Transactions A 2018.

[116] Paul Schwartz and Daniel Solove, Reconciling Personal Information in the United States and European Union' 102 California Law Review (2014), pp. 877-916, 902.

[117] Even under the application of Data Protection Directive (95/46/EC), the European Court of Justice (ECJ), broadly interpreted the DPD to include certain IP addresses into the definition of personal data because controllers could "likely reasonably" compare their data with a third-party's separate system, which contains identifying information, to identify individual users. See Case C-582/14, Breyer v. Bundesrepublik Deutschland, 2016 E.C.R. II-779. Even if personal information only entails reference ID numbers, such identifiers are typically unique to a specific person. While in all such cases additional information may be necessary to attribute information to the data subject, such information would be merely pseudonymised and count as personal information. See M. Berberich and M. Steiner, Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers? European Data Protection Law Review , Volume 2 (2016), Issue 3, pp. 422 – 426, 424 .

added to the indicative list of features that may identify a natural person, directly or indirectly (Article 4 par 1 (a)[118].

The key concept and choice of "identifiability" allows an open interpretation "as what constitutes a relevant possibility of identification and a relevant relationship between information and an individual"[119]. It is the identifiability of a person that results in the applicability of the law. Identifiability is understood as the ability to single out and/or identify an individual on the bases of particular pieces of information which we may call "identifiers" and which hold a particularly privileged and close relationship with the particular individual[120]. To ascertain whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, by the controller or by another person, to identify the natural person directly or indirectly. By formulating its opinion on the definition of personal data the Article 29 Data Protection Working Party (hereafter Article 29 DPWP) stated that the possibility of identifying an individual no longer necessarily means the ability to find out his or her name : "even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense"[121].

As clarified by the Article 29 DPWP "'identification not only means the possibility of retrieving a person's name and/or address, but also includes

[118] Recital 30 of GDPR states that" natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them".

[119] N. Purtova (2018) The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, 10:1, pp. 40-81, 44.

[120]Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, p. 12f.

[121] Article 29 DPWP, Opinion 4/2007, p. 14.

potential identifiability by singling out, linkability and inference"[122]. With Recital 26 GDPR expands indeed the scope of personal data through reference to "singling out"[123] . In this context, data such as name, age or e-mail address but also metadata or background data (location, search history, preferences) as well as biometric data such the voice or the facial patterns fall under the notion of personal data. As personal data may also be qualified the so- called forecast data, that enable predictory statements about a person[124].

Identifiability is conceived as a vague but dynamic criterion, that is to be assessed also by taking into consideration the available technology at the time of the processing and technological developments[125]. Article 29 DPWP emphasized that if data are intended to be stored or processed during a lifetime of 10 years the controller should consider the possibility of identification that may occur also in the ninth year of their lifetime, and which may make them personal data at that moment[126]. For data protection law to apply, it does not matter what the intentions are of the data controller or recipient. As long as the data are identifiable, data protection rules apply.

[The lack] of identifiability serves also as criterion to identify what is fallen under the concept of anomymous / anonymized data. The legislation on data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is

[122] Article 29 DPWP, Opinion 05/2014 on Anonymisation Techniques, p. 10.

[123] It has been suggested that it is clear that as long as a person can be singled out he or she is regarded as identifiable. See M. Mourby, E. Mackey, M. Elliot, H. Gowans, S. E. Wallace, J.Bell, H. Smith, S. Aidinlis, J. Kaye, Are "pseudonymized" data always personal data? Implications of the GDPR for administrative data research in the UK, Computer Law & Security Review 34 (2018), pp. 222–233, 225.

[124] Gola; in: Gola, DS-GVO, Art. 4, Rn. 13.

[125] Recital 26 GDPR adopts a test of reasonable likelihood of identification 'by the controller or by another person', taking into account not the subjective ability to identify, but the state of art of technology at the time of processing.

[126] Article 29 DPWP, Opinion 4/2007, p. 15.

not or no longer identifiable. GDPR does not concern the processing of such anonymous information, including for statistical or research purposes. According to Recital 162 the statistical purpose implies that the result of processing for statistical purposes[127] is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person. If only statistics are output and the rules applied to the set are well chosen, it should not be possible to use the answers to single out an individual[128].

The notion of data processing is also indicatively described[129] but as open-ended conceived as it refers to "any operation or set of operations which is performed on personal data". Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes but it is not limited to the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data. A definition that undoubtedly includes any AI/ machine learning operation performed on personal data. Offering and using applications of AI and cognitive services initiates the applicability of the law, in this case the GDPR[130].

---

[127] [3]Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results.

[128] It is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data.

[129] As processing operation is indicatively mentioned collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4 (2) of GDPR).

[130] Provided that this use is not restricted to personal or household purposes. The "old" wording, namely the reference to "purely personal and household activity", has been the recourse of the European legislator. Recital 18 of the GDPR includes the lack of "connection to a professional or commercial activity" as delimitation element while "social networking and online activity" is explicitly referred as a category of personal/household activity. In parallel, it is clarified that controllers or processors which provide the means for processing personal data for such personal or household

2.2. The scope of application

The provisions of the GDPR (Article 4a) apply to the processing of personal data in the context of the activities of an establishment of a controller in the Union, regardless of whether the processing itself takes place within the Union[131]. The extension of the applicability also to processors constitutes a novelty thus creating a basis for independent obligations pertaining to processors[132]. Regardless of the location of establishment, the GDPR suggests that even non-EU based controllers and processors will be in the future subject to the provisions and requirements of EU law whether they are performing activities related to the offering of goods or services to data subjects in the Union or to the monitoring of the behavior of data subjects insofar as their behaviour takes place within the Union (Recital 24).

Addressees of this provision are foreign controllers and processors that are active on the EU market through online offering of goods and services, irrespective of whether a payment of the data subject is required. Criteria meant to determine whether the controller apparently envisages offering goods or services to data subjects in the Union are "the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language", these factors being indicatively and non-exhaustively mentioned in Recital 23 of the GDPR. In any case, offering of goods and services gives rise to a "(quasi)-automatic establishment of jurisdiction"[133].

---

activities are subject to the provision, an addition that – strictly systematically viewed – was not necessary.

[131]As well as to the processing by a controller or a processor not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

[132] As processors, i.e. a natural or legal person which processes personal data on behalf of controller, are considered also the cloud providers and/or the cognitive services providers with regard to their customers who/which act as data controllers.

[133] See D.J.B Svantensson, The extraterritoriality of EU data privacy law - its theoretical justification and its practical effect on U.S. businesses. Stanford Journal of International Law 50(1) 2013, pp 53-117, 58. Based on this approach we can recognize the influence of the "effects doctrine" upon which conduct on the Internet that has effects within other states may assert their jurisdiction. The effects doctrine has been criticized by various

The criterion of territoriality ("in/within the Union") is still present in the new provisions but there is a shift to the user (data subject) as (the) main point of reference. The monitoring of the behaviour of the data subjects becomes a sufficient ground for the applicability of European law[134]. However, the territoriality requirement has also to be met, as this "behaviour" has to "take place within the Union" to extend the applicability of the law. In this case territoriality corresponds to the physical location of the user, although we can assume that in this context the respective provision is referring to "online behaviour". As far as it concerns "monitoring", the European legislator illuminates this notion by referring to "potential subsequent use of personal data processing techniques which consist of profiling a natural person".

The GDPR does not apply if the data processing is performed by a natural person in the course of a purely personal or household activity. The underlying reason for this exception is that an intrusion of the law into the "private sphere and space", in practice into the daily activities of individuals, would be perceived as unjustified and excessive. The criterion invoked by the European Court of Justice as to the scope of the so-called "household exception" was the extent of accessibility to information processed[135]. Recital 18 of the GDPR includes the lack

authors who underline that in this case jurisdiction becomes open-ended, as in principle all countries have a link to all websites by virtue of their accessibility and since in a globalized economy, everything has an effect on everything. See C. Kuner ,Data Protection Law and International Jurisdiction on the Internet (Part 1) International Journal of Law and Information Technology, Vol. 18 (2010)pp 176-193, 190 and T. Schultz, Carving up the Internet: Jurisdiction, Legal orders, and the Private/Public International Law Interface' European Journal of International Law 19 (4) 2008, pp. 799- 839, 815.

[134] Skouma and Léonard argue that the on-line tracking was one of the key factors that was taken into account in order to decide on the need of legislative reshuffling. See G. Skouma and L. Léonard, On-line behavioral tracking: What may change after the legal reform on personal data protection. In: Gutwirth S et al. (eds.) Reforming European Data Protection Law. Springer Netherlands 2015, pp. 35-60, p. 52.

[135] CJEU, Bodil Lindqvist Case C-101/01, Judgment of 6 November 2003: " [the](household) exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the Internet so that those data are made accessible to an indefinite number of people"(paragraph 47 of the judgment).

of "connection to a professional or commercial activity" as delimitation element while "social networking and online activity" is explicitly referred as a category of personal/household activity.

Individuals that process personal data with the support of AI apps with reference to "purely personal and household activity" are not bound by the GDPR[136]. In parallel, it is clarified (Recital 18) that controllers or processors which provide the means for processing personal data for such personal or household activities are subject to the provision, an addition that – strictly systematically viewed – was not necessary[137].

The applicability of GDPR results in the obligation of data controllers (and processors) to comply with its requirements that relate to a) the legal ground of processing, the (fundamental) data protection principles, c) the respect for the rights of the persons and d) the new instrumentarium for organizing, ensuring and demonstrating compliance (accountability, DPIA, data protection by design). In case of the deployment of AI-based applications a data controller is subject to the data protection principles that set the framework of data processing that responds to the fundamental right of data protection, as embedded in the Charter of Fundamental Rights and Freedoms of EU.

[136] That was the case also under the Data Protection Directive (95/46/EC). Privacy advocates underlined that "maintaining an equally broad exception for personal or household activity in the new Regulation (would) pose an increasing danger for data protection as there will be no legal instrument to defend data protection standards versus natural persons in their online activity". European Digital Rights (EDRi): Position on the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2013) p. 6.

[137] More about L. Mitrou, The General Data Protection Regulation: A law for the Digital Age? in T. Synodinou et al. (Eds), EU Internet Law, Regulation and Enforcement, Springer 2017, pp. 19-57.

3. Lawfulness and Fairness of processing - AI, consent and legitimate interests

Under the first DPA principle, personal data must be "processed fairly, lawfully and in a transparent manner in relation to the data subject" (GDPR: Article 5(1)(a)). Lawful processing requires the processing to be based on one of the legitimate grounds provided in the GDPR. Article 6 (1) of the GDPR, includes, in addition to consent of the data subject, five lawful grounds for processing, i.e. when processing personal data is necessary for the performance of a contract, for the performance of a task carried out in the exercise of public authority, for compliance with a legal obligation, for the purpose of the legitimate interests of the controller or third parties, or if necessary to protect the vital interests of the data subject.

The processing of personal data has to meet one of the conditions set in GDPR (Articles 6, 7 and 9). Consent is one of them, considered to be a substantial, or even indispensable, instrument as it safeguards the participation of the individual regarding his/her decision of the use of his/her data[138].

Consent has to meet the requirements set by the Regulation : Article 4 (11) contains its prerequisites : "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action[139], signifies agreement to the processing of personal data

[138] Also in USA, consent has been for several decades the key principle of information privacy protection.

[139] Such as ticking a box on a website or choosing particular technical settings for "information society services" (services delivered over the internet, eg a social-networking app). Moreover, it is suggested that taking into account the sensors and smart devices in big data, other types of usable and practical user positive actions, which could constitute consent (e.g. gesture, spatial patterns, behavioral patterns, motions), need to be analysed." See G. D' Acquisito, et al. Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. ENISA, December 2015. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-dataprotection

relating to him or her"[140] while Article 7 sets the obligations of the controller when consent serves as legal ground of processing. In the GDPR emphasis is placed also on the way request for consent is presented requiring an intelligible and easily accessible form, using clear and plain language (Article 7 par. 2). In case of a request by electronic means, this has to be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided (Recital 32).

Lawful processing may not rely on implicit consent, such as the installation of the application or pre- ticked boxes. Consenting refers to specific purposes and uses of personal information: in the European approach the fact that individuals post information about them onto social media does not indicate that they legitimize – through implied consent – any secondary, further use[141]. Authors notice that consent is difficult to obtain (or re-obtain) where data is observed rather than directly provided by data subjects, as in this context it is unlikely that data subjects will provide the "clear, affirmative action" required by Article 4(11)[142].

Furthermore, consent, and especially the "digital" one, has been repeatedly and intensively criticized as it is likely to turn into an empty, ritual process, thus resulting in a "fallacy"[143]. Online, notice is to be found by clicking a "privacy policy" link usually placed at the bottom of each page or within app settings. Consent is sometimes signified by clicking an "OK" box in a cookie banner or settings pop-up (express action) or more commonly remaining on the site without leaving or changing settings (omission)[144].

---

[140] In case that a processor processes data on behalf of a data controller, especially with regard to the provision of cloud/ AI services it is the controller who has to obtain the consent from the data subjects.

[141] As noted by ICO, this is particularly an issue if social-media analytics is used to profile individuals, rather than for general sentiment analysis (the study of people's opinions). See ICO, Report, p.90.

[142] M. Butterworth, The ICO and artificial intelligence: The role of fairness in the GDPR framework, p. 261.

[143] See P. Schwartz (2000), p. 341 f.

[144] M. Butterworth, The ICO and artificial intelligence: The role of fairness in the GDPR framework , p. 261

The consent model has also been criticized because of its binary character: a "user" finding herself in a controlled online environment, being offered a restricted, mostly binary choice of options and expecting gains from a rewarding online activity is keen and encouraged to provide consent[145]. New approaches to consent have been proposed to overcome the shortcomings of this binary model: the Information Commissioner has proposed "a process of graduated consent, in which people can give consent or not to different uses of their data throughout their relationship with a service provider, rather than having a simple binary choice at the start", which could or should be related to "just in time notifications"[146]. V. Mayer-Schönberger and Y. Padova propose the shifting from collection-based mechanism to use-based mechanism[147]. However, it remains questionable if the so called "notice and consent" model is suitable or practical in a "big data-AI context".

Given its morally transformative nature (valid) consent requires a clearly defined scope of action, i.e. the consenting individual must have the relevant information so she knows what she consents to[148]. As Johnson states, the use of "opt-in" rather than "opt-out" goes hand in hand with transparency[149]. For consent to be informed, the data subject should be aware, at least, of the identity of the controller, the categories of data to be processed and the purposes of the

[145] See E. Carolan, The continuing problems with online consent under the EU's emerging data protection principles. Computer Law & Security Review 32(3) 2016, pp. 462-473, 472.

[146] See ICO, Big data, artificial intelligence, machine learning and data protection (par. 59,) who mentions as example that users can be asked to give their consent, at the point when an app wants to use mobile phone location data or share data with a third party, p. 30.

[147] See V. Mayer- Schönberger and Y. Padova, Regime change? Enabling big data through Europe's New Data Protection Regulation. Columbia Sci Technol Law Rev 17(2016), p. 315.

[148] Consent plays a morally transformative role in interpersonal interactions, as it (if valid) can render permissible an otherwise impermissible action. See Meg Leta Jones, Ellen Kaufman, and Elizabeth Edenberg, AI and the Ethics of Automating Consent, IEEE Security & Privacy (Volume 16 , Issue: 3 , May/June 2018), pp. 64-72.

[149] See D. Johnson, Computer Ethics, Pearson, Upper Saddle River, NJ 2009, p. 105.

processing for which the personal data are intended. When the processing has multiple purposes, consent should be given for all of them[150].

It remains disputable if this legislative array will ensure that "users would review, rationally assess and deliberatively respond to that information when exercising their consent entitlements"[151] as people are reluctant to read privacy notices[152]. Even if policies and notices satisfy legal obligations, it is highly questionable if consent is adequate as legal ground[153]. Technology and applications are changing steadily and rapidly having a serious impact on the foreseeability of the future uses of data based on consent submitted[154]. The substantial increase in development of processing capabilities (storage, mining, crawling, matching profiles) may entirely transform the context and the conditions under which personal data are processed thus augmenting its

[150] The GDPR provides for an exception with regard to the processing for scientific research purposes as it was accepted that is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. In this case the data subject's consenting statement may refer to areas of specific research (Recital 33).

[151] See E. Carolan, The continuing problems with online consent under the EU's emerging data protection principles. Computer Law & Security Review 32(3) 2016 , pp. 462-473, 468.

[152] The European Data Protection Supervisor questions, whether it would be fair to subject individuals to terms and conditions for online services which would require, on average, 25 days a year to read them. See European Data Protection Supervisor, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of Big Data, 2016, p.13. The ICO suggests that organisations become more innovative in the presentation, wording and format of their privacy notices, explaining that they could be provided in video or cartoon format to encourage people to read them. See par. ICO, par. 143-148.

[153] Barocas and Nissenbaum suggest that even if informed consent were achievable, it would not be effective against contemporary information harms because modern data practices revolve around future and unanticipated uses. See S. Barocas and H. Nissenbaum, Big Data's End Run around Procedural Privacy Protections, Communications of the ACM, vol. 57, no. 11 (2014), pp. 31–33.

[154]See A. Noain-Sánchez, Privacy by default and active informed consent by layers: essential measures to protect ICT users' privacy. Journal of Information, Communication and Ethics in Society 14(2), 2016, pp. 124-138, 134 f.

informative value in an unpredictable way and increasing the potential adverse effects for individuals' rights [155].

However big data processing based on AI/machine learning results often to the repurposing of data. The adequacy of information provided and subsequently the consciousness of choice is questioned also by the capability and tendency of AI analysis to identify new correlations[156] between data and (re)group it or to create new types and categories of data[157] and sometimes without the foresight of the data controller[158]. The data subject's informed consent becomes more unrealistic and less meaningful also due to the mutable character of data processed and the unpredictability of processing outcomes[159]. The complexity and the transformative use of Big Data does not offer to data subjects a real chance to understand potential future uses so as to make a conscious choice. As expressed by the European Data Protection Supervisor, "we may not have the

[155] See L. Mitrou, The General Data Protection Regulation: A law for the Digital Age? in T. Synodinou et al. (Eds), EU Internet Law, Regulation and Enforcement, Springer 2017, pp. 19-57.

[156] As emphasized by Mantelero, "since Big Data analytics are designed to extract hidden or unpredictable inferences and correlations from datasets, the description of these purposes is becoming more and more evanescent". Mantelero A. (2014) The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics, Computer Law & Security Review Volume 30, Issue 6 (2014), pp. 643-660, 652.

[157] Given the tendency of big data analytics and artificial intelligence to create new types of data, these new forms of enhanced analytics challenge the ability to draw a distinction between "special" and other categories. Zarsky notices that Big Data potentially undermines the entire distinction between these categories. See T. Z. Zarsky, Incompatible: the GDPR in the age of big data. Seton Hall Law Rev 2017;47(2): Available from: https://ssrn.com/ abstract=3022646.

[158] Butterworth states as example that the artificial intelligence may not process the special category of data itself, it may inadvertently create a profile based on secondary data (for example post code, social media data and shopping habits) of which all the individuals matched by the profile are of the same race or share another special category of data, p. 262.

[159] The suggested "popular solution to the problems of obtaining consent in digital environments to use AI to predict what information practices a user would consent to and have such preferences signaled to smart systems attempting to collect or use data about the user", mentioned by Meg Leta Jones, Ellen Kaufman, and Elizabeth Edenberg, raises new issues. See AI and the Ethics of Automating Consent, IEEE Security & Privacy (Volume 16 , Issue: 3 , May/June 2018), pp. 64-72.

appropriate information about how our personal data is used and importantly, how decisions concerning us are taken, therefore making it impossible to meaningfully consent to the use (processing) of our data''[160].

A further challenge refers to the impact of withdrawal of consent. The right to withdraw consent reflects and guarantees the right of the individual to informational self-determination and data controllers need to build in the technical capability to fulfil data subjects' requests to withdraw consent. However, withdrawal of consent and, respectively, the withdrawal / erasure of data[161] may pose a threat to the development of AI because it could limit the amount of data available to learn from. The AI system could no longer use these specific data references to develop its algorithms. Therefore, it has to ensured that the dataset has not been skewed or undermined because of a withdrawal of certain data, which constitutes a major problem for organisations with smaller datasets (e.g. start-up services) as the proportional effect of any individual with drawing consent to use of their data would be higher [162]. Humerick indicates this risk as AI continues to learn from past data and raises the question how to simultaneously stop AI's learning from this data, without impacting its prior development[163]. The solutions proposed are of technical nature taking the form of isolation or deletion of the strand of learning, which incorporated the now nonconsensual data or retraining of existing the AI models using the modified data sets.

[160] Buttarelli G, (2016) A smart approach: counteract the bias in artificial intelligence. https://edps.europa.eu/press-publications/press-news/ blog/smart-approach-counteract-bias-artificial-intelligence_en.

[161] As a consequence of the lack of legal basis and/or of the exercise of the right to erasure as laid down in the GDPR (Article 17 par. 1 b).

[162] Butterworth, p. 262. This is a quite high risk in combination with the concern that this situation may result into continual liability risks.

[163] M. Humerick, Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, 34 Santa Clara High Tech. L.J.393 (2018). Available at: https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3

A part of legal theory rejects the notice and consent model as they believe that such a response does not face the challenges of the techno-economic environment[164]. While pointing to the cognitive limitations of data subjects and the complexity of data processing (both in terms of actors involved and the operations they perform) that decrease individuals informed assessment and increase rational choice fallacies, critics of notice and choice approach underline the information power asymmetries, which cannot longer be counterbalanced by the user's self-determination[165]. On the other side other authors think that "preserving the consent-based principle is still the last stronghold to preserve decisional privacy"[166].

Because of the doubts over the validity of consent to data processing and the difficulties associated with consent in a big data/AI context, organisations are likely to also wish to develop a justification under the legitimate interests basis for processing. The GDPR provides this legal basis under the condition that these legitimate interests (of the data controller or a third person) are [not] overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Both the wording and the interpretation of the provision of Article 6 par. 1 (f) and the accountability principle embedded in the GDPR (Article 5 par. 2) requires greater responsibility on the controller to carry out an inherent balancing test of its legitimate interests against those of the data subject. The processing must be necessary for the legitimate interests to be pursued, "which means that it must be more than just potentially interesting. The processing is not necessary if there is another way of meeting the legitimate

[164] As stated in CoE Consultative Committee Report on AI "long and technical data processing notices, social and technical lock-ins, obscure interface design, and a lack of awareness on the part of the data subject are some of the reasons for [the] weakness [of data subjects' consent in terms of self-determination", p. 9.

[165] See A. Mantelero , The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. Computer Law & Security Review 30(6) (2014), pp. 643-660, 652.

[166] So Kaori Ishii, Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects, AI & Soc (published online 31 August 2017).

interest that interferes less with people's privacy"[167]. Using legitimate interests as justification requires "an assessment of what is fair in the circumstances"[168].

4. AI, Fairness and Discrimination

Fairness is a key requirement and issue for persons and organisations using personal data in the context of AI applications. Fairness is quite difficult to define but it involves - much - more as compliance with data protection legal requirements and "it governs primarily the relationship between the controller and the data subject"[169]. The definition and principle of fairness refers not so much to rights of data subjects as to obligations of data controllers towards them.

In relation to AI applications and services, the features of data processing systems must make it possible for data subjects to really understand what is happening with their data, regardless of the legal ground of processing. In any case, the principle of fairness goes beyond transparency obligations [170]. It could be linked to processing of personal data in an ethical manner and involve the requirement of values-sensible design/ responsible (research and)innovation. How applications are designed and how personal data is used is an important factor in assessing fairness[171] . As mentioned in Council of Europe Report on AI, potential bias may relate to the methods (e.g. measurement bias, bias affecting

[167] ICO, para 67.

[168] M. Butterworth, The ICO and artificial intelligence: The role of fairness in the GDPR framework, p. 263.

[169] Fundamental Rights Agency, Handbook on European data protection law, Edition 2018, p. 118.

[170] Hijmans and Raab are not sure if transparency is an element of fairness or a separate requirement. See H. Hijmans and C. Raab Ethical Dimensions of the GDPR,in: M. Cole and F. Boehm (eds.) Commentary on the General Data Protection Regulation Cheltenham: Edward Elgar (2018).

[171] ICO, Big data, artificial intelligence, machine learning and data protection, p.38

survey methodologies), the object of their investigation (e.g. social bias due to historical bias or underrepresentation of some categories), their data sources (e.g. selection bias) or the person responsible for the analysis (e.g. confirmation bias)[172].

A – as primary as important – requirement deriving from the fairness principle refers to the need that organizations deploying AI applications are aware of the effects and implications that this deployment may have on individuals and their rights and freedoms but also on communities and societal groups[173]. With regard to fairness, scholars/ authors point to the significance of fairness when designing and deploying machine learning processes: Machine learning processes may be made "biased" so as to produce the results pursued by their designer [174]. CNIL rightly points out that " all algorithms are biased in a sense, insofar as they are always the reflection – through their configuration and operating criteria, or through their training input data – of a set of societal choices and values".

Problems result from discrimination risks[175]. Unfairness can arise already with the choice of training data. By introducing a direct or indirect bias into the process, the quantity and quality of data used to train the algorithm, including the reliability of their sources and labelling may have a significant impact on the construction of profiles, face recognition or detection of emotions. Bias may be introduced into machine learning processes at various stages, including algorithm

[172] Council of Europe Consultative Committee, Report on Artificial Intelligence, September 2018, p. 11.

[173] It is noteworthy that some authors have raised the issue of collective privacy especially with regard to the impact of profiling on societal groups. See A. Mantelero, Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, Computer Law & Security Review 32 (2016), pp. 238–255.

[174] D. Kamarinou, C. Millard, and J. Singh, Machine Learning with Personal Data, p. 16.

[175] CNIL, COMMENT PERMETTRE À L'HOMME DE GARDER LA MAIN ?- Les enjeux éthiques des algorithmes et de l'intelligence artificielle, 2017, p. 31.

design and selection of training data, which may embed existing prejudices into automated decision-making processes [176].

Beyond the "representativeness" of data[177], fairness concerns are raised with reference to bias that may lead to inaccurate or – mostly – discriminating outcomes. If the example of Google's face recognition algorithm that identified black people as gorillas is quite extreme and shocking[178], the example of underrepresentation of a minority group in historic data that may reinforce discrimination against that group in future hiring processes or credit-scoring, illustrates the effects that a machine learning process may produce[179].

Machine learning models can build in discrimination through choices in how models are constructed. Of particular concern are choices about which data models should consider, a problem computer scientist call "feature selection". A direct bias in this case might be to direct the algorithm to develop a model that filters people by race, gender, or religion where there is no justification for doing so[180]. Discrimination might be based on choice of data to be used might not be

[176] C. Kuner, D.P. Svantesson, F.H. Cate, O. Lynskey, and C. Millard, Machine learning with personal data: is data protection law smart enough to meet the challenge? International Data Privacy Law, 2017, Vol. 7, No. 1, p.1.

[177] The example stated by the Authors of the Future Computed is noteworthy: when an AI system, designed to help employers screen job applicants, is trained on data from public employment records, this system might "learn" that most software developers are male. As a result, it may favor men over women when selecting candidates for software developer positions. See Microsoft, The Future Computed, p. 59.

[178] See Barr, Google Mistakenly Tags Black People as 'Gorillas,' Showing Limits of Algorithms, Wall Street Journal (July 1, 2015). The Fundamental Rights Agency (FRA) mentions another "real-life example" to indicate the possibly discriminating effect of an automated description of images training. Namely, a baby with white skin colour was described as a "baby", but a baby with a black skin colour was described as a "black baby". The FRA adds that this is biased data because it assigned additional attributes only to a certain group, while objectively either both cases should be described including the colour or none of them.

[179] See Kuner, D.P. Svantesson, F.H. Cate, O. Lynskey, and C. Millard, Machine learning with personal data: is data protection law smart enough to meet the challenge? International Data Privacy Law, 2017, Vol. 7, No. 1, p.1.

[180] See J. A. Kroll, J. Huey, S. Barocas, E. W. Felten, J. R. Reidenberg, D. G. Robinson & H. Yu, Accountable Algorithms, 165 UNIV. OF PENN. L. REV (2017), pp. 633-705, 685.

neutral. If the data used for building an algorithm are biased against a group (i.e. systematic differences due to the way the data are collected or prepared), the algorithm will replicate the human bias in selecting them and learn to discriminate against this group. Data can be biased for several reasons, including the subjective choices made when selecting, collecting and preparing data.

Models based on training data that render a biased picture reality or they aren't relevant to the area in question contravene the fairness principle[181]. Data that embed past prejudices may lead to unreliable conclusion thus resulting into perpetuation of these prejudices: in a hiring application, if fewer women have been hired previously, data about female employees might be less reliable than data about male employees[182].

Bias may exist in the criteria or technical policy that the designer instructs the algorithm to follow when answering a specific question or reaching a specific goal. It seems that the crucial, even if difficult, task is asking and formulating the right questions and assess the appropriateness of outcomes[183]. Identifying and controlling for such biases is a critical challenge in designing and evaluating the fairness of AI/machine learning processes. If artificial intelligence is supposed to perform more objective analyses[184] , such a system could be " unfair if people do not understand the limitations of the system, especially if they assume technical systems are more accurate and precise than people, and therefore more

---

[181] Datatilsylnet, Artificial intelligence and privacy , (2018), p.16.

[182] Kroll et al, p. 681. Hacker mentions also the example of COMPAS algorithm , a software increasingly used by US courts to predict the future behavior of criminal defendants (more precisely: their recidivism likelihood), which in turn influences sentencing decisions.. However, COMPAS has been shown to discriminate against black offenders. See Philipp Hacker, Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law with reference to Larson et al., "How We Analyzed the COMPAS Recidivism Algorithm", Pro Publica (May 23, 2016), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

[183] D. Kamarinou, C. Millard, and J. Singh, Machine Learning with Personal Data, p. 17.

[184] "…. not be affected by low blood sugar, by having a bad day, or by the desire to help a friend" See Datatilsylnet, p. 16.

authoritative"[185]. The Fundamental Rights Agency points to the danger that machine-learning procedure and its results are regarded as objective, without taking into account the potential problems in the underlying data[186].

Embedding into the algorithm fundamental values is not only an imperative related to ethics and responsible or values-sensible design. The GDPR requires the data controller to prevent "inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect" (Recital 71). Moreover, the European legislators point to the need "to use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized".

5. AI and the Data Processing /Protection Principles

5.1. The purpose limitation principle

The principle of purpose limitation is one of the fundamental principles of European data protection law, embedded also in Article 8 of the Charter of Fundamental Rights and Freedoms of the European Union. Article 5(1)(b) of the GDPR requires that data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, which means that any processing of personal data must be done for a specific, well-defined purpose and only for additional purposes that are compatible with the original purpose.

[185] See Microsoft, The Future Computed, p. 59.

[186] European Union Agency for Fundamental Rights, European Union Agency for Fundamental Rights, #BigData: Discrimination in data-supported decision making, 2018, p. 5.

The purpose of processing must be established and indicated at the phase of collection so that the data subjects are able to exercise control over their data. The clear delineation of the purpose is important not only to enable data subjects to effectively exercise their rights but also to define the overall compliance with the law and its assessment. Complying with the purpose limitation principle prohibits the use of recorded voices by Siri, Alexa and similar for analyzing this voices and extract biometric findings and Fitness-Trackers is not allowed to serve as pharmacy-shops[187]. In this perspective the purpose limitation principle is inseparately connected with transparency, predictability and fairness.

The purpose limitation principle seems to be at odds with AI processing capabilities: the use of algorithms and the usefulness of machine learning is grounded on and fueled by the tendency to collect as much data as possible and the generation of new data and new types of data. The re-purposing of use figures as a main feature of AI applications in their combination of big data: big data analytics involves repurposing data in unexpected ways, using complex algorithms, and drawing conclusions about individuals with unexpected and sometimes unwelcome effects[188].

Some suggest that the purpose limitation principle restricts an organisation's freedom to make these discoveries and innovations. In the opinion of the ICO, the purpose limitation principle prohibits arbitrary re-use, but it need not be an insuperable barrier to extracting the value from data thus permitting under certain circumstances organisations to re-purpose and extract enhanced value from their datasets[189].

The purpose limitation principle prevents arbitrary re-use but in this context the key question refers to what is perceived as compatibility and how to

[187] See S. Conrad, Künstliche Intelligenz – Die Risiken für den Datenschutz, Datenschutz und Datensicherheit 12/2017,p.743.

[188] ICO, par. 30.

[189] M. Butterworth, The ICO and artificial intelligence: The role of fairness in the GDPR framework, p. 260.

assess and demonstrate it, following the accountability requirement: According to Recital 50 the following factors have to be considered when ascertaining the compatibility of the further processing: any connection between the original purpose and the purposes of the intended further processing, the context in which the data was collected, the data subject's relation to the controller and how this may affect the subject's reasonable expectations with regard to further processing, the nature of the personal data , the consequences for the data subject of the intended further processing , whether the original processing operations and the new ones are subject to the appropriate safeguards. If the further processing is not considered to be compatible with the original one, a new legal ground (such as a distinct, new consent) has to be sought.

On the contrary the purpose limitation principle does not prevent re-use of personal data for scientific and/ or statistical purposes[190]. Scientific research is to be conceived broadly to include technological development and demonstration, basic research as well as applied and privately funded research (Recital 159). The use of personal data for scientific research is subject to the specific provisions of Article 89 of GDPR and to the appropriate safeguards provided, including ensuring the data subject's rights and taking technical and organizational security measures. With regard to scientific research in relation to AI we have to note that it is difficult to establish a distinction between (scientific) development and application of AI. The Norwegian DPA considers to be difficult to make such a differentiation, as AI models develop and improve continuously as they are fed with more (personal) data, and hence to distinguish "where research stops and usage begins" [191].

[190] For the impact of GDPR on scientific research see E.J. Kindt, Why research may no longer be the same, Computer Law & Security Review 32 (2016), pp 729–748.

[191] Datatilsylnet, p. 18.

5.2. AI, Proportionality and Data Minimization Principle

The Directive 95/46/EC had embedded the proportionality as one of the main principles regulating the lawful use of personal data and as element of balance between the rights and interests of the data controller and the data subject. An example of innovation pursued through the adoption of GDPR is a stronger emphasis on proportionality expressed through the so called "data minimization" (Article 5 par 1 c)[192]. Data minimization is for many the major notion underlying data protection law, being a combination of the traditional principles of collection limitation, data quality (requiring data to be relevant), purpose specification, and use limitation[193].

In this respect, processing must be limited to what is necessary to fulfil a legitimate purpose. Moreover: Data processing may not disproportionately interfere with the interests, rights and freedoms at stake. The categories and the volume of data chosen for processing must be necessary in order to achieve the declared overall aim of the processing operations. There must be a fair balance between all interests concerned at all stages of the processing. This means that "[p]ersonal data which is adequate and relevant but would entail a disproportionate interference in the fundamental rights and freedoms at stake should be considered as excessive".

The short version of this principle as expressed by the former European Data Protection Supervisor ("the best protection is to process as few data as possible")[194] seems to be in contradiction with the "needs" of machine learning.

---

[192] Also Article 5 (1) of Modernised Convention 108 (May 2018) contains a proportionality requirement for processing personal data in relation to the legitimate purpose pursued.

[193] Bert-Jaap Koops, The trouble with European data protection law, International Data Privacy Law, 2014, Vol. 4, No. 4 , pp. 250-261, 256.

[194] See Peter Hustinx (former European Data Protection Supervisor), EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation .

The principle of data minimisation is – almost by definition - opposed to Big data analytics and machine learning systems that are based, if not dependent on an excessive data collection and the possibility to re-combine and re-use them. As mentioned by ICO, regarding data minimisation is not simply the amount of data being used, but whether it is necessary for the purposes of the processing, or excessive. The data minimization principle states that personal data may not be collected, processed and retained "in reserve"[195]. As noted by M. Butterworth, if the processing satisfies the purpose limitation principle then it will also satisfy the data minimisation principle[196]. This is not a hypothetical problem: in a study of businesses in the UK, France and Germany, 72% said they had gathered data they did not subsequently use[197].

The challenge for data controllers is to define from the outset: a) the purposes of the processing, a challenge not at all easy to respond to, as it is not normally possible to predict what the algorithm will learn and b) the data that will be relevant, thus limiting the amount of data included in training or in the use of a model[198] . In this perspective the data minimization principle relates both to the volume of data and the processing activity. Complying with the data minimization principle may restrict the extent of the intervention in an individual's (informational) privacy or even lead to abstaining from the use of AI models/ methods if the objective of processing can be achieved in a less invasive for the individuals' privacy way. The compliance with data minimisation principle forms part of good governance processes thus helping to improve data quality and – consequently – assisting the analytics[199] .

---

[195] See P. Scholz in S. Simitis, Bundesdatenschutzgesetz-Kommentar (2014), p. 421 f. This approach is shared also by the ICO who argues that "acquiring and keeping data just in case it may be useful" does not help to improve data quality . See ICO, par. 91.

[196] See M. Butterworth, The ICO and artificial intelligence: The role of fairness in the GDPR framework, p. 260.

[197] ICO, Big data, artificial intelligence, machine learning and data protection, par. 85.

[198] Datatilsylnet, p.18. The Norwegian Authority pointed out that "it would be natural to start with a restricted amount of training data, and then monitor the model's accuracy as it is fed with new data".

[199] See ICO, par. 91

Another principle, deriving from the imperative of proportionality while processing personal data is that of "storage limitation": data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (Article 5 par.1 e). Exception is provided only for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes under the condition of implementing the appropriate technical and organisational measures required by the Regulation (in Article 89) in order to safeguard the rights and freedoms of the data subject[200].

5.3. AI and the Accuracy Principle

The quality of data is particularly important in the age of Big Data as data is often collected and generated without any quality control[201]. According to Article 5 par. 1 c personal data have to be accurate and, where necessary, kept up to date. The obligation to ensure accuracy of data must be seen in the context of the purpose and the nature/ category of data processing.

Lack of quality may arise as a result of implications regarding the accuracy of personal data itself at all stages of collection, analysis and application. However even personal data is accurate, it doesn't ensures the accuracy of analysis due to

[200] Humerick points to the implications that the erasure of data may have for AI and suggests that "rather than requiring a complete erasure of personal data, controllers and processors should be able to retain information up to the point of erasure. In this way, the AI's machine learning would remain at the point where it progressed, rather than creating forced amnesia" . According to Humerick this would balance the balance the interests of deleting the individual's PII without causing the AI to regress. See M. Humerick, Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, 34 Santa Clara High Tech. L.J.393 (2018). Available at: https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3

[201] See European Union Agency for Fundamental Rights, #BigData: Discrimination in data-supported decision making, 2018, p. 5.

possible "unrepresentativeness "of data and/or biases in datasets and models that may lead to inaccurate predictions.

As accuracy is both a quality principle[202] and a means to protect data subjects form potential damages which might be caused if data were to remain inaccurate, it is questionable if "big data analytics can tolerate a certain amount of "messy" (i.e. inaccurate) data, because the volumes of data being processed are generally so large"[203] . In any case "messiness" cannot be tolerated if it may affect data subjects when the result of analytics is used to profile individuals leading to incorrect outcomes and hence predictions with regard to performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Issues of accuracy may result due to misinterpreting the meaning and implications of AI results[204]. Inaccurate predictions may be the outcome of confusing correlation and causation. As explained by Hildebrandt, the correlations identified by the algorithms point to some type of relation between different data but without necessarily providing an explanation as to what that relation is, nor whether there is a causal link between the data[205]. Inaccuracy may arise also due to a specific type of bias, the unequal ground truth, which is the case if capacities

[202] As noted by the ICO also a good practice in terms of information management. See ICO, par. 92.

[203] As suggested by V. Mayer-Schönberger and K. Cukier, Big data. A revolution that will transform how we live, work and think. John Murray, 2013, pp. 32 ff.

[204] For example, if the bank extends credit every time to people with the 70 percent "risk of default," 70 percent of those people will, in fact, default. Such a system may be unfair in application, however, if loan officers incorrectly interpret "70 percent risk of default" to simply mean "bad credit risk" and decline to extend credit to everyone with that score — even though nearly a third of those applicants are predicted to be a good credit risk. See Microsoft, The Future Computed, p. 59.

[205] So M. Hildebrandt, Defining Profiling: A New Type of Knowledge? in M. Hildebrandt and S. Gutwirth (eds.), Profiling the European Citizen (Springer Netherlands, 2008), p. 18. With this regard Kamarinou et al. mention a telling example: it may be predicted that a female candidate may be less likely to be suitable for a CEO position but the cause for this may be that fewer women than men have had the opportunity to reach that executive level. See D. Kamarinou, C. Millard, and J. Singh, Machine Learning with Personal Data, p. 17.

or risks are unevenly distributed between protected groups, resulting in the so called "statistical discrimination"[206].

The accuracy principle requires that data controllers that perform machine learning processes need to ensure that the training data is representative of the environment in which the trained algorithm will be deployed and that it does not incorporate existing real-world bias.[207]. It is interesting to note that the training data can be assessed for bias, incompleteness or taking irrelevant factors into account, but it cannot be assessed for accuracy with respect to the data subject because the event it is predicting does not relate yet to a particular data subject[208].

6. AI and Transparency

Individuals are often not aware of the use of personal data for processing. Collection of mobile phone location and processing of data consisting in filtering of search results may not be apparent to the average user. Similarly, we record a lack of awareness with regard to the process and flow of decision making, such as the use of social media data for credit scoring[209].

AI/machine learning applications that lead to discriminatory predictions and decision making not only impede individuals' fundamental rights but they may also undermine the trust on fairness and lawfulness of the respective decisions. A lack of trust influences people's perceptions and becomes a barrier to data sharing

[206] See P. Hacker, Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law, SSRN-id3164973.pdf

[207] ICO, para 97.

[208] See M. Butterworth, p. 261.

[209] See ICO,.para 51. The ICO is referring to the so called filter bubble" effect with reference to E. Pariser, Beware online "filter bubbles". TED Talk, March 2011. http://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles/transcript?language =en

thus affecting social[210] and economic interests. (Informed) trust[211] is grounded on openness and accessibility in decision making and actions, while helping to ensure and demonstrate respect for data subjects and their rights.

The major challenge, i.e. how to safeguard the right to informational self-determination and prevent harms to individuals caused by algorithmic activities and algorithm-driven outcomes, raises the issue of "traceability' of these outcomes, which in its turn poses the question how to ensure transparency. In a broader perspective, transparency is articulated as a need to face the "opacity of the algorithm". As underlined by the CNIL, "algorithms are not only opaque to their end users …., the designers themselves are also steadily losing the ability to understand the logic behind the results produced"[212].

The ability to look inside the "black box"[213] of machine learning algorithms, in the obscure rationale of algorithm classifying new inputs or predicting unknown correlations and variables[214], has provoked a significant debate between industry, data protection advocates, academics and policy-makers. Primarily, the transparency requirement is addressed both to technology producers and data controllers. The firsts have to respond to this incentive and

[210] A study into public attitudes to the use of data in the UK emphasizes the low level of understanding and awareness of how anonymised health and medical data is used and of the role of companies in medical research. Ipsos MORI Social Research Institute. The one-way mirror: public attitudes to commercial access to health data. Ipsos MORI, March 2016.
http://www.wellcome.ac.uk/stellent/groups/corporatesite/@msh_grants/documents/web_document/wtp060244.pdf

[211] So the recommendation of P. Evans and P. Forth, Borges' map: navigating a world of digital disruption. Boston Consulting Group, 2 April 2015. https://www.bcgperspectives.com/content/articles/borges-map-navigating-world-digitaldisruption/

[212] CNIL, COMMENT PERMETTRE À L'HOMME DE GARDER LA MAIN ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, p. 51.

[213] See F. Pasquale, The black box society: the secret algorithm behind , money and information. Harvard University Press, Massachusetts, 2015, pp. 320.

[214] See B.D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, L. Floridi, The ethics of algorithms: mapping the debate. Big Data Soc July– December 1–21 2016, p. 6.

improve technology to face opacity, while the seconds should give data subjects notice about how information about them is processed[215].

Above all transparency constitutes a substantial founding principle of data protection strictly interrelated with fairness[216]. Unless individuals are provided with appropriate information and control, they "will be subject to decisions that they do not understand and have no control over"[217]. A normative view on algorithmic transparency implies that such systems may only be used if their underlying reasoning can be (adequately) explained to users[218].

Transparency refers to the obligation for the controller to take any appropriate measure in order to keep the data subjects – who may be users, customers or clients – informed about how their data are being used. Controllers should notify data subjects and the general public that they will process data in a lawful and transparent manner. Processing operations must not be performed in secret and data subjects should be aware of potential risks. Furthermore, controllers, so far as possible, must act in a way which promptly complies with the expectations of the data subject concerning the respect of her rights, especially when the consent forms the legal ground of processing. Especially when the processing is not grounded on the (informed) consent of the data subject transparency and openness are becoming especially compelling.

Individuals have the right to know how and which personal data is collected, used or otherwise processed, as well as to be made aware of the risks,

---

[215] See Zarsky, T. Transparent Predictions. University of Illinois Law Review 4 (2013), p. 1503.

[216] CNIL, COMMENT PERMETTRE À L'HOMME DE GARDER LA MAIN ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle. According to CNIL transparency is a condition for fairness. Also see ICO who considers transparency as a key element of fairness, par. 54.

[217] 38th International Conference of Data Protection and Privacy Commissioners, Artificial intelligence, Robotics , Privacy and Data Protection, October 2016, p. 4.

[218] See M. Eiband, H.Schneider, D. Buschek, Normative vs Pragmatic: Two Perspectives on the Design of Explanations in Intelligent Systems, ExSS '18, March 11, Tokyo, Japan., p. 1.

safeguards and their rights regarding processing. Article 13 and Article 14 of the GDPR deal with the right of data subjects to be informed, either in situations, where personal data were collected directly from them, or in situations where the data were not obtained from them, respectively. The GDPR obliges data controllers to inform data subjects subjects (at the time of data collection) about the key elements of processing[219]. The data controller is especially required [Articles 13(2)(f) and 14(2)(g)] to inform data regarding the "existence of automated decision-making" and to provide "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing...".

What is understood under "meaningful information" about "logic" must be evaluated from the perspective of the data subject. The primary components of transparency are accessibility and comprehensibility of information. The Norwegian DPA emphasizes how challenging is it to satisfy the transparency requirement in the development and use of AI because of the difficulty "to understand and explain" "how information is correlated and weighted in a specific process"[220]. The CNIL points out the recommendation of specialists to give

[219] This information should include the controller's identity and contact details, including the DPO's details, if any; the purpose and legal basis for the processing, i.e. a contract or legal obligation; the data controller's legitimate interest, if this provides the basis for processing; the personal data's eventual recipients or categories of recipients; whether the data will be transferred to a third country or international organisation, and whether this is based on an adequacy decision or relies upon appropriate safeguards; the period for which the personal data will be stored, and if establishing that period is not possible, the criteria used to determine the data storage period; the data subjects' rights regarding processing, such as the rights of access, rectification, erasure, and to restrict or object to processing; whether the provision of personal data is required by law or a contract, whether the data subject is obliged to provide his or her personal data, as well as the consequences in case of failure to provide the personal data; the existence of automated decision-making, including profiling; the right to lodge a complaint with a supervisory authority; the existence of the right to withdraw consent. In cases where the personal data is not obtained from the data subject directly, the data controller must notify the individual about the origin of the personal data. It is noteworthy to point out that the Council of Europe Report on artificial intelligence states that although transparency is important to have a public scrutiny of automated decision-making models, a generic statement on the use of AI does little to tackle the risk of unfair or illegitimate data use (p. 15).

[220] Datatilsylnet, p.19

precedence to algorithm explicability or intelligibility over transparency: " What would seem to matter …. is the capacity to understand the general logic underpinning the way the algorithm works. It should be possible for everyone to understand this logic, which must therefore be explained in words rather than in lines of code" [221]. A high-level, non-technical, description of the decision-making process is more likely to be meaningful[222].

The information must be easily available and formulated in a clear and comprehensible language (Article 12 GDPR) thus enabling the individuals to exercise their rights anchored in GDPR. From a data subject's perspective, any meaningful information about the logic involved in automated decision-making, including profiling, and the envisaged consequences of such processing may depend on the right to access relevant personal data, including metadata[223].

Legal and procedural responses are necessary to create some necessary conditions for transparency, but technical ones are also needed. In this context, we should not ignore the legal and technical barriers set to algorithmic transparency. Transparency about models and processes may infringe intellectual property rights and trade secrets that may restrict the extent of information to be provided[224]. State secrets and pursue of public interests may

[221] CNIL, COMMENT PERMETTRE À L'HOMME DE GARDER LA MAIN ?, p. 51.

[222] See C. Kuner, D. J. B. Svantesson, F. Cate, O. Lynskey and C.Millard, Machine learning with personal data: is data protection law smart enough to meet the challenge? International Data Privacy Law, 2017, Vol. 7, No. 1, p. 2.

[223] See N. Diakopoulos, Accountability in Algorithmic Decision Making, (2016) Communications of the ACM 59 (2), pp. 57-62, 60.

[224] The Norwegian Datatilsylnet states however that "consideration of others' rights, such as the commercial secrets of an organisation, may nevertheless not be used to deny a data subject access to all data relating to her. The answer is to find a pragmatic solution. In most cases, furnishing the data subject with the information she needs to protect her interests, without at the same time disclosing trade secrets, will not be problematical" (p. 19).

present another legal ground for restricting to right to information as they cannot be revealed to the public[225].

An - intrinsic - difficulty in providing information for an artificial intelligence algorithm and its uses lies in the logic behind the machine reasoning that may not be expressible in human terms. Another technical limitation results from design processes that involve some element of randomness produce unpredictable results that are not reproductive by design[226]. Furthermore, we have to take into consideration the dynamic nature of algorithms, which are continuously updated and changed. Authors point to the case of neural networks arguing that where machine learning technology's decision-making element comprises such a network or similar technology, it will be difficult and perhaps impossible to provide any explanation at all[227]. One the other side it is suggested that the claim that explanations of how AI functions and how it has arrived at decisions are not possible must be rejected, as there is already vivid research on interpretability of AI[228].

---

[225] "Were the public to know exactly what items on a tax return are treated as telltale signs of fraud or tax evasion, tax cheats may adjust their behavior, causing these indicators to potentially lose their predictive value for the tax authorities." See Kaori Ishii, p… M. Brkan, states the example of police authority not willing to disclose the rule behind the choice of neighbourhood or persons to monitor, for example for the purposes of prevention of terrorism or drug trafficking. See M. Brkan Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond, (Paper submitted in view of presentation at the conference 'Terminator or the Jetsons? The Economics and Policy Implications of Artificial Intelligence', Technology Policy Institute, Washington 22 February 2018.). Veale et al note that in some cases transparency may prevent public bodies from carrying out their duties (e.g. predictive policing systems), or conflict with the data controller's security obligations concerning the personal data of data subjects other than those requesting access. See M. Veale, B. Reuben and L. Edwards, Algorithms That Remember: Model Inversion Attacks and Data Protection Law, Philosophical Transactions of the Royal Society, 2018.

[226] See Kaori Ishii, Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects.

[227] See C. Reed, How Should We Regulate Artificial Intelligence? Philos Trans A Math Phys Eng Sci. 2018 Sep 13;376(2128). doi: 10.1098/rsta.2017.0360.

[228] See P. Niemitz, Constitutional Democracy and Technology in the age of Artificial Intelligence, Accepted for publication in Royal Society Philosophical Transactions A 2018 DOI 10.1098/RSTA.2018.0089. About interpretability see M. Miron, Joint Research Center of the European Commission "Interpretability in AI and its relation to fairness,

Dealing with the pragmatic aspect of transparency some authors wonder if the mere option to obtain an explanation about a system's workings may be regarded as more important than the actual design of this explanation and suggest that the option itself strengthens the trust in a system. In this case information should be available to users and reflect the underlying algorithmic processing in detail and as comprehensively as possible[229].

These potential restrictions do not supersede the considerably growing demand "for how and where an algorithm is responsible for profiling or decision-making, both in public and private sectors"[230]. Transparency presents an element of accountability and controllability of processing[231]. It enables responsibility for decision-making failures or biased predictions to be traced and assigned appropriately: "[to] assess whether there should be negligence liability for an AI-based decision, the courts need to be told how the AI made its decision"[232]. According to the remarks of CNIL, " the principle of transparency is associated with the performance of the platform so that we can assess the compliance with what is promised with regard to the offering of this service"[233] .

---

transparency, reliability and trust" 9.4.2008, at https://ec.europa.eu/jrc/communities/community/humaint/article/interpretability-ai-and-its-relation-fairnesstransparency-reliability-and

[229] See M. Eiband, H. Schneider, D. Buschek, Normative vs Pragmatic: Two Perspectives on the Design of Explanations in Intelligent Systems, ExSS '18, March 11, Tokyo, Japan.

[230] See N. Diakopoulos (2016). "Accountability in Algorithmic Decision Making." Communications of the ACM 59 (2), pp. 56–62.

[231] As noted by the House of Commons algorithms have to be transparent to allow the investigation of a wrong decision made be an AI system. House of Commons, Science and Technology Committee (2016) Robotics and artificial intelligence: fifth report of session 2016–17. https://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/145.pdf

[232] So C. Reed, who notes that requiring transparency about the workings of AI might be a suitable interim solution to some of the legal problems, and has already been recommended as a tool for regulation. See C. Reed, How Should We Regulate Artificial Intelligence ?

[233] CNIL, COMMENT PERMETTRE À L'HOMME DE GARDER LA MAIN ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, p. 51

7. Accountability and Risk Assessment

The European legislators have enriched the instruments of informational privacy by adding not only "transparency" but also "accountability" to the list of the data protection principles. One of the most important elements of the Regulation is the shift from notification system and nominal responsibility to accountability for controllers[234].

Article 5 par. 2 states that the controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 ("accountability"). In broad terms, a principle of accountability would place upon data controllers the burden of implementing within their organizations specific measures in order to ensure that data protection requirements are met. Such measures could include the implementation of data protection impact assessments or employing a privacy-by-design system architecture. Accountability is further emphasised by several provisions throughout the GDPR that promote it such as Article 24 of the GDPR that requires organisations to implement "appropriate technical and organisational measures" to be able to 'demonstrate' their compliance with the Regulation, which shall also include "the implementation of appropriate data protection policies"[235]. Data processors are also bound by the accountability principle.

Demonstrating compliance means among others that the controller should be able to explain how personal data processing was implemented and how a particular decision was reached. In AI environment, responding to accountability requirements seems not to be an easy task, given the opacity of processing and the use of algorithms that do not have a decision tree structure but rely on the analysis

[234] See P. Hustinx (former EDPS), EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation.

[235] This includes internal and publicly-facing policies, records and notices, but also technical measures, and fundamental personnel and strategic changes to their processing operations. See G. Buttarelli (EDPS), Privacy in an age of hyperconnectivity. Keynote speech to the Privacy and Security Conference 2016 Rust am Neusiedler See, 7 November 2016.

of large amounts of data to establish correlations. Artificial intelligence powered systems whose decisions cannot be explained raise fundamental questions of accountability[236].

Additional difficulties may arise by the potential lack of clarity regarding the ultimate reasons for processing[237]. As emphasized by the European Data Protection Supervisor, AI raises fundamental questions of accountability for outcomes, as well as accountability for collection and use of massive quantities of personal data[238]. The requirements of this new principle have several implications for organisations undertaking big data analytics and/or machine learning. Accountability in this context means - also and specifically - to check and be able to demonstrate that the algorithms developed and used by machine learning systems " are actually doing what we think they're doing and aren't producing discriminatory, erroneous or unjustified results"[239].

One of the aspects of accountability that will have further implications for AI development and applications is the new obligation imposed on data controllers: the data protection impact assessment (DPIA). DPIAs form part of a more general "risk-based approach"[240] to data protection, intended to turn regulation of data processing towards risk management practices that also include

---

[236] 40th International Conference of Data Protection and Privacy Commissioners, DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE, Tuesday 23rd October 2018, Brussels.

[237] See ICO, par. 113.

[238] See Giovanni Buttarelli, 8th Annual Data Protection and Privacy Conference Brussels, 30 November 2017 Keynote speech.

[239] See ICO par. 115.

[240] A "progressive" risk-based approach would suggest instead that more detailed obligations should apply where the risk is higher and less burdensome obligations where it is lower. As advantage of this approach has been suggested that compliance efforts should be primarily directed at areas where this is most needed, having regard, for example, to the sensitivity of the data or the risk involved in a specific processing operation, rather than at a notification exercise to satisfy bureaucratic requirements. About a critical analysis of "risk – based approach" see N. van Dijk, R. Gellert, K. Rommetveit, A risk to a right? Beyond data protection risk assessments, Computer Law & Security Review 32 (2016), pp. 286–306.

other characteristic measures such as data protection by design and default, data protection officers, data breach notification, and prior consultation.

As a historical descendant to environmental and technology impact assessments and sharing similarities with Security Risks Assessments and Privacy Impact Assessments, which progressively developed from the 1990s, the Data Protection Impact Assessment[241] is expected to form another tool for better monitoring and ensuring compliance with the GDPR. In this perspective the introduction of Data Protection Impact Assessments as requirement is one on the innovative elements of the Regulation that may serve to respond also proactively to unforeseen technological challenges and anticipate and/or mitigate the respective risks.

We have to consider that risk is inherent to any data processing. Actually, anyone who process personal data has a duty, deriving at least from the data minimization principle, to assess purposes, means and risks involved. This assessment becomes mandatory[242] when the planned processing is likely to pose "a high risk" to individual's fundamental rights and freedoms. As indicated in the Article 29 Data Protection Working Party (WP29) Statement (14/EN WP 218), the reference to "the rights and freedoms" of the data subjects primarily concerns the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination,

[241] As PIA is defined as "a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative impacts" . See D. Wright and P. De Hert (eds.), Privacy Impact Assessment 2012, p. 5.

[242] Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)), carrying out a DPIA in an incorrect way (Article 35(2) and (7) to (9)), or failing to consult the competent supervisory authority where required (Article 36(3)(e)), can each result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. See Article 29 DPWP, 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, p. 4.

right to liberty, conscience and religion[243]. This approach has been reinforced by the Declaration of the 40th International DPAs Conference that acknowledges the need for data protection and privacy authorities to think about human rights more broadly[244].

The text of the Regulation does not define what is understood under "high risk". According to Recital 75 "a 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, unauthorised reversal of pseudonymisation, 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 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 analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles[245]; 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" . The Privacy and Data Protection Commissioners state that by assessing

[243] Article 29 DPWP 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, p. 15.

[244] See 40th International Conference of Data Protection and Privacy Commissioners, DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE, October 2018.

[245] The Article 29 DPWP refers as examples a bank that screens its customers against a credit reference database, or a company building behavioural or marketing profiles.

the risks one should take into consideration the collective impact that the use of AI may have on groups and on society at large[246].

Recital 76 clarifies when a risk is assessed "the likelihood and severity of the risk … should be determined by reference to the nature, scope, context and purposes of the processing". In order to identify a risk as "high" , it has to be evaluated "on the basis of an objective assessment".

The cases that a "high risk" could occur are indicatively listed in the Regulation, which refers to the "use of new technologies" also "taking into account the nature, scope, context and purposes of the processing" (Article 35 par. 1). In this context Article 35 (par. 3) defines the cases that definitely fall under the category of "high risk" : these pertain a) to profiling or to any "systematic and extensive evaluation of personal aspects" and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person[247] b) the processing on a large scale of special categories of data[248] or data related to criminal convictions and offences (sensitive data) or c) the large-scale monitoring of a public area (par. 2).

The GDPR provides a process-oriented approach to risk and high risk by enumerating the steps to be taken, including the necessary consultation[249]. A data

[246] See 40th International Conference of Data Protection and Privacy Commissioners, DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE, October 2018.

[247] See Recital 71 that clarifies ""in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles".

[248] These are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9 par.1).

[249] The GDPR does not specify which DPIA process must be followed but instead allows for data controllers to introduce a framework which complements their existing working practices provided it takes account of the components described in Article 35(7). As noted by the Article 29 DPWP in its Guidance on DPIA, such a framework can be bespoke to the data controller or common across a particular industry (p.20). The Article 29 DPWP provides also examples of EU generic frameworks. Standards like the ISO/IEC 29134:2017 may provide helpful guidance. The ISO/IEC 29134:2017 "Guidelines for

protection impact assessment should include the following as a minimum: a) a systematic description of the process, its purpose and which justified interest it protects, b) an assessment of whether the process is necessary and proportional, given its purpose ,c) an assessment of the risk that processing involves for people's rights, including the right to privacy, d)the measures selected for managing risk identified

At any event, the impact assessment ought to be drafted prior to undertaking such processing. However it has to taken into consideration that - as significant element of such assessments is the continuity of the evaluations, which follow the processing / application during their entire life-cycle - a DPIA has to be updated, when new features or modifications are introduced or new purposes are pursued.

Despite the uncertainty of "high risk threshold" , it is highly likely that most AI/ machine learning applications[250] will fall into the category of processing for which a DPIA should be conducted: this is obviously the case of profiling but also the processing of sensitive data. Authors have suggested that in view of the predictive nature of Big Data and the impossibility to define ex ante the "specified" purposes of data processing, it seems to be more adequate to require a mandatory data protection impact assessment in any cases in which these analytics are applied to datasets containing personal information[251] .

In any case AI applications involve novel technological applications as well as complex and often unexpected outcomes with respect to personal data. Therefore and in order to comply with fairness and accountability requirements

---

privacy impact assessment" standard aims to provide detailed directions for the privacy impact assessment process and the structure of its report.

[250] The ICO in its report on big data, artificial intelligence, machine learning, and data protection notes firmly that "potential privacy risks" have already been identified with "the use of inferred data and predictive analytics" (par. 160).

[251] P. Schwartz, risk-and-high-risk-walking-the-gdpr-tightrope. https://iapp.org/news/a/risk-and-high-risk-walking-the-gdpr-tightrope/ (March 2016).

it is of major importance to conduct a DPIA to assess to what extent the processing is likely to affect the individuals whose data is being used and to identify possible mitigation measures[252]. One inherent limitation of data protection impact assessment is however that forecasting is not an easy task because assessments are made on the basis of known or potential applications of the technology. Moreover, it has to be taken into account that there is often a significant time delay between the emergence of technology and the understanding of its consequences.

When the processing is related to social and ethical aspects and risks the assessment must be conducted not only by experts in data protection but also by auditors with specific and multi-disciplinary skills as the wide range of interests that should be considered requires the involvement of different stakeholders and experts[253] . Therefore the Regulation not only requires the participation of the Data Protection Officer (Article 35 par. 3)[254] but moreover it provides that, where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations. The stakeholder participation will allow to discover and discuss risks otherwise not considered. Stakeholder participation can also be used to assess risk perceptions and take more accountable decisions with respect to the envisaged processing[255]. If the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary

[252] See ICO, par. 158.

[253] See A. Mantelero, The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm inthe new era of predictive analytics, Computer Law & Security Report · November 2014, pp. 643-660, 657.

[254] The controller must also seek the advice of the Data Protection Officer (DPO), where designated (Article 35par. 2) and this advice, and the decisions taken, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA (Article 39 par. 1c=

[255] See L. Hempel and H. Lammerant, H., Impact Assessments as Negotiated Knowledge. In S. Gutwirth and P. de Hert (eds.), Reforming European Data Protection Law, Springer Netherlands 2015, pp. 125-145.

information[256]. Especially in cases where the processor provides cognitive services to developers acting as controllers, the processor has to support the processor with respect to identifying the nature and extent of potential interference of the envisaged processing with privacy and other fundamental rights of the data subjects and the respective risks and design the necessary measures to mitigate these risks.

Should the DPIA reveal that the planned processing may represent a high risk that cannot be faced by the controller, the latter has to consult the competent Data Protection Authority. Where the supervisory authority is of the opinion that the intended processing would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, it may exercise either its advisory[257]or its corrective powers.

8. AI and the Data Subject: Profiling and the Rights to Human Intervention and Explanation

Beyond the legal grounds of processing and the data protection principles the GDPR stipulates a number of responsibilities of data controllers and rights of data subjects that are relevant to AI algorithms. The GDPR takes a self-determination approach with respect to the rights it grants to individuals, an arsenal that is enhanced in comparison to the 1995 Data Protection Directive. Specific provisions are addressing rights with regard to profiling.

The Regulation does not regulate profiling separately; profiling as other forms of processing is subject to the legal grounds and the data protection principles as well as to all the rules governing the processing of personal data

w[256] See Article 29 DPWP which clarifies that regardless who is carrying the DPIA it is the controller who remains accountable for this task. See Article 29 DPWP, Guidance on DPIA, p. 13.

[257] According to Article 36 par. 2 the DPA may provide written advice.

(Recital 72)[258]. However GDPR devotes a specific definition to profiling which states that "profiling means 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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

The GDPR includes, however, specific provisions with reference to "automated individual decision-making, including profiling". The provision is formulated as right of the data subject "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" (Article 22 par.1). Article 22 right is quite narrow, and does not include preparatory activities taken prior to a decision making process (e.g. the creation of the original profile criteria)[259].

A first condition for the application of this right is that there cannot be any form of human intervention in the decision-making process, i.e. "a human must have undertaken an independent assessment of the underlying personal data, and be authorised to re-examine the recommendations the model has produced[260] . With regard to "human intervention" in AI context, Kuner et. al. note that it may not at all be feasible for a natural person to conduct a meaningful review of a process that may have involved third-party data and algorithms, prelearned models, or inherently opaque machine learning techniques[261]. Indeed "when

[258] The European legislators seem however to know that issues of interpretation will arise with regard to profiling. In this respect it is provided that "the European Data Protection Board should be able to issue guidance in this context".

[259] See also Butterworth with reference to the report of ICO (Par. 60).

[260] See Datatilsylnet, p. 20.

[261] See C. Kuner, D.J. B. Svantesson, F.H. Cate, O. Lynskey, and C. Millard Machine learning with personal data: is data protection law smart enough to meet the challenge? , p. 1.

computers learn and make decisions, they do so "without regard for human comprehension"[262].

In the Regulation there is no further explanation neither about the meaning of "legal effect" nor about what is meant with a decision that may significantly affect a data subject. As far as it concerns the "legal effect" it is related to decisions with impact on data subject's rights and duties (legal rights or rights set out in a contract)[263]. The meaning of decisions that are likely to significantly affect a person includes, for example, automatic refusal of an online credit application or e-recruiting practices without any human intervention. Another example could be this of the imposition of a fine solely on the basis of an image recorded by an automatic speed camera. Further it is suggested that given that a feature of big data is the ability to profile individuals and make decisions about them, by applying algorithms to large amounts of granular data, it is likely to significantly affect those individuals extending the scope of this right also to cases[264].

Article 22(2) of the GDPR does contain specific exemptions from the application of this right: a) necessity for the performance of a contract, b) authorization of profiling by law provided that suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are laid down in the legal act, c) data subject's explicit consent . That means that data subjects also have a right to object to automated processing, when data processing is for either public interest reasons or when the data subject's fundamental rights and freedoms outweigh the interests of the processing controller or third party. Concerning the latter case, the burden is on the controller to demonstrate that it has "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

---

[262] See J. Burrell, How the machine "thinks": Understanding opacity in machine learning algorithms. Big Data & Society 3, no. 1 (2016), pp. 1-12, 10.

[263] The Norwegian Datatilsylnet refers also to legal effects in cases such as banning from entering a country, receiving unemployment or social security benefits or cut of electricity because of unpaid bills. See Datatilsylnet, p. 19f.

[264] See ICO, par. 105.

Automated decision making is prohibited with respect to the special categories of data (sensitive data). However, the Regulation provides (22 par.4) also in this case for exemptions in the case that a) the data subject has explicitly consented to or b) the processing is necessary for reasons of substantial public interest and is performed on the basis of the law[265].

The exemptions that narrow the scope of the right not to be subject to a solely automated decision have been criticized especially with regard to the legal ground of consent. The consent has to be explicit, but it is doubtful how can informed consent be obtained in relation to a problem that may be inherently opaque and how the algorithmic process can be explained in an comprehensible way.

As counterbalance to these restrictions are granted with some specific rights in case that automated decision making that affects them is based on consent or a contractual relationship. Beyond the specific rights to information in Articles 13 (2) and 14 (2) the data subject can challenge the decision also by obtaining human intervention on the part of the controller[266], to express his or her point of view and to contest the decision[267]. Furthermore data subjects may ask for further explanations. Recital 71 states that the data subject has the right to obtain an explanation of the decision reached after such assessment.

[265] Both Article 22 par. 3 and Article 9 par. 2 (g) provide that suitable and specific measures to safeguard the fundamental rights and the interests of the data subject have to be taken by the data controller. Additional safeguards are required in Recital 71 that has been already dealt with.

[266] The European Group on Ethics in Science and New Technologies states that we have to consider on the debate about the introduction of the right to meaningful human contact (p. 9).

[267] Datatilsylnet emphasizes that the rules governing automated decision-making cannot be circumvented by fabricating human intervention (p. 20) . However, some have suggested that this right can be easily circumvented. See L. Jaakonsaari, Who sets the agenda on algorithmic accountability? EurActiv, 26 October 2016. https://www.euractiv.com/section/digital/opinion/who-sets-the-agendaon-algorithmic-accountability/

The data controller has to explain the decision in such a way that the data subject is able to understand the result and exercise her rights[268]. This "right to explanation"[269] particularizes the right to information as established in the data protection legislation and enhanced by the GDPR. The right of individuals to be provided with appropriate information in order not to "be subject to decisions that they do not understand and have no control over"[270] derives from the principle of (ex post) transparency as well as from "algorithmic accountability"[271].

The rights to obtain human intervention and explanation set new challenges to industry and developers. The ICO stress the attention to Big data organisations to the need to "exercise caution before relying on machine learning decisions that cannot be rationalised in human understandable terms"[272]. Authors point out that as Article 22's right to human intervention and explanation of logic requires that AI decisions be explainable, it is impractical to employ unsupervised models of machine learning. While a supervised model of learning uses labeled sets of data to develop algorithms, supplemented by human oversight, unsupervised models allow AI to evolve on its own[273]. With unsupervised models, it may not be possible to trace the AI's learning processes or to explain its decisions, due to a lack of data labels and relationships[274].

---

[268] Datatilsylnet , p. 21

[269] See B. Goodman and S. Flaxman, EU Regulations on Algorithmic Decision-making and a 'Right to Explanation' (2016) arXiv.org. Also L. Edwards and M. Veale, Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law and Technology Review, 16 (1), 2017, pp. 1-65. ISSN 2328-9600

[270] WP29 Opinion 3/2013 on purpose limitation, Annex 2.

[271] S. Taneja Hemant, The need for algorithmic accountability. TechCrunch, 8 September 2016. https://techcrunch.com/2016/09/08/the-need-for-algorithmic-accountability/

[272] See ICO, par 119.

[273] For an explanation of supervised and unsupervised AI learning, see Bernard Marr, Supervised V Unsupervised Machine Learning—What's The Difference?, FORBES (Mar. 16, 2017, 3:13 AM), http://bit.do/Marr_Supervised

[274] The human intervention is contested as "AI algorithms benefit from the allure of mathematical objectivity, which, combined with the complexity of data management and the subordinate position of those taking decisions in an organisation, can make it harder

Other authors suggest that even supervised models may be too hard to explain. However, explanation does not necessarily mean to open the "black box": the information must enable the data subject to understand why a particular decision was reached"[275] . According to Diakopoulos, there are in fact a number of elements of the algorithmic process that could be disclosed: Information on human involvement, quality of data (e.g. information about how training data have been collected and labelled, reliability of sources, accuracy and timeliness), the model and variables of the algorithm, the inferencing (including the margin of error predicted), and information on whether an algorithm was indeed used[276].

Serious concerns have been expressed with respect to the impact of this new right on AI industry as well as on AI development in general. According to Mittelstadt et al., "explainability may prove particularly disruptive for data intensive industries…. [given the connectivity and dependencies of algorithms and datasets in complex information systems, and the tendency of errors and biases in data and models to be hidden over time]"[277]. Other authors argue that GDPR "extensive protection of data privacy rights restrains the use of AI's most useful features: autonomy and automation"[278] risking to "impair one of AI's most useful purposes: automated decisions and forecasts"[279] .

---

for a human decision-maker to take a decision other than one suggested by the algorithm". See Council of Europe Consultative Committee, Report on Artificial Intelligence, p. 14.

[275] See S. Wachter, B. Mittelstadt and C. Russel, Counterfactual explanations without opening the black box: automated decisions and the GDPR, 2017.

[276] See N. Diakopoulos, Accountability in Algorithmic Decision Making, Communications of the ACM 59 (2) 2016, pp. 57, 60.

[277] See B. D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter and L. Floridi, The ethics of algorithms: Mapping the debate, p. 14.

[278] So M. Humerick, Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, 34 Santa Clara High Tech. L.J.393 (2018), p. 412.

[279] See N. Wallace, EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence, TECHZONE360 (Jan. 25, 2017), http://bit.do/Wallace_EU-Right-to-Explanation (explaining why algorithms and AI decisions are often not easily explained, because "[a]n algorithm can spot a correlation, but it cannot explain the link between them because it cannot infer meaning the way a human can").

C. AI, ETHICS AND FUNDAMENTAL RIGHTS

1. Does GDPR deal sufficiently with AI?

In light of concerns with regard to the implications of AI on privacy and data protection rights consideration must be given to the adequacy of the new legal framework to respond to the new challenges. Does GDPR deal sufficiently with AI? Is AI controllable and subject to regulation? Are artificial intelligence and data protection incompatible?

It is true that the potential of AI is likely to result to – non predictionable – penetrating data processing. As R. Calo notes, "[a]rtificial intelligence is increasingly able to derive the intimate from the available …[as] freely shared information of seeming innocence — where you ate lunch, for example, or what you bought at the grocery store — can lead to insights of a deeply sensitive nature"[280]. AI challenges the concepts that define the material scope of data protection law, this of "personal data" and that of the "data subject": the notion and extent of identifiability[281] will be subject to further, far-reaching transformations[282].

It is supported that AI, in a manner analogous to Big Data, represents a challenge for the application of traditional data processing principles and may necessitate the elaboration of new applicative solutions to safeguard informational privacy and other fundamental rights[283]. Indeed, AI and Robotics

[280] See Ryan Calo, Artificial Intelligence Policy: a primer and roadmap, p. 17. However we must note that this is actually a feature of ICTs that led to the need to adopt data protection regulations.

[281] See also P. Niemitz, Constitutional Democracy and Technology in the age of Artificial Intelligence.

[282] So N. Purtova notes that in this context "everything in this environment – weather, waste water, exam scripts–is being increasingly "datified", and literally any data can be plausibly argued to be personal ". S. Nadezhda Purtova (2018) The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, 10:1, 40-81, p. 41.

[283] Council of Europe, Report on Artificial Intelligence -Artificial Intelligence and Data Protection: Challenges and Possible Remedies, September 2018, p. 9.

are advancing more rapidly than the process of finding answers to ethical, legal and societal questions[284].

But this is the case of every data intensive technology. Regulations like the GDPR will always fall behind new advances in technology[285], if only because it is too difficult for the regulatory change to keep pace with the technological one. On the other side reforming the law to reflect new technologies may be proved a "fallacy"[286]. It is extremely difficult to – steadily? - change or update legislation like GDPR. Such an ambition would stimulate a vicious circle as technology changes also during the consultation and negotiation procedures, thus posing the risk to result into legal uncertainty.

In our view, GDPR - due to the technology independent regulatory approach -will apply to AI when personal data is processed. The provisions of GDPR with regard to the rights of the data subjects, the obligations deriving from accountability or the obligations of processors will contour the way AI and machine learning will be developed and applied. Moreover, the GDPR comprises, in our opinion, the elements to face the technological transformations. A first tool consists in the Data Protection Impact Assessments that have to be carried out before deployment of high-risk technologies. A second tool, strictly interrelated to DPIA is the duty to protect personal data by design that the GDPR compels to data controllers.

[284] European Group on Ethics in Science and New Technologies, Artificial Intelligence, Robotics and 'Autonomous' Systems, p.11.

[285] See E. Fosch Villaronga , P. Kieseberg and L. Tiffany, Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten, Computer Law and Security Review 34 (2018), pp. 304-313, 304.

[286] So Niemitz, who states that the claim that the law is not precise and no detailed enough to regulate complex technology is another fallacy of the engineering view of the world. See P. Niemitz Constitutional Democracy and Technology in the age of Artificial Intelligence.

2. Data Protection friendly AI by design?

The GDPR recognizes the contribution of technology to the transformation of economy and social life and the need to facilitate the free flow of data, "while ensuring a high level of the protection of personal data" (Recital 6). Data protection by design falls between the responsibilities of controllers, referring mainly to the concept that information and communications technologies and systems should be designed and also operated as taking data protection by design into account, even from the outset, as a default setting[287]. The article 25 par. 1 requires the data controller to implement -both at the time of the determination of the means for processing and at the time of the processing itself-appropriate technical and organisational measures, which are designed to implement data-protection principles and to integrate the necessary safeguards into the processing in order to meet the requirements of the Regulation[288].

Data Protection by Design, like is "ancestor" Privacy by Design, is not a new concept: it embraces a practical approach that orientates the entire life cycle activities pertinent to a technology or system- from research, design, development, implementation, use and disposal – towards the embedment of privacy and data protection into the design of the technology or system. Another concept, Privacy in Design is closely related with Privacy by Design. Privacy in Design emphasizes on raising awareness about the processes through which values and norms become embedded in the technological architecture[289].

---

[287] Attila Kiss and Gergely László Szoke, Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation IN Reforming European Data Protection Law, p. 311 ff.

[288] Data protection by design has regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data.

[289] According to the European Group on Ethics, privacy in design refers to the Constructive Technology Assessment (CTA), which was developed in the Netherlands and Denmark.

Like the performance of data protection impact assessments, the requirement of data protection by design underlies that risk awareness and a precautionary approach are crucial for addressing the challenges of new technologies. If Data Protection Impact Assessments have been suggested as a useful tool for engineers and software developers to help them to consider potential negative consequences of particular elements of a technology design, data protection by design enables the adaptation of the data protection framework to technological developments.

As emphasized by the European Group on Ethics in Science and New Technologies, "applications of AI and robotics should not pose unacceptable risks of harm to human beings, and not compromise human freedom and autonomy"[290]. On the contrary they should aim at the protection of fundamental rights and values and developed with the aim to "serve mankind"[291] and in a way that facilitates human development and does not obstruct or endanger it. AI technologies should "be designed, developed and used in respect of fundamental human rights and in accordance with the fairness principle [292]. Not binding AI technologies to basic constitutional principles would led to a "widespread culture of disregard of the law and put democracy in danger"[293].

CTA focusses on broadening design, development, and implementation processes. This model emphasizes the early involvement of a broad array of actors to facilitate learning about technology and its potential impacts. See European Group on Ethics in Science and New Technologies to the European Commission, Ethics of security and surveillance technologies - Opinion no. 28, 2014.

290 European Group on Ethics in Science and New Technologies, Artificial Intelligence, Robotics and 'Autonomous' Systems, p. 17.

291 See Recital 4 of GDPR.

292 40th International Conference of Data Protection and Privacy Commissioners, DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE. This is a regulatory approach shared also by private actors. In the analysis of Microsoft is stated that "AI systems should also be designed so that private information is used in accordance with privacy standards and protected from bad actors who might seek to steal private information or inflict harm". See Microsoft, The Future Computed, p.68.

293 As it was the case with the absence of efficient framing of internet economy. See P. Niemitz, Constitutional Democracy and Technology in the age of Artificial Intelligence.

To be able to protect fundamental rights, research, design and development of AI, robotics and "autonomous" systems should be guided by an authentic concern for research ethics, social accountability of developers, and global academic cooperation. In this perspective privacy conscious engineering[294] or – more specifically – data protection by design echoes the discourse about Responsible Research and Innovation (RRI). One of the first definitions of RRI is offered by von Schomberg, who suggests that it can be understood as "a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view on the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society)"[295] .

A simple view of Responsible Research and Innovation's emergence to prominence as the most influential framework for research and innovation governance might interpret it as a result of problems with particular innovations, and as an attempt to prevent those problems recurring in the future. One important issue for research and innovation is the observation that there are often systematic forms of unfairness embedded in innovation processes. Key elements of an RRI approach is being anticipatory, reflective, collective, responsive and transparent. Such a framework should anticipate both intended and unintended impacts of technology. Innovators must reflect on the underlying purposes, motivations and potential impacts, what is known and what is not known, and associated uncertainties, risks, areas of ignorance, assumptions, questions and dilemmas. Important is to deliberate visions, purposes, questions and dilemmas

[294] According to G. Buttarelli (EDPS) privacy conscious engineering is one of the pillars of the Big Data Protection Ecosystem. G. Buttarelli, Privacy in an age of hyperconnectivity Keynote speech to the Privacy and Security Conference 2016 Rust am Neusiedler See, 7 November 2016.

[295] D. R. von Schomberg, Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields, Publicaitons Office of the European Union, Luxembourg, 2011, p.3.

collectively and in an inclusive manner and be responsive to issues relate to R&I in an iterative, inclusive and open and transparent manner. To be responsible means to consider future uses of technologies and their possible privacy implications as well as consequences for other human rights[296].

3. Of Fundamental Rights and AI Ethics

Enhanced accountability and transparency requirements of GDPR pose technical challenges for AI developers to mitigate adverse effects of AI. However, data Protection, even by design, is not merely a technical issue. Accountability and transparency are mere tools to support the protection of values and principles while developing and using AI technologies. Addressing the impact of those technologies necessitates to identify rights at risk, the underlying principles and values and the way to protect them.

In the last period there has been a trend[297] that underlines the need for an ethical approach that supports and goes beyond compliance with legal requirements[298]. However, ethics is not conceived as alternative to compliance to the law but as the underpinning for genuine compliance, for avoiding box-ticking approaches which undermine trust in digital services [299].

Data protection laws are actually based on ethical notions that underpin the fundamental rights of privacy and data protection. Accountability implies that

[296] See B. C. Stahl, Responsible research and innovation: The role of privacy in an emerging framework, Science and Public Policy 40 (2013) pp. 708–716.

[297] Hijmans and Raab note that beyond the GDPR and data protection more generally, in recent years there has been a proliferation of more directly 'ethical' discourse in the data protection community among commercial and governmental data controllers, as well as supervisory authorities, featuring the formation of ethical codes of practice, ethics advisory processes and groups, and an increasing awareness of data ethics.

[298] ICO, Big data, artificial intelligence, machine learning and data protection, par. 172.

[299] Giovanni Buttarelli, 8th Annual Data Protection and Privacy Conference Brussels, 30 November 2017 Keynote speech .

a responsible controller endeavours to respect the underlying principles of data protection and demonstrates its compliance both with regard to the performance of tasks, even when this is not explicitly required by the GDPR[300].

Furthermore, data protection frameworks depend to a great extent on balancing between rights of the data subjects and interests of data controllers, either legitimate interests of private persons or public interests expressed by the law or a public body acting as a controller. The GDPR contains a number of mandatory rules that may require a judgement, especially when it comes to identify and assess risks, the nature, likehood and severity of them defines the obligations of data controller (risk-based approach). However, even if balancing as core part of decision making with regard to processing, does not consist in ethical assessments, it acquires an ethical perspective "when it includes the weighing of moral values or human rights and, hence, a judgement about what is good and bad for an individual and society" [301].

The European Group on Ethics in Science and New Technologies identifies a clear need for a collective, wide-ranging and inclusive process towards a commonly acceptable framework for the design, production, use and governance of AI, robots and "autonomous" systems[302]. The current trend in addressing the ethical and legal aspects of AI and machine learning is to focus on fairness, autonomy, responsibility and ethical principles[303]. Microsoft suggests fairness, reliability and safety, privacy and security, inclusiveness, transparency and accountability as the six ethical principles to govern AI[304].

[300] Hijmans and Raab, Ethical Dimensions of the GDPR, p.10

[301] Hijmans and Raab, p.10.

[302] European Group on Ethics in Science and New Technologies Artificial Intelligence, Robotics and 'Autonomous' Systems, p. 10ff.

[303] See Aída Ponce Del Castillo (Senior researcher at the European Trade Union Institute) Artificial intelligence: a game changer for the world of work, Foresight Bried June 2018, p.8.

[304] Microsoft, The Future Computed, p.137.

Assessing risks and balancing of interests requires contextual assessments taking into consideration the constitutional values framework. The European Parliament has highlighted the need for ethical principles concerning the development of robotics and artificial intelligence for civil use. It points out that a guiding ethical framework should be "based on […] the principles and values enshrined in Article 2 of the Treaty on European Union and in the Charter of Fundamental Rights, such as human dignity, equality, justice and equity, non-discrimination, informed consent, private and family life and data protection", among other principles[305].

Assessment of compliance with ethical and social values is more complicated than the "traditional" data protection assessment, as it addresses rights like the right to non-discrimination[306]. A core principle and starting point is the inviolability of human dignity, that is not only a fundamental right but also the foundation for subsequent freedoms and rights, including the rights to privacy and to the protection of personal data[307]. Without doubt there is an interference with human dignity when a person is treated not as an end-in-itself but as means to an end.

Both dignity and autonomy are affected if individuals are deprived from the right to exercise influence over decision-making processes that significantly affect them[308]. Moreover, it is of importance, whether they have the ability to exercise this influence and who is responsible and accountable to enable them. Even if we accept the argument that automated decision making is supposed to be fairer and more efficient or effective, such a procedure may dehumanize

[305] European Union Fundamental Rights Agency, #BigData: Discrimination in data-supported decision making, 2018, p. 2.

[306] COUNCIL OF EUROPE – REPORT ON AI -SEPTEMBER 2018, p. 17.

[307] INTERNATIONAL PRIVACY CONFERENCE, Artificial intelligence and robotics, p.16.

[308] See I. Mendoza and L.A. Bygrave, The Right not to be Subject to Automated Decisions based on Profiling, University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20, at 3.

individuals or social processes[309]. Beyond the establishment of a right to human intervention in the GDPR (Article 22 par. 3), the European Group on Ethics in Science and New Technologies Artificial Intelligence points to the ongoing debate about the introduction of two new rights: the right to meaningful human contact and the right to not be profiled, measured, analysed, coached or nudged [310].

Furthermore, autonomy and self-determination refer to the freedom of choice over the use of AI, a choice that has to be informed and free. Guaranteeing the right to informational self-determination means ensuring that individuals are always informed appropriately when they are interacting directly with an artificial intelligence system or when they provide personal data to be processed by such systems. Strong data protection and privacy safeguards help to build individuals' trust in how their data is processed, which encourages data sharing and thereby promotes innovation[311]. Solving the control problem is a critical prerequisite over the long term in order for more powerful AI systems to have positive impacts on society[312].

In this context, the 40th International Conference of Data Protection and Privacy Commissioners underlined the significance of promoting transparency, intelligibility and reachability and called for common governance principles on artificial intelligence to be established, fostering concerted international efforts in this field, in order to ensure that its development and use take place in accordance with ethics and human values, and respect human dignity.

---

[309] See Meg Leta Jones, The right to a human in the loop: Political constructions of computer automation and personhood, Social Studies of Science 2017, Vol. 47(2), p. 216 –239.

[310] European Group on Ethics in Science and New Technologies Artificial Intelligence, Robotics and 'Autonomous' Systems, p. 19.

[311] 40th International Conference of Data Protection and Privacy Commissioners.

[312] M. Brundage, Scaling Up Humanity: The Case for Conditional Optimism about Artificial Intelligence in Should we fear the future of artificial intelligence?

BIBLIOGRAPHY

Ali R., *Technological Neutrality*, Lex Electronica, vol. 14 n°2 (Automne / Fall 2009).

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*, 2017

Article 29 Data Protection Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, 2014

Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 2014

Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data,* 2007.

Barnet B.A., *Idiomedia: The rise of personalized, aggregated content*, Continuum 23(1) 2009, pp. 93–99.

Barocas S. and Nissenbaum H., *Big Data's End Run around Procedural Privacy Protections*, Communications of the ACM, vol. 57, no. 11 (2014), pp. 31-33

Berberich M. and Steiner M., *Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?* European Data Protection Law Review, Volume 2 (2016), Issue 3, pp. 422 – 426

Brkan M., *Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond*. Paper submitted in view of presentation at the conference "Terminator or the Jetsons? The Economics and Policy Implications of Artificial Intelligence", Technology Policy Institute, Washington 22 February 2018.

Brundage M., *Scaling Up Humanity: The Case for Conditional Optimism about Artificial Intelligence*, in European Parliament – European Parliamentary Research Service, Should we fear Artificial Intelligence?, March 2018

Burrell J*., How the machine "thinks": Understanding opacity in machine learning algorithms,*Big Data & Society 3, no. 1 (2016), pp. 1-12

Burri, M., & Schär, R., *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, *Journal of Information Policy, 6* (2016), pp. 479-511

Buttarelli G., *A smart approach: counteract the bias in artificial intelligence*. (2016) Accessible at https://edps.europa.eu/press-publications/press-news/blog/smart-approach-counteract-bias-artificial-intelligence_en

Buttarelli G. (EDPS), *Privacy in an age of hyperconnectivity*, Keynote speech to the Privacy and Security Conference 2016 Rust am Neusiedler See, 7 November 2016

Buttarelli G. (Assistant *European Data Protection Supervisor), Internet of things: ubiquitous monitoring in space and time*, European Privacy and Data Protection Commissioners' Conference Prague 2010

Butterworth M., The *ICO and artificial intelligence: The role of fairness in the GDPR framework*, Computer Law & Security Review 34 (2018) 257–268

Calo R., *Artificial Intelligence Policy: a primer and roadmap*, Accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015350

Carolan E., *The continuing problems with online consent under the EU's emerging data protection principles*, Computer Law & Security Review 32(3) 2016, pp. 462-473

Čas J., *Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions*, In: Gutwirth S., Poullet Y., De Hert P., Leenes R. (eds) Computers, Privacy and Data Protection: an Element of Choice. Springer, Dordrecht, (2011), pp. 139-169

Cath S., Wachter B., Mittelstadt M., Tadde L., Floridi L., *Artificial Intelligence and the 'Good Society': the US, EU, and UK approach*, Science and Engineering Ethics, Volume 24, Issue 2 (2018), pp. 505–528.

CNIL, *COMMENT PERMETTRE À L'HOMME DE GARDER LA MAIN ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Décembre 2017

Collingwood L., *Privacy implications and liability issues of autonomous vehicles*, Information & Communications Technology Law, 26:1 (2017), pp. 32-45

Conrad S., *Künstliche Intelligenz – Die Risiken für den Datenschutz*, Datenschutz und Datensicherheit 12/2017, pp. 740-744.

Conti M., Passarella A., Das S. K., *The Internet of People(IoP) :A new wave in pervasive mobile computing*, in Pervasive and Mobile Computing, 41 (2017), pp. 1-27.

Copeland J., *What is Artificial Intelligence?* (AlanTuring.net, May 2000). Accessible http://www.alanturing.net/turing_archive/pages/reference%20articles/what%20is%20ai.html

Couldry N. and Yu J., *Deconstructing datafication's brave new world*, New media & Society 2018, pp. 1-19

Council of Europe, *Report on Artificial Intelligence*, September 2018

Datatilsynet, *Artificial Intelligence and Privacy – Report*, January 2018

D' Acquisito G. et al. *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*. ENISA, December 2015.

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-dataprotection

de Andrade N.N.G., *Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights*, in S. Fischer-Hübner, P. Duquenoy, M. Hansen, R, Leenes, Ge Zhang (Eds.), Privacy and Identity Management for Life, Springer 2011, pp. 90-107.

Diakopoulos N., *Accountability in Algorithmic Decision Making*, Communications of the ACM 59 (2) 2016, pp. 57-62

Dinant J.-M., Lazaro C., Poullet Y., Lefever N., Rouvroy A., *Application of Convention 108 to the profiling mechanism. Some ideas for the future work of the consultative committee (T-PD)*, Strasbourg 2008.

Edwards L. and Veale M., *Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*. Duke Law and Technology Review, 16 (1) 2017, pp. 1-65. ISSN 2328-9600

Eiband M., Schneider H., Buschek D., *Normative vs Pragmatic: Two Perspectives on the Design of Explanations in Intelligent Systems*, ExSS '18, March 11, Tokyo, Japan

European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Towards a new Framework for Electronic Communications Infrastructure and Associated Services.* Communications Review COM (1999) 539 final

European Digital Rights (EDRi): *Position on the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (2013)

European Group on Ethics in Science and New Technologies, *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*, March 2018

European Union Agency for Fundamental Rights, #*BigData: Discrimination in data-supported decision making*, 2018

European Union Agency for Fundamental Rights, *Handbook on European data protection law*, Edition 2018.

European Union Agency for Network and Information Security (ENISA), *Privacy, Accountability and Trust– Challenges and Opportunities*, 2011

Executive Office of the President - National Science and Technology Council - Committee on Technology, *Preparing for the future of artificial intelligence*. (2016). Accessible at https://obamawhitehouse.

Finlay S. , *Artificial Intelligence and Machine Learning for Business*, Third edition 2018.

Floridi F., *Big data and their epistemological challenge*, Philosophy & Technology 25(4) 2012, pp. 435–437

Fosch Villaronga E., Kieseberg P. and Tiffany L., *Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten*, Computer Law and Security Review 34 (2018), pp. 304-313

Glancy D., *Privacy in Autonomous Vehicles,* 52 Santa Clara L. Rev (2012), pp 1171-1839.

Greenfield A., *Everyware. The dawning age of ubiquitous computing* (Berkeley: New Riders, 2006)

Hacker P., *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*, SSRN-id3164973.pdf

Hempel L. and Lammerant H., H., *Impact Assessments as Negotiated Knowledge*, In S. Gutwirth and P. de Hert (eds.), Reforming European Data Protection Law, Springer Netherlands 2015, pp. 125-145.

Hijmans H. and Raab C., *Ethical Dimensions of the GDPR*, in: M. Cole and F. Boehm (eds.) Commentary on the General Data Protection Regulation Cheltenham: Edward Elgar (2018).

Hildebrandt M., *Law as Information in the Era of Data-Driven Agency*, The Modern Law Review 79 (2016), pp. 1-30.

Hildebrandt M. and Tielemans L, *Data protection by design and technology neutral law*, Computer Law & Security Review Volume 29, Issue 5 (2013), pp. 509-521

Hildebrandt M. and Gutwirth S., *Profiling the European citizen: cross-disciplinary perspectives*, Springer, New York (2008)

Humerick M., Taking AI Personally: *How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence*, 34 Santa Clara High Tech. L.J.393 (2018). Accessible at: https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3

Hustinx P. , *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, 2013

Information Commissioner Office (ICO), *Big data, artificial intelligence, machine learning and data protection*, 2017

International Conference of Data Protection and Privacy Commissioners (38th), *Artificial Intelligence, Robotics, Privacy and Data Protection* – Room Document, October 2016

International Conference of Data Protection and Privacy Commissioners (40th) *DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE* (Tuesday 23rd October 2018, Brussels).

Jaakonsaari L., *Who sets the agenda on algorithmic accountability?* EurActiv, 26 October 2016. https://www.euractiv.com/section/digital/opinion/who-sets-the-agendaon-algorithmic-accountability/

Johnson Δ., *Computer Ethics*, Pearson, Upper Saddle River, NJ 2009

Jones M. Λ., Kaufman E., and Edenberg E., *AI and the Ethics of Automating Consent*, IEEE Security & Privacy (Volume 16 , Issue: 3 , May/June 2018), pp. 64-72

Kamarinou D., Millard C, and Singh J., *Machine Learning with Personal Data* , Queen Mary University of London, School of Law Legal Studies Research Paper 247/2016

Kaori Ishi, *Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects*, AI & Soc (published online 31 August 2017)

Kindt E.J., *Why research may no longer be the same*, Computer Law & Security Review 32 (2016), pp 729–748

Kiss A and Szoke G., *Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation* In: Gutwirth S, Leenes R, de Hert P (eds.) Reforming European Data Protection Law, Springer, Netherlands, pp. 311-331

Kleinberg J., Himabindu Lakkaraju, Leskovec J., Ludwig J., Sendhil Mullainathan, *Human Decisions and Machine Predictions, The Quarterly Journal of Economics, Volume* 133, Issue 1, 1 February 2018, pp. 237–293

Koops B.-J., *The trouble with European data protection law*, International Data Privacy Law, 2014, Vol. 4, No. 4, pp. 250-261

Koops J-P, *Should ICT Regulation be Technology-Neutral? Starting points for ICT regulation. Deconstructing prevalent policy one-liners*, IT & LAW SERIES, Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens (eds.), Vol. 9, , The Hague: T.M.C. Asser Press, 2006, pp. 77-108

Kroll J.A., Huey J., Barocas S., Felten E. W., Reidenberg J. R., Robinson D. G. & Yu H., *Accountable Algorithms*, 165 UNIV. OF PENN. L. REV (2017), pp. 633-705

Kuner C., Svantesson D. J. B., Cate F.H., Lynskey O. and Millard C., *Machine learning with personal data: is data protection law smart enough to meet the challenge?* International Data Privacy Law, 2017, Vol. 7, No. 1, pp. 1-2

Kuner C., *Data Protection Law and International Jurisdiction on the Internet (Part 1)*, International Journal of Law and Information Technology, Vol. 18 (2010), pp. 176-193

Mantelero A., *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, Computer Law & Security Review 32 (2016), pp. 238–255

Mantelero A., *The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics*, Computer Law & Security Review 30(6) 2014, pp. 643-660

Mayer -Schönberger V. and Padova Y., *Regime change? Enabling big data through Europe's New Data Protection Regulation*, Columbia Science and Technology Law Review 17(2016), pp. 315-325.

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

Mendoza I. and Bygrave L.A., T*he Right not to be Subject to Automated Decisions based on Profiling*, In: Synodinou TE., Jougleux P., Markou C., Prastitou T. (eds) EU Internet Law. Springer, Cham, pp. 77-98.

MICROSOFT, *The Future Computed, Artificial Intelligence and its role in society.* Published by Microsoft Corporation Redmond, Washington. U.S.A. 2018 (Foreword by Brad Smith and Harry Shum), 2018

Minsky J., *Steps Toward Artificial Intelligence*, PROCEEDINGS OF THE IRE, 1961, pp. 8-30.

Miron M. (Joint Research Center of the European Commission*), Interpretability in AI and its relation to fairness, transparency, reliability and trust*, 9.4.2008, at https://ec.europa.eu/jrc/communities/community/humaint/article/interpretability-ai-and-its-relation-fairnesstransparency-reliability-and

Mitrou L., *The General Data Protection Regulation: A law for the Digital Age?* in T. Synodinou et al. (Eds), EU Internet Law, Regulation and Enforcement, Springer 2017, pp. 19-57

Mitrou L., *Privacy Challenges and Perspectives in Europe* in M. Bottis (ed.) An Information Law for the 21st Century (Proceedings of Third International Seminar on Information Law), Athens 2011, pp. 220-236

Mitrou L., *The Commodification of the Individual in the Internet Era: Informational Self-determination or "Self-alienation"?* in Proceedings of 8th International

Conference of Computer Ethics Philosophical Enquiry (CEPE 2009), INSEIT, Athens 2009, pp. 466-485.

Mittelstadt B. D., Allo P. , Taddeo M., Wachter S. and Floridi L., *The ethics of algorithms: Mapping the debate*, Big Data & Society July–December 2016, pp. 1–21

Mourby M., Mackey E., Elliot M., Gowans H., Wallace S. E., Bell J., Smith H., Aidinlis S., Kaye J., *Are "pseudonymized" data always personal data? Implications of the GDPR for administrative data research in the UK*, Computer Law & Security Review 34 (2018), pp. 222–233

Niemitz P., *Constitutional Democracy and Technology in the age of Artificial Intelligence*. Accepted for publication in Royal Society Philosophical Transactions, 2018

Noain-Sánchez A., *Privacy by default and active informed consent by layers: essential measures to protect ICT users' privacy*, Journal of Information, Communication and Ethics in Society 14(2), 2016, pp. 124-138.

Pasquale F. , *The black box society: the secret algorithm behind , money and information*. Harvard University Press, Massachusetts, 2015

Purtova N. , *The law of everything. Broad concept of personal data and future of EU data protection law*, Law, Innovation and Technology, 10:1(2018), pp. 40-81

PWC, *Leveraging the upcoming disruptions from AI and IoT How Artificial Intelligence will enable the full promise of the Internet-of-Things*, 2017

Reed C., *How Should We Regulate Artificial Intelligence*? Philos Trans A Math Phys Eng Sci. 2018 Sep 13;376(2128). doi: 10.1098/rsta.2017.0360

Reimer S. H. and Wegener C. , *Künstliche Intelligenz: Vorsicht Hype! Datenschutz und Datensicherheit 10/2018*, pp. 599-600

Russell S. and Norvig P. , *Artificial Intelligence: A Modern Approach* (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall 2003.

Schermer B. W, *The limits of privacy in automated profiling and data mining*, Computer Law and Security Review 27 (2011), pp. 45-52

Schultz T., *Carving up the Internet: Jurisdiction, Legal orders, and the Private/Public International Law Interface,* European Journal of International Law 19 (4) 2008, pp. 799- 839.

Schwartz P. and Solove D., *Reconciling Personal Information in the United States and European Union,* 102 California Law Review (2014), pp. 877-916

Schwartz P., *risk-and-high-risk-walking-the-gdpr-tightrope*. (March 2016). https://iapp.org/news/a/risk-and-high-risk-walking-the-gdpr-tightrope/

Simitis S., *Kommentar zum Bundesdatenschutzgesetz*, Nomos Baden-Baden 2014

Simitis S., *Die Erosion des Datenschutzes – Von der Abstumpfung der alten Regelungen und den Schwierigkeiten, neue Instrumente zu entwickeln*, in B. Sokol (Hrsg.), Neue Instrumente im Datenschutz, Düsseldorf 1999.

Skouma G. and Léonard L., *On-line behavioral tracking: What may change after the legal reform on personal data protection*. In: Gutwirth S et al. (eds.) Reforming European Data Protection Law. Springer Netherlands 2015, pp. 35-60

Stahl B.C. and Wright D., *AI ETHICS*- IEEE Security & Privacy (Special Issue) May/June 2018.

Stahl B. C., *Responsible research and innovation: The role of privacy in an emerging framework*, Science and Public Policy 40 (2013) pp. 708–716.

Svantensson D.J.B, *The extraterritoriality of EU data privacy law - its theoretical justification and its practical effect on U.S. businesses*. *Stanford Journal of International Law* 50(1) 2013, pp 53-117

Taneja Hemant S., *The need for algorithmic accountability*. TechCrunch, 8 September 2016. https://techcrunch.com/2016/09/08/the-need-for-algorithmic-accountability/

Turing A., *Computing Machinery and Intelligence*, 49 Mind (1950), pp. 433– 460

UK Government Office for Science, *Artificial intelligence: opportunities and implications for the future of decision making*, 2015

UNESCO-World Commission on the Ethics of Scientific Knowledge and Technology (COMEST), *Report on Robotics Ethics*, Paris 2014

Yunhe Pan, *Heading toward Artificial Intelligence 2.0*, Engineering 2 (2016), pp. 409-413

van Dijk N., Gellert R., Rommetveit K*., A risk to a right? Beyond data protection risk assessments* , Computer Law & Security Review 32 (2016), pp. 286–306.

Van Otterlo M., *A machine learning view on profiling*, In: Hildebrandt M and de Vries K (eds) Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology. Abingdon: Routledge 2013, pp. 41–64

Veale M., Reuben B. and Edwards L., *Algorithms That Remember: Model Inversion Attacks and Data Protection Law*, Philosophical Transactions of the Royal Society, 2018.

von Schomberg D.R. , *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, Publications Office of the European Union, Luxembourg, 2011

Wallace N., *EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence*, TECHZONE360 (Jan. 25, 2017), Accessible at http://bit.do/Wallace_EU-Right-to-Explanation

White House Office of Science and Technology Policy (OSTP), *Preparing for the Future of Artificial Intelligence*, October 2016.

Wright D. and De Hert P. (eds.), *Privacy Impact Assessment*, Springer 2012

Zarsky T. Z., *Incompatible: the GDPR in the age of big data*, Seton Hall Law Rev 2017;47(2): Accessible at https://ssrn.com/ abstract=3022646

Zarsky, T., *Transparent Predictions*. University of Illinois Law Review 4 (2013), pp. 1503-1570.