AI LAW

INTERNATIONAL REVIEW
OF ARTIFICIAL INTELLIGENCE LAW

Data Processing and Algorithms: A Constitutionally Oriented AI?*

Nadia Maccabiani

Professoressa associata di Diritto pubblico
nell'Università degli Studi di Brescia

Abstract

(EN): Starting from multiple and entangled paradigm shifts prompted by improved artificial intelligence (AI) systems, the paper focuses on the fundamental value of human dignity and insulates a 'dehumanising' process that flows through three channels: data, knowledge and power. It delves into the stance undertaken by the European Union to 'rehumanise' these aspects by means of its latest legislative acts (AI Act, DMA, DSA, Data Governance Act, Data Act). It concludes with an interdisciplinary proposal of reflection on profiling techniques aimed not only at complementing the approach adopted by the GDPR and DSA, thus introducing collective safeguards, but also at streamlining the solutions undertaken by the AI Act and completing the DMA kick-in for combination and cross use of data. Thus, the addressed goal is the adoption of a more substantial defence for the sake of human dignity and equality, against a process (profiling) that stands at the crossroads of data, knowledge and power and acts as an enabler of intrusive and pervasive insights on people.

(ES): Partiendo de múltiples y entrelazados cambios de paradigma impulsados por sistemas mejorados de inteligencia artificial (IA), el artículo se centra en el valor fundamental de la dignidad humana y aísla un proceso 'deshumanizador' que fluye a través de tres canales: datos, conocimiento y poder. Profundiza en la postura adoptada por la Unión Europea para 'rehumanizar' estos aspectos mediante sus últimos actos legislativos (Ley de IA, DMA, DSA, Ley de Gobernanza de Datos, Ley de Datos). Concluye con una propuesta interdisciplinaria de reflexión sobre técnicas de perfilado que no solo complementan el enfoque adoptado por el RGPD y la DSA, introduciendo así salvaguardias colectivas, sino que también optimizan las soluciones emprendidas por la Ley de IA y completan la activación del DMA para la combinación y el uso cruzado de datos. Así, el objetivo abordado es la adopción de una defensa más sustancial en pro de la dignidad humana y la igualdad, frente a un proceso (perfilado) que se encuentra en la

* Report presented at the Conference «Piattaforme online, dati e intelligenza artificiale tra interessi pubblici e garanzie dei privati», held at the University of Sannio in Benevento on June 13-14, 2024.

encrucijada de datos, conocimiento y poder y actúa como habilitador de conocimientos intrusivos y omnipresentes sobre las personas.

(FR): À partir de multiples changements de paradigme entrelacés, déclenchés par des systèmes d'intelligence artificielle (IA) améliorés, l'article se concentre sur la valeur fondamentale de la dignité humaine et isole un processus 'déshumanisant' qui passe par trois canaux: les données, la connaissance et le pouvoir. Il explore la position adoptée par l'Union européenne pour 'réhumaniser' ces aspects au moyen de ses derniers actes législatifs (Loi sur l'IA, DMA, DSA, Loi sur la gouvernance des données, Loi sur les données). Il conclut par une proposition interdisciplinaire de réflexion sur les techniques de profilage visant non seulement à compléter l'approche adoptée par le RGPD et la DSA, en introduisant ainsi des garanties collectives, mais également à rationaliser les solutions entreprises par la Loi sur l'IA et à compléter l'activation du DMA pour la combinaison et l'utilisation croisée des données. Ainsi, l'objectif abordé est l'adoption d'une défense plus substantielle au nom de la dignité humaine et de l'égalité, contre un processus (profilage) qui se trouve à la croisée des chemins des données, de la connaissance et du pouvoir et agit comme un facilitateur de connaissances intrusives et omniprésentes sur les personnes.

(DE): Ausgehend von mehreren und miteinander verflochtenen Paradigmenwechseln, die durch verbesserte künstliche Intelligenz (KI)-Systeme angestoßen wurden, konzentriert sich das Papier auf den grundlegenden Wert der menschlichen Würde und isoliert einen 'entmenschlichenden' Prozess, der durch drei Kanäle fließt: Daten, Wissen und Macht. Es vertieft sich in die Haltung, die die Europäische Union eingenommen hat, um diese Aspekte mittels ihrer neuesten Gesetzgebungsakte (KI-Gesetz, DMA, DSA, Datengovernance-Gesetz, Datengesetz) zu 'rehumanisieren'. Es schließt mit einem interdisziplinären Vorschlag zur Reflexion über Profilierungstechniken, die nicht nur den Ansatz der DSGVO und DSA ergänzen, indem sie kollektive Schutzmaßnahmen einführen, sondern auch die durch das KI-Gesetz unternommenen Lösungen optimieren und die Aktivierung des DMA für die Kombination und die gemeinsame Nutzung von Daten abschließen. Somit wird das angestrebte Ziel einer substanzielleren Verteidigung im Namen der menschlichen Würde und Gleichheit gegen einen Prozess (Profilierung) angesprochen, der an der Schnittstelle von Daten, Wissen und Macht steht und als Ermöglicher von aufdringlichen und allgegenwärtigen Einblicken in Menschen wirkt.

(PT): Partindo de múltiplas e entrelaçadas mudanças de paradigma impulsionadas por sistemas de inteligência artificial (IA) aprimorados, o artigo foca no valor fundamental da dignidade humana e isola um processo 'desumanizante' que flui através de três canais: dados, conhecimento e poder. Aprofunda-se na postura adotada pela União Europeia para 'reumanizar' esses aspectos por meio de seus mais recentes atos legislativos (Lei de IA, DMA, DSA, Lei de Governança de Dados, Lei de Dados). Conclui com uma proposta interdisciplinar de reflexão sobre técnicas de perfilamento que visam não apenas complementar a abordagem adotada pelo RGPD e DSA, introduzindo assim salvaguardas coletivas, mas também otimizar as soluções empreendidas pela Lei de IA e completar a ativação do DMA para combinação e uso cruzado de dados. Assim, o objetivo abordado é a adoção de uma defesa mais substancial em prol da dignidade humana e igualdade, contra um processo (perfilamento) que está na encruzilhada de dados, conhecimento e poder e atua como facilitador de insights intrusivos e pervasivos sobre as pessoas.

(IT): Partendo da molteplici e intrecciati cambiamenti di paradigma innescati da sistemi di intelligenza artificiale (IA) migliorati, il documento si concentra sul valore fondamentale della dignità umana e isola un processo 'disumanizzante' che scorre attraverso tre canali: dati, conoscenza e

potere. Esamina la posizione adottata dall'Unione Europea per 'riumanizzare' questi aspetti mediante i suoi più recenti atti legislativi (AI Act, DMA, DSA, Data Governance Act, Data Act). Conclude con una proposta interdisciplinare di riflessione sulle tecniche di profilazione finalizzate non solo a integrare l'approccio adottato dal GDPR e DSA, introducendo così salvaguardie collettive, ma anche a ottimizzare le soluzioni intraprese dall'AI Act e a completare l'attivazione del DMA per la combinazione e l'uso incrociato dei dati. Pertanto, l'obiettivo affrontato è l'adozione di una difesa più sostanziale a favore della dignità e dell'uguaglianza umana, contro un processo (profilazione) che si trova all'incrocio tra dati, conoscenza e potere e agisce come abilitatore di intuizioni intrusive e pervasive sulle persone.

1. Multifaceted and intertwined paradigm shifts

Since the beginning of the 'new century', law and technology scholars have increasingly been speaking about the coming into existence of a new paradigm or a paradigm shift with respect to consolidated legal categories. This paradigm shift underlies further paradigm shifts that have affected traditional technologies as well as the consequent socioeconomic dynamics [1].

The paradigm shift has been fuelled by technological advancements. In the 1990s, it was the creation of the Internet that brought about a real data deluge [2]. In the 21st century, this worldwide connection was coupled with in-

[1] The perspective adopted by R. BROWNSWORD-E. SCOTFORD-K. YEUNG, *Law, Regulation and Technology. The Field, Frame and Focal Questions*, in R. BROWNSWORD-E. SCOTFORD-K. YEUNG (eds.), *The Oxford Handbook of Law, Regulation and Technology*, Oxford, 2017, p. 3, is telling: «the field of "law and information technology" (sometimes presented as "law and technology")… is one of the extraordinarily dynamic activity in the "world-to-be-regulated" – evidenced by the almost daily announcement of a new technology or application – but also technological innovation puts pressure on traditional legal concepts… and transforms the instrument and institutions of the regulatory enterprise itself».

[2] For the delineators of big data, its 3Vs (volume, velocity and variety) and the addition of further v-words over the years, see R. KITCHIN, *The Data Revolution. A critical Analysis of Big Data, Open Data & Data Infrastructures*, Los Angeles, 2022, p. 61 ff.

creased computing power (according to Moore's law) and new computer algorithms [3]. This process has allowed the passage from the 'good old-fashioned artificial intelligence' (GOFAI) [4], which is characterised by the formalisation of knowledge-based systems [5], to a new framework of learning forms [6]. While the main drawback of the former was linked to the knowledge representation bottleneck, the latter (i.e., machine learning techniques) has overcome this obstacle [7]. It relies upon huge amounts of data and learns from it, extracting by means of data correlation patterns that help to fulfil certain objectives (i.e., narrow artificial intelligence) [8]. The cyberspace is now composed of two en-

[3] As stressed by R. KITCHIN, *op. ult. cit.*, p. 98, «the analysis of very large numbers of data records can only be undertaken in a timely fashion by computer algorithms».

[4] The main shortcoming that affects logical agents that belong to the 'good old-fashioned AI' (GOFAI) is due to the difficulty to capture every contingency of appropriate behaviour in a set of necessary and sufficient logical rules to be formalised and codified in a computer program, see S. RUSSELL-P. NORVIG, *Artificial intelligence – A Modern Approach*, Hoboken, 2021, pp. 981-982.

[5] S. RUSSELL-P. NORVIG, *op. ult. cit*., p. 208, observe that «knowledge-based agents use a process of reasoning over an internal representation of knowledge to decide what action to take».

[6] S. RUSSELL-P. NORVIG, *op. ult. cit*., p. 651, describe that: «an agent is learning if it improves its performance after making observation about the world… When the agent is a computer, we call it machine learning: a computer observes some data, builds a model based on the data, and uses the model as both a hypothesis about the world and a piece of software that can solve problems… There are… three main types of learning: in supervised learning the agent observes input-output pairs and learns a function that maps from input to output… in unsupervised learning the agent learns patterns in the input without any explicit feedback… in reinforcement learning the agent learns from a series of reinforcements: rewards or punishments».

[7] G. SARTOR, *Introduzione*, in *Riv. fil. dir.*, 1/2020, p. 66. As explained also by F.A. RASO-H. HILLIGOSS-V. KRISHANAMURTHY-C. BAVITZ-L. KIM, *Artificial Intelligence & Human Rights: Opportunities & Risks*, in *Berkman Klein Cernter for Internet & Society at Harvard University*, 6/2018, p. 2, «The impossibly large set of technologies, techniques, and applications that fall under the AI umbrella can be usefully classified into two buckets. The first is comprised of *knowledge-based systems*, which are "committed to the notion of generating behaviour by means of deduction from a set of axioms". These include "expert systems" which use formal logic and coded rules to engage in reasoning. Such systems, which are sometimes also called "closed-rule algorithms" … cannot, however, learn or automatically leverage the information they have accumulated over time to improve the quality of their decision-making… The second bucket of technologies uses statistical learning to continuously improve their decision-making performance. This new wave of technology, which encompasses the widely discussed techniques known as "machine learning" and "deep learning" has been made possible by the exponential growth of computer processing power, the massive decline in the cost of digital storage, and the resulting acceleration of data collection efforts».

[8] M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, in M. EBERS-S.

tangled units: a structural unit made up of the Internet connection and a functional unit that entails artificial intelligence (AI) [9]. Broadening the perspective, this technological paradigm shift has also affected scientific research at large by challenging established epistemologies, such as empirical methodologies, and the underlying constraints stemming from theory (upon which the traditional scientific method relies) [10].

In addition, data availability, automated algorithms and computer power have disrupted traditional business models, giving rise to the broad and blurring concept of platform economy. This involves a two-sided market, data as a strategic asset and profiling and targeting techniques [11]. It encompasses a new form of digital-enabled capitalism, known as surveillance capitalism, in which «competitive pressure produced this shift, in which automated machine processes not only *know* our behaviour but also *shape* our behaviour at scale… In this phase… the means of production are subordinated to an increasingly complex and comprehensive "means of behavioural modification"» [12]. Thus, the perception of our personal identity has also been affected, along with the way humans enter relationships and interact with others and with technologies [13]. Scholars argue that this change has determined a further shift towards the beginning of both a new era, called hyper history, and a new faith, called dataism. Hyper history implies that information and data are not only generated, gathered, stored and transmitted but also automatically processed and deployed so that decisions can be taken and human behaviour can be assessed, monitored and foreseen. As a result, the human being is experiencing an onlife

NAVAS NAVARRO (eds.), *Algorithms and Law*, Cambridge, 2019, p. 61, underlines the shift from causation to correlation brought by AI, since «most data mining techniques rely on inductive knowledge and correlations identified within a dataset. Instead of searching for causation between the relevant parameters, powerful algorithms are used to spot patterns and statistical correlations». In a similar way, R. KITCHIN, *op. cit*., p. 98, describes how «machine learning seeks to evolve iteratively an understanding of a dataset: to learn automatically to recognise complex patterns and construct models that explain and predict such patterns and optimise outcomes».

[9] M. MIRTI, *Il cyberspace. Caratteri e riflessi sulla Comunità Internazionale*, Naples, 2021, p. 65.

[10] As recalled by R. KITCHIN, *op. cit*., p. 115.

[11] A. PERUCCI, *L'impatto delle piattaforme digitali sui sistemi economici*, in *mondoperaio*, 11-12, p. 25 ff.

[12] S. ZUBOFF, *The age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, London, 2019, p. 8.

[13] L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milan, 2017, pp. 27 and 69.

within an infosphere made of informations in which both the border between analogue and digital and the border between the personal and social self-blur [14]. In turn, dataism underlines that «humans can no longer cope with the immense flows of data, hence they cannot distil data into information, let alone into knowledge or wisdom», and as a consequence, «the work of processing data should therefore be entrusted to electronic algorithms, whose capacity far exceeds that of the human brain» [15].

The intertwined technological and socioeconomic paradigm shifts that have been recalled have affected the legal system, with the issue addressed by law and technology scholars. Law reflects societal developments since it is an inherently social phenomenon [16]. Moreover, since law historically intervenes in assuring and safeguarding the so-called commons (i.e., preconditions for human social existence), it necessarily deals with the coming of new opportunities and risks brought about by technological developments [17]. More specifically, a «two-way discourse» has taken place: «the law is more and more involved in regulating scientific activities, products and results; at the same time legal intervention is often grounded on expert knowledge and scientific notions and concepts penetrate legal categories» [18]. Consequently, law not only strives to regulate new technologies but, in turn, is shaped by technological advancements in a twofold way: for its content and for the deployed regulatory techniques that evolve according to the different types of technologies and implied risks [19], reaching the possibility of embedding the legal rule in a technological system that automatises its respect [20].

---

[14] L. FLORIDI, *op. ult. cit*., p. 47.

[15] Y.N. HARARI, *Homo Deus. A brief History of Tomorrow*, London, 2015, p. 429.

[16] M. VOGLIOTTI, *Postdiritto: una questione moderna*, in *Riv. fil. dir.*, 2/2023, p. 239 ff.

[17] J. BLACK, *The role of risk in regulatory processes*, in R. BALDWIN-M. CAVE-M. LODGE (eds.), *The Oxford Handbook of Regulation*, Oxford, 2010, p. 314 ff.

[18] E. PALMERINI, *The interplay between law and technology, or the RoboLaw project in context*, in E. PALMERINI-E. STRADELLA (eds.), *Law and Technology – The Challenge of Regulating Technological Development*, Pisa, 2013, p. 13.

[19] A. IANNUZZI, *Il Diritto capovolto – Regolazione a contenuto tecnico-scientifico e costituzione*, Naples, 2018.

[20] R. BROWNSWORD, *Law, Technology and Society – Re-imagining the Regulatory Environment*, New York, 2019, p. 4. The Author describes «technological management… [as] the use of technologies… with a view to managing certain kinds of risk by excluding (i) the possibility of certain actions, which, in the absence of this strategy, might be subject only to regulation, or (ii) human agents who otherwise might be implicated (whether as rule-breakers or as the innocent victim of rule-breaking) in the regulated activities».

Within this broader framework, the peculiarities of Artificial Intelligence (AI) come into play. AI can positively serve society by implementing collective wellbeing and promoting human dignity as well as equality, pluralism, fundamental rights and freedom [21].

However, this is not the scenario with which this paper deals. The seminal goal of a legal system is the protection of human beings from different types of risk [22]; and the original goal of modern constitutionalism was to limit public power and protect the essential values of human dignity and the fundamental principles of equality and pluralism. These aspects are touched upon by the 'value chain' consisting of Big Data and data analytics and their automated deployment within AI systems [23]. Consequently, it will be the anthropological basis of the «homo dignus» that will be addressed so that it can be safeguarded [24]. Some 'dehumanising' [25] processes are currently flowing through different channels. Not only does 'dehumanisation' result from the artificial triggering and steering of the processes but also because they differ in scale and scope from past similar challenges posed by market and technoscience and are featured by the emergence of real pervasive 'private powers' that complement the already existing public powers. In the aftermath, it is this three-tiered 'dehumanisation' that will be tackled with respect to data, knowledge and power.

[21] For a broad understanding of risk and opportunities of new technologies, AI included, see G. SARTOR, *Human Rights and Information Technologies*, in R. BROWNSWORD-E. SCOTFORD-K. YEUNG (eds.), *op. cit.*, p. 424 ff.

[22] As stressed by A. STERPA, *L'ordine giuridico dell'algoritmo: un nuovo ordinamento giuridico*, in A. STERPA (eds.), *L'ordine giuridico dell'algoritmo*, Naples, 2024, p. 9, the legal scholar is requested to verify the impact of technology on human beings.

[23] As for the connection between privacy, personal data protection and the fundamental value of human dignity, see S. RODOTÀ, *Privacy, Freedom and Dignity*, 26th International Conference on Privacy and Personal Data Protection, Wroclaw, 14-16 September 2004, in https://www.garanteprivacy.it.

[24] S. RODOTÀ, *Antropologia dell'«homo dignus»*, in *Riv. crit. dir. priv.*, 2010, p. 547 ff.

[25] As remarked by B. CUSTERS-E. FOSCH-VILLARONGA, *Humanizing Machine: Introduction and Overview*, B. CUSTERS-E. FOSCH-VILLARONGA (eds.) in *Law and Artificial Intelligence. Regulating AI and Applying AI in Legal Practice*, The Hague, 2022, p. 11, «humanizing machines might dehumanize people and encourage poor human decision-making in allocating resource and responsibility».

2. Data dehumanisation

Beyond the debated question about personal data tradability [26], our concern is about additional kinds of data dehumanisation.

Data are more and more artificially generated. They are observed, inferred, derived and synthetically produced by machines [27]. As a consequence, data are more and more machine readable at their source and it is easier for them to be automatically processed and combined in order to determine patterns, predictions, assessments and decisions [28]. Such correlations rely upon mixed data or even non-personal data, but they nonetheless can lead to personal inferences [29]. Thus, it may not be the collection of data that encroaches upon the right to personal data protection but the artificially generated output that entails the mining and extraction of personal features [30]. In other words, it is the 'pluripotent' machine learning system that is able to 'synthetically' produce inferences regarding personal characteristics, interests, status and behaviours. In this respect, «Big Data's processes can generate a predictive model of what has a high probability of being personally identifiable information»; thus, «Big Data has radically expanded the range of data that can be personally identifying» because «prediction… [can be] as personally sensitive as if it had

[26] G. CERRINA FERONI (eds.), *Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione*, Turin, 2024.

[27] For the distinction between observational data, derived, inferred and synthetic data, see the Report for the Data Governance Working Group of the Global Partnership on AI, *The Role of Data in AI*, 16th November 2020.

[28] M.C. CARROZZA-C. ODDO-S. ORVIETO-A. DI MININ-G. MONTEMAGNI, *AI: profili tecnologici. Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'intelligenza artificiale*, in *BioLJ*, 2019, p. 237 ff.

[29] S. CALZOLAIO, *Protezione dei dati personali*, in *Dig. disc. pubbl.*, Aggiornamento, Milan, 2017, pp. 605-606.

[30] According to N. PURTOVA, *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Innovation and Technology*, 1/2018, p. 80, «there is a third option which too deserves a careful consideration, namely, to abandon the concept of personal data as a cornerstone of data protection altogether, and seek remedies for "information-induced harms" – understood broadly as any individual or public negative consequences of information processing – without a sentimental attachment to this familiar proxy. To preserve this formal distinction will always imply that there is also data that is not personal, and while the former triggers legal protection, the latter should not. This duality is at odds with the world where any information has a potential to affect people. Therefore, all information should trigger at least an obligation to assess what impact its processing is likely to have. In this sense, to abandon the formal use of the notion "personal data" amounts to accepting that all data is personal».

been collected or shared inappropriately» [31]. Consequently, beyond our physical identity, we are also bearers of a digital identity shaped by machines [32].

Other aspects of data dehumanisation deal with poor-quality data or discriminatory data. Data are not neutral in their composition or in their outcomes. Either they reproduce cultural and deeply rooted societal beliefs and behaviours, or they are selected according to the beliefs and understanding of those that collect them and, thus, could be biased [33].

On the one hand, data are poor in quality when they lack some essential features that would make them reliable and fit for their purpose. These are cases of underrepresentation, lack of representation or misrepresentation that can lead to the invisibility of certain groups or the characteristics of certain groups according to the motto that only «what gets counted counts» [34]. Thus, the negative impacts of the outcomes of such data primarily fall on those who are the most vulnerable [35]. Since datasets can be affected by different errors and anomalies, different characteristics/dimensions/metrics that vary according to the context of use have been elaborated for improving data quality (in terms of reliability, completeness, accuracy, accessibility, consistency, timeliness and understandability) [36] [37]. Against this backdrop, big data poses new

[31] K. CRAWFORD-J. SCHULTZ, *Big Data and Due process: Towards a Framework to Redress Predictive Privacy Harms*, in *Boston College Law Review*, 1/2014, p. 98.

[32] S. RODOTÀ, *Privacy, Freedom and Dignity*, cit.

[33] As evidenced by A.C. AMATO MANGIAMELI, *Intelligenza artificiale, big data e nuovi diritti*, in *Riv. it. inf. dir.*, 1/2022, p. 93 ff., and by G. MOBILIO, *L'Intelligenza Artificiale e I rischi di una «disruption» della regolamentazione giuridica*, in *BioLJ*, 2020, p. 296, behind the alleged "neutrality" of algorithms and AI, there are both the mindset and errors committed by the technicians and, above all, the interests of Big Tech companies that derive huge profits from the exploitation of these technologies. This "ideological" orientation can also be inscribed within the broader relation between the Global North and the Global South. In this respect, E. TRERÉ, *Data and De-westernization*, in L. DENCIK-A. HINTZ - J. REDDEN - E. TRERÉ (eds.), *Data Justice*, Los Angeles-London-New Delhi, 2022, p. 46, has underlined that a «culturally-bound worldview… can lead to biases in the selection of topics, research frameworks, methods and data interpretation that will be filtered through a Western axiology, epistemology and ontology. In this process, indigenous literary and philosophical traditions and worldviews risk being disregarded, and western contents, visions and conceptualizations uncritically applied».

[34] C. D'IGNAZIO-L.F. KLEIN, *Data Feminism*, Cambridge-London, 2023, p. 97.

[35] L. TAYLOR, *What is data justice? The case for connecting digital rights and freedoms globally*, in *Big Data & Society*, 2017, p. 4.

[36] For data quality requirements, see ISO/IEC 25012:2008; ISO/IEC 25024:2015.

[37] D. ARDAGNA-C. CAPPIELLO-W. SAMÁ-M. VITALI, *Context – aware data quality assessment for big data*, in *Future Generation Computer Systems*, 89, 2018, p. 550.

challenges due to its volume, variety, velocity and the kind of algorithm that runs the system [38]. Traditional data quality dimensions are consistently insufficient to assess big data quality (they are mainly suitable for structured data while big data is mostly unstructured). Moreover, not all metrics yield useful results, while additional dimensions like trustfulness and credibility should be taken into consideration [39]. Scholars have given evidence to the grossly affected outcomes of machine learning algorithms even when the inaccuracy of data is small in scale, which means that «the algorithm degrades so quickly under inaccurate data» [40]. According to the well-known concept of 'garbage in–garbage out' [41], poor-quality data leads to incorrect findings that hinder the consequent decision-making process [42].

Even when a dataset is complete and accurate, it can give rise to direct or indirect discrimination because of the recording of protected attributes (under European Union antidiscrimination law) or proxies for protected attributes (i.e., apparently neutral requirements that could convey special categories of data) [43]. The data used in training the algorithm could also reflect discriminatory human decisions [44]. As denounced by the European Parliament, «algo-

[38] L. BUDACH et al., *The effects of Data Quality on Machine Learning Performance*, in arXiv:2207.14529, 2022, Cornell University.

[39] O. REDA-I. SASSI-A. ZELLOU-S. ANTER, *Towards a data quality assessment in Big Data*, in *ACM International Conference Proceeding Series*, 2020, p. 92.

[40] V. SESSIONS-M. VALTORTA, *The effects of data quality on machine learning algorithms*, in *ICIQ*, 6/2006, p. 485.

[41] As stressed by L. CAI, Y. ZHU, *The challenges of Data Quality and Data Quality Assessment in the Big Data Era*, in *Data Science Journal*, 2/2015, p. 2, «high-quality data… is a necessary condition for generating value from data».

[42] M. TALHA et al., *Big data: Trade – off between Data Quality and Data Security*, in *Procedia Computer Science*, 2019, p. 917.

[43] As stressed by B.H.M. CUSTERS, *Reconsidering discrimination grounds in the data economy: an EU comparison of national constitutions*, in *Computer Law and Security Review*, 2023, p. 2, «Indirect discrimination (i.e., discrimination by proxy) occurs a lot in automated decision-making and profiling. Because there are so many attributes involved in the data analytics, it seems easy to circumvent those attributes that constitute grounds for discrimination. However, when apparently neutral characteristics are correlated to sensitive characteristics, discrimination may occur. A typical example of this is redlining, in which characteristics are ascribed to people on the basis of their zip codes (an apparently neutral characteristic), whereas zip codes may be a strong indicator for someone's ethnic background (a ground of discrimination)».

[44] As explained by the Fundamental Rights Agency, *Big Data: Discrimination in data-supported decision-making*, 2018, p. 5, algorithmic discrimination «happens when the predicted outcome for a particular group is systematically different from other groups and therefore

rithms learn to be as discriminatory as the data they are working with, and, as a result of low-quality training data or biases and discrimination observed in society, might suggest decisions that are inherently discriminatory, which exacerbates discrimination within society» [45]. In a few words, the algorithm transfers into the digital world already existing discrimination perpetrated by the analogue world [46].

These types of data processing activities by themselves bear some 'dehumanising' features that are at odds with the constitutional principles of human dignity, equality and pluralism [47].

3. Knowledge dehumanisation

A further paradigm shift is represented by the displacement of knowledge beyond humans' scope of action and its extension to automated processes.

First, knowledge dehumanisation occurs because AI represents a technological system that for the first time competes with a cognitive ability, traditionally conceived of as an exclusive prerogative of human beings [48]. These self-learning technologies can act with a certain level of autonomy for the attainment of given goals [49]. AI has also proven to outperform human beings in

one group is consistently treated differently to others... This can occur when the data used to train the algorithm include information regarding protected characteristics (e.g. gender, ethnicity, religion). Furthermore, so-called "proxy information" is sometimes included in the data. This may include the height of a person, which correlates with gender, or a postcode, which can indirectly indicate ethnic origin in cases of segregated areas in cities, or more directly, a person's country of birth».

[45] European Parliament Resolution of 3 May 2022 on artificial intelligence in a digital age, point 94.

[46] A. ODDENINO, *Intelligenza artificiale e tutela dei diritti fondamentali: alcune notazioni critiche sulla recente Proposta di Regolamento della UE, con particolare riferimento all'approccio basato sul rischio e al pericolo di discriminazione algoritmica*, in A. PAJNO-F. DONATI-A. PERRUCCI (eds.), *Intelligenza Artificiale e Diritto: una rivoluzione?*, I, Bologna, 2022, p. 192.

[47] See S. RODOTÀ, *Privacy, Freedom and Dignity*, cit.

[48] A. SIMONCINI-S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Riv. fil. dir.*, 1/2019, p. 88: remember that today «artificial intelligence means the ability of machines to reproduce or execute typical operation of human cognitive functions, such as learning, problem solving, face recognition, language translation».

[49] B. CUSTERS-E. FOSCH-VILLARONGA, *op. cit.*, p. 8. The Authors underline that «compared to the previous generation of information technologies, two things are novel about these new technologies. Firstly, these new technologies are capable of *self-learning*, i.e. a process by

achieving certain tasks [50]. This perspective implies delving into the complex domain of mind, thinking and rationality that is beyond our reach, and which instead concerns the domains of philosophy, neuroscience and psychology that, in turn, have evidenced difficulties in drawing clearcut borders and definitions.

Second, knowledge dehumanisation could be articulated along a double-tiered path: information submitted to human beings is more-and-more artificially generated [51]; and we are increasingly exposed to the risk of non-reliable, artificially generated information that we are not able to detect (i.e., fake news, deep fakes). This path undermines the trustworthiness of information and the autonomy of humans in implementing their awareness and adopting consequent decisions.

In addition, human moral agency and self-determination [52] are hindered by what scholars have termed the «overwhelming practical force of the algorithm» [53]. Even in cases in which the artificially generated decision is not aimed at replacing a human decision but only to support it, humans lean towards following the artificially generated output for reasons of practical convenience instead of engaging in complicated research and reasoning to figure out different solutions [54]. The result is a sort of total or partial delegation of cognitive functions that had previously been the exclusive domain of living

which a system takes the initiative without assistance of humans to identify patterns, discover new information, and predict future events with similar data. In this sense, AI is often referred to in one breath with technologies like algorithms, data mining and machine learning… Secondly, and related to the self-learning characteristic, AI can act with a certain level of *autonomy.* This means that AI systems can make decisions themselves, decisions that are not preprogrammed… Higher levels of autonomy usually involve that the technology is assigned with a specific task and can choose the optimum strategy to execute that task».

[50] B. CUSTERS-E. FOSCH-VILLARONGA, *op. cit.*, p. 9.

[51] As highlighted by A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLJ*, 2019, p. 70, human knowledge and understanding, which ground human decisions, are increasingly generated by technological systems with different degrees of automation. Consequently, technology influences human decisions by forming the informational basis of human actions.

[52] S. TIRIBELLI, *La dimensione etica e politica dell'algoritmo*, in A. STERPA (eds.), *L'ordine giuridico dell'algoritmo*, cit., p. 38, refers to the impact and effect of algorithms on the two main pre-conditions of cognitive freedom, which are the availability of different moral options and moral agency (i.e., self-determination).

[53] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, cit., p. 81.

[54] A. SIMONCINI, *op. loc. ult. cit*.

creatures to technological systems [55]. Consequently, this algorithmic-driven knowledge flattens and replaces not only the possibilities of human creative and original thinking [56] but also their pluralism, filtering our thinking within bubbles and echo chambers that implement polarisation in society [57].

Against this background, it is once again human dignity along with self-determination and the personalistic and pluralistic principles that are undermined [58].

4. Power dehumanisation

When big data, data analytics and machine learning algorithms come into play, the possibility of broadening and deepening information and knowledge of people's behaviour increases since these automated techniques can extract, infer and determine correlations and patterns that a human mind can't afford [59].

It is commonly agreed that knowledge and power go hand in hand. Not only is their interplay well described by M. Foucault [60] but it is also common sense that deliberation necessarily involves collection and analysis of data and information [61]. The European Union formally endorsed this stance in its Better Regulation and Better Law-Making approaches, according to which evidence and information allow rules to be designed in a more suitable way to be fit for their purposes, gain effectiveness and deliver output legitimacy [62]. Conse-

[55] A. SIMONCINI, *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC*, 2/2023, p. 8.

[56] K. CHAIKA, *Filterworld. How Algorithms flattened culture*, New York, 2024.

[57] C.R. SUNSTEIN, *#republic. Divided Democracy in the age of social media*, Princeton-Oxford, 2018.

[58] F. BALAGUER CALLEJÓN, *Social network, società tecnologiche e democrazia*, in *Nomos*, 3/2019.

[59] R. KITCHIN, *op. cit*., p. 100, explains that «data mining is the process of extracting data and patterns form large datasets», and he describes (pp. 145 ff.) the new and different insights it provides to businesses and government's knowledge.

[60] M. FOUCAULT, *Surveiller et punir*, in M. FOUCAULT (eds.), *Oeuvres II*, Gallimard, Paris, 2015, p. 261 ff.

[61] A. SIMONCINI, *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti*, cit., p. 23. The Author recalls the motto «to know in order to deliberate».

[62] M. DAWSON, *Better Regulation and the Future of EU Regulatory Law and Politics*, in *Common Mark. LR*, 53/2016, p. 1210.

quently, it goes without saying that the greater the amount of data and information that are held, the more effectively can control and power be exercised.

Against this premise, power dehumanisation takes knowledge dehumanisation a step further. Beyond the automated way of processing data and its potential for interfering in human decision making, it is the locus of deployment of knowledge that has undergone a paradigm shift: Not only does the traditional and well-established *loci* of public power come into play, such as governments or public authorities at large that are deemed to act for the public and collective interest, but also the rise in true 'private powers'.

The struggle between public authorities and the private techno-economic domain to impose their will and power on people is not new, as it was well described by Natalino Irti [63]. However, what is new is both private power's scale and scope of action and the consequent efficacy of the tools at its disposal in targeting people. In this respect, it is the traditional mission of constitutions to limit power that is under strain.

As is known, modern constitutionalism has placed the human being at its core and, thus, the fundamental value of human dignity as well as its relevant equality and personalistic and pluralistic principles. Constitutionalism has consistently introduced limits to the exercise of power to make it a servant to people's welfare. As evidenced by doctrine, not only traditional public powers but also economic power, science and technique were 'caught' by constitutions [64]. According to this perspective, constitutions humanised power, placing it at the service of humans' wellbeing. However, first globalisation and then new disruptive technologies have increasingly undermined this constitutional balance. On the one hand, transnational corporations skipped national territorial borders and gave rise to a system of transnational regulations [65] and governance [66] that embodied a sort of counter-sovereign with respect to traditional and legitimised sovereign nation states [67]. On the other hand, this 'state of the art' has been worsening in the face of the scope and scale of the action of the so-called «lords of the algorithm» [68]. Their power is strengthened and multiplied in respect of classical multinational corporations since it is fuelled by

[63] N. IRTI, *Il diritto nell'età della tecnica*, Naples, 2007, p. 12.

[64] M. LUCIANI, *L'Antisovrano e la crisi delle costituzioni*, in *Riv. dir. cost.*, 1/1996, p. 161.

[65] F. CAFAGGI, *New foundations of transnational private regulation*, in E. PALMERINI-E. STRADELLA (eds.), *Law and Technology – The Challenge of Regulating Technological Development*, cit., p. 77 ff.

[66] M.R. FERRARESE, *Globalizzazione giuridica*, in *Enc. dir.*, agg., IV, Milan, 2011, p. 547 ff.

[67] M. LUCIANI, *op. ult. cit.*, p. 165.

[68] L. AMMANNATI, *I "signori" nell'era dell'algoritmo*, in *Dir. pubbl.*, 2/2021, p. 381 ff.

profiling techniques and targeting strategies. They embody an overwhelming powerful intersection between market and technology, giving rise to real digital giants, that is, Big Techs [69].

Thus, the depicted paradigm shift is both quantitative and qualitative in nature with respect to traditional market forces. First, Big Techs rely upon a huge amount of data and extract value from it; second, the data and their deployment by automated algorithms give Big Techs the potential to influence individual choices, behaviours (i.e., a hypernudge) [70] and public debates that are unprecedented in scale and scope [71].

Not only are these «lords of the algorithm» often steered by the necessity to overcome existing rules [72] and, therefore, protections and safeguards posed in the interest of individual rights and freedoms, but they also exploit nonhuman language (i.e., the language of the machine) for their purposes [73], thereby contributing to dehumanising social relations [74]. Here, the experiment carried out by Facebook is telling, in which two bots started to speak to each other during the training phase in a language that only they could understand [75].

This multiplied power, scaled up by artificially generated insights on people's interests, habits, preferences, opinions and behaviours, has led scholars to call for both an integration of antitrust law with data protection law [76] and a serious reflection on the role of data in a data-driven economy in order to

[69] M. BETZU, *I poteri privati nella società digitale: oligopoli e Antitrust*, in *Dir. pubbl*, 2021, p. 741.

[70] K. YEUNG, '*Hypernudge': big Data as a mode of regulation by design*, in *Information, Communication & Society*, 1/2017, p. 118. The Author observes that (p. 119): «By configuring and thereby personalising the user's informational choice context, typically through algorithmic analysis of data streams from multiple sources claiming to offer predictive insights concerning the habits, preferences and interests of targeted individuals (such as those used by online consumer product recommendation engines), these nudges channel user choices in directions preferred by the choice architect through processes that are subtle, unobtrusive, yet extraordinarily powerful».

[71] In this sense, cfr. O. POLLICINO, *Potere Digitale*, in *Enc. dir.*, agg., V, Milan, 2023, p. 411.

[72] L. AMMANNATI, *op. ult. cit.*, p. 383.

[73] A. SIMONCINI, *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti*, cit.

[74] O. POLLICINO, *Potere Digitale*, cit., p. 410, speaks about a digital power that increasingly lacks a human appearance due to being driven by automated algorithms.

[75] https://www.huffingtonpost.it.

[76] G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Dir. pubbl.*, 2019, p. 89 ff.; M. BETZU, *op. ult. cit.*, p. 753.

promote data sharing, pooling and data quality [77]. Scholars have argued that an evolutive interpretation of competition law in a data-driven economy should broaden the concept of the relevant market (taking into consideration the two-sided market that features the platform economy) [78] and should consequently lead to an evolutionary interpretation of unfair competition that takes into account whether and how the legal duties related to privacy and data protection are fulfilled. In addition, to avoid the abuse of a dominant position that hinders both consumers and other economic operators (due to the lock-in effect), a need for more openness of data has been claimed [79].

5. The EU path towards data, knowledge and power rehumanisation

Since the launch of its strategy on AI, the EU has incessantly asserted the need to preserve a «human-centric» approach [80]. As stated by the European Commission, «In a society where individuals will generate ever-increasing amounts of data, the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules» [81].

By adopting a series of interconnected legal acts, the EU has proven to be aware of the intersection between the three building blocks of the new digital economy and digital society: data, knowledge and power.

a) EU concern about data

The EU has tried to take care of the need to 'humanise' data by dealing with data quality and the removal of data biases.

Drawing on this, the Artificial Intelligence Act (AI Act) has implemented and strengthened the path already outlined by the GDPR [82] and has taken stock

[77] M. BETZU, *op. ult. cit.*, p. 759.

[78] V. ZENO-ZENCOVICH, *do "data markets" exist?* in *Media Laws*, 2/2019, p. 10, provides a reminder that not all data markets are two sided, depending on services that require data for their functioning.

[79] G. DE MINICO, *op. ult. cit.*, p. 99 ff.

[80] COM(2018) 237 final, 12.

[81] COM(2020) 66 final, 1.

[82] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on

of the suggestion delivered by the report of the European Commission's High Level Expert Group on AI [83]. Consequently, a specific Article dedicated to data quality and its governance was introduced in the AI Act.

The GDPR did not delve into the issue of data quality due to its individual rather than collective scope. It made a limited reference to only one dimension of data quality (i.e., accuracy of personal data) in Recital 71, which is not reproduced in its prescriptive provisions. Moreover, this Recital referred to discriminatory effects on natural persons, omitting to deal with the possible inherent biased nature of the collected data. Consistent with this individual stance, the GDPR charged the data subject with the right (and duty) to rectification in case of inaccurate personal data (Article 16). In contrast, the AI Act has adopted a collective approach (i.e., it protects against risks to both individuals and communities, groups or societies at large) and not only prohibits certain practices but also introduces the concept of systemic risk (for General Purpose AI models) and high-risk. As part of this risk-based approach, it has referred to the inherent quality of training, validation and testing of datasets, it has explicitly addressed the purpose of avoiding biases and it has charged providers with the responsibility to comply with requirements and fulfilments in order to uphold data quality [84]. As such, it has proved to be

the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[83] The High Level Expert Group on AI, *Ethics Guidelines for Trustworthy AI*, 2019, 11, 17, underlines that «In an AI context, equality entails that the system's operations cannot generate unfairly biased outputs (e.g. the data used to train AI systems should be as inclusive as possible, representing different population groups). This also requires adequate respect for potentially vulnerable persons and groups, such as workers, women, persons with disabilities, ethnic minorities, children, consumers or others at risk of exclusion». Thus, «The quality of the data sets used is paramount to the performance of AI systems. When data is gathered, it may contain socially constructed biases, inaccuracies, errors and mistakes. This needs to be addressed prior to training with any given data set. In addition, the integrity of the data must be ensured. Feeding malicious data into an AI system may change its behaviour, particularly with self-learning systems».

[84] As explained by Recital No. 44, «The datasets should also have the appropriate statistical properties, including as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used, with specific attention to the mitigation of possible biases in the datasets, that are likely to affect the health and safety of persons, negatively impact fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations ("feedback loops"). Biases can for example be inherent in underlying datasets, especially when historical data is being used, or generated when the systems are implemented in real world settings. Results provided by AI systems could be influenced by such inherent biases that are inclined to gradually increase and thereby perpetuate and amplify existing discrimination, in particular for persons belonging to certain vulnerable groups including racial or ethnic groups».

aware that «discrimination occurs primarily at the process level when the algorithmic model is fed with biased training data» and that «such bias can take two forms. One occurs when errors in data collection lead to inaccurate depiction of realty due to improper measurement methodologies, especially when conclusions are drawn from incorrect, partial or nonrepresentative data… The second type of bias occurs when the underlying process draws on information that is inextricably linked to structural discrimination, exhibiting long-standing inequality» [85].

However, the AI Act presents some shortcomings. While it has limited the scope of the obligations set out in Article 10 to high-risk AI systems, it has failed to provide specifications on what is meant by 'bias' [86]. Instead, it has adopted a functional definition of biases that refer to their negative impact on the safety and health of people, their fundamental rights or discrimination prohibited under EU law [87]. In doing so, Article 10 has enacted a perspective that does not fit the fast-moving world of AI since it has statically and solely mentioned forbidden discrimination pursuant to EU law when further grounds of discrimination brought by new technological changes deserved to have been considered by making a broader reference to unfair decisions [88].

b) EU concern about knowledge

The EU has taken up a clear political option to dismantle the obscurity behind which power, enabled by AI systems, can thrive and threaten individuals. It has implemented some procedural fulfilments that uphold transparency along with some prohibitions. While the former are addressed at improving the knowledge of the recipients of the service or the end users of the system,

[85] M. EBERS, *op. ult. cit.*

[86] M. EBERS-V.R.S. HOCH-F. ROSENKRANZ-H. RUSCHEMEIER-B. STEINRÖTTER, *The European Commission's Proposal for an Artificial Intelligence Act – A critical Assessment by Members of the Robotics and AI Law Society*, in *Multidisciplinary Scientific Journal*, 4/2021, p. 596.

[87] See Recital 44 and Article 10, par. 2(f), of the AI Act.

[88] B.H.M. CUSTERS, *Reconsidering discrimination grounds in the data economy: an EU comparison of national constitutions*, cit., p. 10. «Data science and related technologies are developing very fast, making it hard to predict which new grounds of discrimination will become relevant in the near future. Legislators will probably always have difficulties keeping pace with these developments»; thus, the Author suggests «a paradigm shift, in which anti-discrimination law is no longer based on lists of discrimination grounds, but rather on unfair decisions… This approach puts more emphasis on the vulnerability of people when offering protection. These vulnerabilities stem from the different economic, social, cultural, and institutional relationships that people are in and influence their opportunities».

making them better able to understand the dynamics in action and better aware of the implied risks, the latter are addressed to cutoff at the root the possibility of gaining intrusive knowledge about people.

The AI Act (Article 52) introduces duties of transparency for providers and deployers of AI systems for outputs synthetically generated or manipulated and for artificial systems that interact with persons or recognise their emotion or biometric features to make a natural person aware of the artificial nature of the products or the process in action. In addition, the AI Act provides a list of prohibited AI practices aimed at protecting human dignity and, hence, autonomous agency and equality of treatment with specific regard to pervasive monitoring and influencing practices [89]. However, pursuant to the AI Act, profiling techniques do not fall under the cover of prohibitions, as they are rather categorised as high risk, without the possibility of reverse burden of proof (Article 6, par. 3) in the case of non-significant harm. The EU legislature considered the opinion of the European Data Protection Supervisor (EDPS) in two cases that seriously threatened human dignity and the principle of equality. Pursuant to the EDPS' opinion, predictive policing systems were switched from high risk (as in the original proposal) to forbidden AI practices (in the final text); in addition, the scope of the forbidden social scoring practices was broadened beyond those carried out by public authorities or on their behalf. In this regard, the EDPS categorically denounced that «these uses of AI are so intrusive and affecting human dignity that they should be prohibited» [90].

The Digital Services Act (DSA) [91] not only imposes upon intermediary service providers the requirement of clear identification of advertising (including its features: Article 26) and clear and understandable notice of the main parameters of recommender systems (Article 27) but also introduces certain prohibitions. First, it forbids service providers to present advertisements to recipients of the service based on profiling that makes use of special categories of

[89] For instance, Article 5 lists (among others) the following prohibitions: (1) when AI systems have the objective or the effect of materially distorting a person or group of person's behaviour in a manner that causes or is likely to cause them significant harm (also should this occur by exploiting vulnerabilities); (2) biometric individual categorisation based on biometric data in order to derive or infer certain sensitive data; (3) social scoring leading to detrimental treatment in unrelated context or disproportionate treatment; (4) real time remote biometric identification systems in publicly accessible spaces for purpose of law enforcement (with exceptions); and (5) profiling of persons for predictive policing.

[90] Opinion 44/2023 of the EDPS on the AI Act.

[91] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

personal data referred to in Article 9(1) of Regulation (EU) 2016/679 (Article 26, par. 3); second, it prohibits targeting minors with advertisements based on profiling (Article 28); third, it prevents providers from designing, organising or operating their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions (Article 25). The EDPS actually urged stricter provisions: the prohibition of recommender systems based on profiling, the prohibition of targeted advertising on the basis of pervasive tracking and the prohibition of content moderation based on profiling [92].

The Digital Market Act (DMA) [93] forbids a series of data processing practices that match personal and nonpersonal data of different origin because it multiplies the profiling potentiality and insights gained by gatekeepers on data subjects or business competitors [94].

By means of these provisions, the EU strategy result is twofold. First, it has implemented some prohibitions on certain surveillance, monitoring and influence practices (for instance, real-time remote biometric identification for law enforcement, the deployment of subliminal techniques, emotion recognition in the workplace and educational institutions [95], deceptive or manipulatory online interfaces [96] and cross use and combination of vast amounts of data [97]). It has also enhanced transparency requirements to increase end users' awareness before automated processing (for instance, evidence of the features of advertisements or recommender systems [98], technical documentation, record keeping of events and provision of information [99]). The EU legislation has laid down new procedural obligations (according to a due process perspective) [100], as such adopting a policy stance that is consistent with the general principles

[92] Opinion of the European Data Protection Supervisor on the Proposal for a Digital Services Act (2021/C 149/03).

[93] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[94] See Articles 5-6, DMA.

[95] Cfr. Article 5 of the AI Act.

[96] Cfr. Article 25 of the DSA.

[97] Cfr. Articles 5-6, DMA.

[98] Cfr. Articles 26-27 of the DSA.

[99] Cfr. Articles, 11,12, 13, 53 of the AI Act.

[100] On the intertwined and mutual supportive relationship between procedural obligations and substantial rights, O. POLLICINO, *Potere Digitale*, cit., p. 440.

of administrative law that feature the «global polity» within which Big Techs operate [101]. The underlying goal is to 'catch up' with procedural practices with which these global corporations are familiar in order to gain compliance with and effectiveness of the (also extra-territorial) scope of action of the EU provisions.

In summary, the path paved by the European Union can be described like this: increasing people's autonomous knowledge, awareness and understanding against the pervasiveness of an artificially empowered knowledge.

c) EU concern about power

The EU has supported more data openness and data sharing by limiting and monitoring both the economic position on the market of intermediary service providers and its main source (i.e., data collection and deployment).

First, the EU has intervened to avoid unfair competition grounded on data collection and deployment. According to the Communication on EU Digital Future, the addressed aim is «a fair and competitive economy: a frictionless single market, where companies of all sizes and in any sector can compete on equal terms, and can develop, market and use digital technologies, products and services at a scale that boosts their productivity and global competitiveness, and consumers can be confident that their rights are respected» [102]. Consequently, reflection on the fitness of the existing antitrust remedies and a revision of the market definition are underway: as a result, more suitable legal provisions have been implemented for new digital business models fuelled by service 'freely' accessed by users in exchange for their data.

This standpoint gave birth to the Digital Market Act (DMA) and the Digital Services Act (DSA), which were enacted for the intended purposes of promoting fair competition, according to both, a business-to-business and a business-to-consumer perspective. Both regulations scale up constraints according to the dimensions of the market players by giving relevance (further than quantitative parameters, like turnover) to the number of end or business users and the consequent relevant amount of data they process. Moreover, data access is fostered to data that is generated by businesses or end users but is held by platforms [103].

[101] In reference to the rise of a rule of law and of due process beyond states (with rules made of transparency, participation, accountability) and, more specifically, in international and transnational relations, see S. CASSESE, *Chi governa il mondo?* Bologna, 2013, 43 ff.

[102] *Shaping Europe Digital Future*, February 2020, 4.

[103] Cfr. Article 6, parr. 8-11 of the DMA. The DSA supports data access for competent authorities and researchers (Article 40).

The DMA reshapes the concept of unfair practices and gives relevance to the specificities of the data-driven market. It introduces the definition of gatekeeper, whose peculiar position is not only determined by economic indicators and the provision of core platform services but also by «network effects and data driven advantages, in particular in relation to that undertaking's access to, and collection of, personal data and non-personal data or analytics capabilities» as well as the consequent lock-in effect [104]. This act is aimed at safeguarding the «contestability» [105] and «fairness» [106] of the market: as such, it encompasses both the ex-post approach typical of antitrust regulation and the ex-ante approach typical of electronic communications and essential facilities protection [107]. Consequently, it introduces certain obligations for gatekeepers that are addressed to limit their possibility to process, combine and cross use vast amounts of data to ensure the protection of end users' personal data (these practices are forbidden pursuant to Article 5, except when specific consent is given) and business users' data (Article 6 prevents gatekeepers from using, in competition with business users, any non-publicly available data that is generated or provided by those business users or their customers).

The European Court of Justice has further underpinned this approach. In its adjudication of 4 July 2023 [108] following a preliminary reference brought by the Düsseldorf Regional Court against Meta Platforms Inc., it stated that:

(1) «access to personal data and the fact that it is possible to process such data have become a significant parameter of competition between undertakings in the digital economy. Therefore, excluding the rules on the protection of personal data from the legal framework to be taken into consideration by the com-

[104] Cfr. Article 3, DMA.

[105] According to Recital No. 32, «For the purpose of this Regulation, contestability should relate to the ability of undertakings to effectively overcome barriers to entry and expansion and challenge the gatekeeper on the merits of their products and services. The features of core platform services in the digital sector, such as network effects, strong economies of scale, and benefits from data have limited the contestability of those services and the related ecosystems… This Regulation should therefore ban certain practices by gatekeepers that are liable to increase barriers to entry or expansion, and impose certain obligations on gatekeepers that tend to lower those barriers».

[106] According to Recital No. 33, «For the purpose of this Regulation, unfairness should relate to an imbalance between the rights and obligations of business users where the gatekeeper obtains a disproportionate advantage».

[107] M. OROFINO, *Il Digital Market Act: una regolazione asimmetrica a cavallo tra diritto della protezione dei dati e diritto antitrust*, in F. PIZZETTI (eds.), *La regolazione europea della società digitale*, Turin 2024, pp. 176-177 and 183.

[108] C-252/21, Meta Platforms Inc. vs. Bundeskartellamt.

petition authorities when examining an abuse of a dominant position would disregard the reality of this economic development and would be liable to undermine the effectiveness of competition law within the European Union» [109];

(2) thus, a national competition authority when assessing an abuse of dominant position may take into consideration all relevant circumstances, included compliance or non-compliance with the GDPR provisions [110];

(3) this does not entail a replacement of competence of data protection supervisory authorities, since national competition authorities are requested to cooperate (in compliance with the duty of sincere cooperation provided in Article 4, par. 3, TEU) by consulting the former when the same or similar conduct has not yet been decided by them and adhere to the delivered decision [111].

The DSA protects recipients of online services against unfair clauses set out by an intermediary; in a more systemic approach, it also forbids deceptive online interfaces (Article 25) and promotes transparency of the functioning of content moderation (Articles 14–17), advertising (Article 26) or recommender systems (Article 27) [112].

To complement these Acts and pursuant to the approach taken with the European Data Strategy [113], the EU has started to push towards more data openness and data sharing for the purpose of «making more data available and improving the way in which data is used» [114]. The goal addressed is represented by the creation of «a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint. It should be a space where EU law can be enforced effectively, and where all data-driven products and services comply with the relevant norms of the EU's single market» [115].

[109] C-252/21, par. 51.

[110] C-252/21, par. 47.

[111] C-252/21, parr. 53-63.

[112] As stressed by doctrine, the real step further taken by the DSA with respect to the previous e-commerce Directive is represented by the establishment of a clear and balanced set of due diligence obligations for providers of intermediary services: M. OROFINO, *op. ult. cit.*, p. 143.

[113] COM(2020) 66 final: *A European Strategy for Data*.

[114] COM(2020) 66 final, 3.

[115] COM(2020) 66 final, 5.

Along this path, the EU has adopted the Data Governance Act [116], the Data Act [117] and the rollout of Common European Data Spaces [118]. The Data Governance Act (taking the Open Data Directive a step further) [119] deals with opening public sector data and introduces the concepts of data altruism and data intermediary. The Data Act addresses the private sector, more specifically, data generated by connected devices, supporting sharing between data holders and data users as well as with third parties (according to a business-to-business and a business-to-consumer perspective) to overcome the lock-in effect and foster data portability across different economic operators (making the switch between different data processing providers easier) [120]. Additionally, it forbids unfair contractual terms regulating access to and the use of data or regulating liability and remedies. It also ensures that if there is an exceptional need, data holders make available to public sector bodies the data that are necessary for the performance of a specific task carried out in the public interest (Chapter V).

In summary, the EU has tackled digitally enhanced power at its roots by limiting data deployment and boosting data sharing.

[116] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

[117] Regulation (EU) 2023/2854 of the European parliament and of the council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

[118] https://digital-strategy.ec.europa.eu.

[119] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. This Act regulates the re-use of publicly available information held by the public sector; thus, it does not involve **protected data** (i.e., personal data and commercially confidential data).

[120] As stated by Recital No. 6 of the Data Act: «Data generation is the result of the actions of at least two actors, in particular the designer or manufacturer of a connected product, who may in many cases also be a provider of related services, and the user of the connected product or related service. It gives rise to questions of fairness in the digital economy as the data recorded by connected products or related services are an important input for aftermarket, ancillary and other services. In order to realise the important economic benefits of data, including by way of data sharing on the basis of voluntary agreements and the development of data-driven value creation by Union enterprises, a general approach to assigning rights regarding access to and the use of data is preferable to awarding exclusive rights of access and use. This Regulation provides for horizontal rules which could be followed by Union or national law that addresses the specific situations of the relevant sectors».

d) A common level playing field

The AI Act, DMA, DSA, Data Governance Act and Data Act have made a leap forward in coping with data, knowledge and power compared to the individualistic perspective of the GDPR.

Rather than embarking on the conferral of new rights in favour of individuals (as done by the GDPR), the regulatory technique adopted by the EU has enshrined a series of duties (prohibitions, requirements or fulfilments) addressed at making more transparent and controlled the margin of manoeuvre for those in power. In doing so, these acts have merged the regulatory techniques usually deployed in different sectors, such as product safety, telecommunication and fundamental rights protections.

In addition, the EU has traced a path along which data start to be conceived as 'new commons' that should not remain closed within powerful data domains. Starting from data quality and governance requirements, it has also consistently fostered data sharing and pooling as a trigger for further limiting the concentration of data in the hands of a few centres of power.

As such, the EU has proven awareness of both the far-reaching scale and scope of action of the power that deploys artificial intelligence systems and can affect not only individuals but also entire groups, civil society and civic debate [121] and the consequent collective relevance of the values at stake that involve human dignity, equality, fundamental principles and fundamental rights.

In summary, the EU has recognised that data stand at the roots of the entanglement between knowledge and power; they are the enabler and enforcer of both. In addition, when data are deployed by AI techniques, the potential for harmful results increases. This is the reason the EU has focused on data in terms of both inherent quality and availability. It has tried to tackle asymmetries in the representation of people, groups or communities that can result in

[121] The DSA uses the concept of systemic risks (Article 34, par. 1, b) in reference to «actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter», as well as in relation to civic discourse and electoral process. In parallel, the AI Act prohibits certain artificial intelligence practices not only when they cause or are likely to cause a significant harm to a single person but also to groups of persons (Article 5). The AI Act also refers to systemic risk for general purpose AI.

unfair treatment and discrimination due to data biases, and it has tried to cope with knowledge and power asymmetries that are due to asymmetric data ownership.

6. Introducing data justice

Drawing on the discussion to this point, it seems that a last paradigm shift could be claimed: a legal stance regarding the concept of data justice. This is a notion that has been developed by social scientists who have given evidence of multiple asymmetries [122] fuelled over the years by data processing practices [123]. In substance, it addresses the same risks that the European Union is now tackling by means of its recent legislative acts focused on the data-driven economy and society.

Data justice has dealt with the issue of data ownership and, thus, with the concentration, accumulation and exploitation of data by economic operators or governments and governmental agencies by warning and calling for more democratic, participative and shared data control and data deployment [124]. It has also dealt with data and algorithmic biases and, thus, asymmetries in the representation of subjects, groups or communities that can result in unfair treatment and discrimination [125]. The Data Harm Record of the Data Justice Lab at Cardiff University has provided evidence that harmful consequences for people not only stem from biased datasets but also from the addressed purposes: «the range of examples detailed across the Data Harm Record reinforce our need to address the fact that the problem identified are not simply the result of biased datasets or algorithms not working as intended; instead, the harms identified are connected to the inequality and power imbalances that pervade our societies. The harms detailed… are manifestations of the structural violence that is rooted across our commercial, governmental, societal and political processes» [126]. Consequently, non-benign purposes can stem from different factors: the tasks entrusted to the algorithm, the context within which

[122] A. HINTZ, *Data and policy*, in L. DENCIK-A. HINTZ-J. REDDEN-E. TRERÉ (eds.), *Data Justice*, Los Angeles-London-New Delhi, 2022, p. 103.

[123] R. KITCHIN, *op. cit*., p. 285 ff.

[124] L. DENCIK, *Data and Capitalism;* J. REDDEN, *Data and Governance*, in L. DENCIK-A. HINTZ-J. REDDEN-E. TRERÉ (eds.), *Data Justice*, cit., p. 11 ff.

[125] C. D'IGNAZIO-L.F. KLEIN, *op. loc. ult. cit*.

[126] J. REDDEN, *Data Harms*, in L. DENCIK-A. HINTZ-J. REDDEN-E. TRERÉ (eds.), *Data Justice*, cit., p. 61.

it is used or the malicious or harmful goals pursued with the deployment of the outcomes delivered by the algorithm [127].

Similar issues have been intersected by some legal scholars who call for digital humanism [128], digital constitutionalism [129] and the constitutional dimension of antitrust provisions [130]. These scholars foster not only on the need to safeguard but also to promote human dignity, putting the person at the core and making datafication, algorithms and computational systems (in a word, AI) revolve around the person. To address this purpose, they share the common objective of making the rule of law operational in both dimensions, not only vertically (towards public authorities) but also horizontally (towards economic operators), to limit the powers that big data and its automated analysis have considerably strengthened in scope, scale and efficacy. According to part of the doctrine, the introduction of procedural rules (i.e., due process) along this path underlies much more than mere formal safeguards [131]. First, procedural rules integrate a common playing field for both public and private powers. Second, unlawful procedures (with particular regard to personal data collection and processing) can also gain relevance for antitrust goals. Third, ex-post interventions can be complemented by ex-ante obligations addressed, according to a by-design and by-default approach (well-known since the GDPR) [132], to minimise the risk of the occurrence of harm. Thus, procedures are not only formal steps to be complied with but substantial guarantees when they support disclosure, transparency, accountability and certainty, which are not only general principles of administrative law but also substantive civic values.

However, the data justice perspective calls on further intervention. Well in line with our premise aimed at preserving the anthropological basis of the

[127] A. HINTZ, *Data and citizenship*, in L. DENCIK-A. HINTZ-J. REDDEN-E. TRERÉ (eds.), *Data Justice*, p. 74 ff.

[128] E. CELESTE-G. DE GREGORIO, *Digital Humanism: The Constitutional Message of the GDPR*, in *Global Privacy Law Review*, 1/2022, p. 4 ff.

[129] O. POLLICINO, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, No. 3/2023, pp. 569 ff.

[130] M. BETZU, *op. ult. cit*., p. 753.

[131] O. POLLICINO, *Potere Digitale*, cit., p. 440.

[132] L. CALIFANO, *Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali* (pp. 34 ff.) and S. CALZOLAIO-L. FEROLA-V. FIORILLO-E.A. ROSSI-M. TIMIANI, *La responsabilità e la sicurezza del trattamento* (pp. 137 ff.), both in L. CALIFANO-C. COLAPIETRO (eds.), *Innovazione tecnologica e valore della persona – Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Naples, 2017.

«homo dignus» [133], our concern is addressed to automated profiling [134] due to its inherent discriminatory nature and its potential intrusiveness and pervasiveness with respect to entire groups of people. This is the aspect with which we deal in our conclusive remarks and as a trigger for further interdisciplinary dialogue and research.

7. Taking AI profiling techniques a step further

Before entering the issue of profiling, some underlying aspects should be borne in mind. Nowadays, people are bearers of millions of data [135], and consequently, scholars have argued that a real datafication of individuals is coming into existence [136]. More specifically, a three-tiered datafication process has been highlighted: from raw data produced by our truly «walking data generators» [137], passing throughout the automated analytics run by machines and ending with information extracted and mined by them [138]. People are made object of calculations, correlations and inferences, and on the basis of these, they are profiled, grouped and clustered [139]. «Through our interactions with the ma-

[133] S. RODOTÀ, *Antropologia dell'«homo dignus»*, cit.

[134] As evidenced by doctrine, profiling is an automated process technique driven by statistical inferences. It applies certain data and features to people to categorise (cluster) them in order to assess personal caracteristics and make forecasts: see O. SESSO SARTI, *Profilazione e trattamento dei dati personali*, in L. CALIFANO-C. COLAPIETRO (eds.), *Innovazione tecnologica e valore della persona – Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, cit., p. p. 585.

[135] V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Media Laws*, 2/2018, p. 32.

[136] S. RODOTÀ, *Privacy, Freedom and Dignity*, cit., refers to the concept of «electronic body». In addition, on 'datafication' of individuals in the age of Big Data, see *ex plurimis*, S. RODOTÀ, *Data Protection as a Fundamental Right* in S. GUTWIRTH-Y. POULLET-P. DE HERT (eds.), *Reinventing data protection?*, Berlin, 2010, p. 77 ff.; B. VAN DER SLOOT, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"*, in *Utrecht Journal of International and European Law*, 2015, p. 25 ff.

[137] As evidenced by S. CALZOLAIO, *Protezione dei dati personali*, cit., p. 598, due to the continuous interaction with connected technological devices, every human being produces – consciously or not – an increasing amount of data that is different in type and nature.

[138] S. CALZOLAIO, *Protezione dei dati personali*, cit., p. 599.

[139] B. CUSTERS-E. FOSCH-VILLARONGA, *op. ult. cit.*, p. 8; recall that «generally, an algorithm is a sequence of computations or instructions. As such, it can be applied to data for performing calculations, data processing, or automated reasoning… Data mining technologies focusing on regression, clustering, and classification to find patterns in large datasets usually

chines that surround us – such as cameras, GPS, smart shoes, DNA chips, face-recognition technologies, Internet search engines and smart cars – we are being digitally measured» [140]. Thus, data contributes to shape us and are constitutive; and data generation, analysis and interpretation have consequences on us since «more and more aspects of everyday life become digitally mediated…, being [them] routinely monitored in a continuous, automated fashion» [141]. This has led to a further shift from humans as subjects of rights to humans as objects of machine measurements for classification, assessment and prediction [142].

It should also be borne in mind that profiling practices are discriminatory in and of themselves [143]: when the algorithms run on huge amounts of data and select certain features rather than others in order to create their models (this is a first discrimination in so far as certain attributes are selected by the statistical correlations found by the algorithm and consequently 'artificially' deemed more significant); and when individuals are grouped within clusters due to these previously selected correlations [144].

Against these processes of datafication and profiling, a novel right has been envisioned by doctrine: a right to not be measured, analysed or e-coached [145]. However, since profiling techniques prove to be more-and-more intrusive, granular and spread, an individualistic approach (like that carried out by the

make use of algorithms, but these algorithms do not evolve automatically. However, the algorithms can also be designed in such a way that they autonomously improve themselves through learning processes».

[140] R. VAN EST, J. GERRISTEN, *Human rights in the robot age. Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality*, Report commissioned by the Parliamentary Assembly of the Council of Europe, 2017, p. 14.

[141] R. KITCHIN, *op. cit*., p. 200.

[142] With respect to profiling and the consequent need to shift from the individualistic approach of the GDPR to a collective approach, see A.C. DI LANDRO, *Big Data. Rischi e tutele nel trattamento dei dati personali*, Naples, 2020, p. 97 ff.

[143] On profiling as a new form of algorithmic discrimination beyond the traditional direct and indirect discrimination provided by EU anti-disrimination law, see C. NARDOCCI, *Quando "manca" il giudice… il Garante della Privacy, l'algoritmo e la profilazione*, in *Forum Quad. cost. – Rass.*, 4/2021, p. 30 ff.

[144] B. PARENZO, *Profilazione e discriminazione. Dal GDPR alla Proposta di Regolamento sull'IA*, in *Tecnologie e Diritto*, No. 1/2023, 106-107, gives evidence to the double discrimination that underlie profiling practices.

[145] R. VAN EST, J. GERRISTEN, *op. ult. cit*., p. 44. In relation to profiling, B.H.M. CUSTERS, *New digital rights: Imagining additional fundamental rights for the digital era*, in *Computer Law & Security Review*, 2022, p. 9, has called on a right to start over with a clean digital slate.

GDPR and the consequent entitlement of individual rights) is no longer enough.

Big data analytics – within AI systems that are usually deployed by online services providers, platforms and gatekeepers – work on vast amounts of data. Thus, the relevant processing activities are often out of reach of the single data subject that is not able to minutely follow and eventually correct the steps run by algorithms that work on mass amounts of data throughout complicated automated procedures [146]. On the other hand, profiling can also not involve the collection of personal data, thus discarding the need for consent of the data subject, since «AI techniques can be used to discover some of our most intimate secrets by drawing profound correlations out of seemingly innocuous bits of data» [147] . Thus, whether the consent that makes data processing lawful is given or no personal data are involved, personal features may come out in the aftermath due to the combination and cross use of huge amounts of data by means of automated techniques [148].

As a consequence, it is not so much a matter of protecting personal data in the input phase, with respect to which the GDPR already sets out significant rules for free and aware consent, but rather increasing the protection of people from the possibility that whatever kinds of data (personal or not) are involved, they are heavily profiled and categorised and, thus, included in clusters that stuck them in «too narrow clothes» that can «become like a prison» [149]. Similarly, it is not so much a matter of protecting the single natural person according to the perspective well-implemented by the GDPR, but rather protecting

[146] F. MARASÀ, *Intelligenza artificiale e tutela dei dati personali. Quali riflessi sulla giustizia predittiva?*, in *Oss. dir. civ. comm.*, 1/2023, p. 94. The author underlines the difference between the GDPR concern for profiling, which is based on a direct and personal relationship between the data subject and the data controller, and the profiling carried out by artificial intelligence systems in which a huge mass of data is processed in order to infer abstract and general behavioural models within which a person is categorised without the possibility of this person to oversee and act on the underlying amount of data and the way it is processed by automated algorithms.

[147] F.A. RASO-H. HILLIGOSS-V. KRISHANAMURTHY-C. BAVITZ-L. KIM, *op. cit.*, p. 7. The authors also underline that «even if techniques such as differential privacy are used to protect the privacy of particular individuals, AI technologies may generate insights from such data that are then used to make predictions about, and act upon, the intimate characteristics of a particular person – all while refraining from identifying the natural person».

[148] For the distinction between information that relates to a person in content, purpose or result, see N. PURTOVA, *op. cit.*, p. 54.

[149] R. DE MEO, *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 3/2013, p. 604.

entire groups of persons due to the pervasiveness of profiling and its inherent and intrinsic discriminatory nature, following the substantial approach suggested by data justice scholars [150].

Against this background, it seems that the current EU legislation does not pay sufficient attention to the collective scope assumed by profiling techniques enabled by AI systems and, consequently, does not provide sufficient safeguards. This legislation evidences a fragmented approach to profiling practices that can no longer be reduced to the individual dimension of the data subject entrusted with the dynamic protection of his or her data [151].

Due to the collective scale and scope of profiling, more public policy engagement would have been helpful to better protect the high level of exposition that people undergo in a world where everything is digitalised and, consequently, intrusive automated calculations related to individuals and groups are made possible. Such an approach takes up one of the claims advanced by data justice scholars when they evidence how profiling skips data subject oversight, skips the individualistic perspective and circumvents the GDPR's scope since it deals with the relational and population-level dimension of data. This is the reason data justice scholars have called on «reconceptualization from securing individual rights to recognizing and institutionalizing collective ordering» [152].

Despite this, the DSA, DMA and the AI Act still rely upon the definition of profiling given by Article 4, point 4 of the GDPR that focuses on personal data processing 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 DMA seems to be willing to broaden the concept of profiling when it makes explicit reference in Recital 72 to «profiling practices employed by gatekeepers, including, but not limited to, profiling within the meaning of Article 4, point (4), of Regulation (EU) 2016/679». However, it does not repeat the statement in its prescriptive text, and in any case, it limits these «profiling practices» that overcome the scope of profiling pursuant to Article 4, point 4 of the GDPR to a market-oriented perspective in order to foster the contesta-

[150] As denounced by A. HINTZ, *Data and Citizenship*, cit., p. 80, this automated and algorithmically driven data processing can lead to «categorizations or "stories" that we may not recognize or identify with».

[151] Scholars had observed this long before, see R. DE MEO, *op. ult. cit.*, p. 591.

[152] A. HINTZ, *Data and Policy*, in L. DENCIK-A. HINTZ-J. REDDEN-E. TRERÉ (eds.), *Data Justice*, cit., p. 104.

bility of core platform services by other undertakings. It also introduces some limits to the practices that are at the basis of profiling, such as combining and cross-using end-users' personal data collected from different services (also from third-party services), but this prohibition not only solely concerns the input of personal data and – as a consequence – can be derogated by consent of the data subject, it is also conceived – once again – according to a pure market perspective: in order to promote fair competition and the contestability of core platform services (Article 5) rather than protecting individuals and groups from profiling techniques themselves.

The DSA prohibits profiling based on the personal data of minors (Article 28) or on special categories of personal data referred to in Article 9(1) of the GDPR (Article 26, par. 3). However, it introduces these prohibitions only in reference to online targeted advertising and limits the protection of adults to the case of special categories of personal data. The protection provided for profiling on the basis of which the recommender systems run is also limited to transparency duties with respect to the «main parameters» involved, the consequent possibility of the recipient of the service to change them (Article 27) and, in reference to very large online platforms and search engine, the possibility of the recipient to opt-out the profiling system (Article 38).

The AI Act classifies profiling as a high-risk practice. It declares that an AI system implies profiling that is «considered to pose significant risks of harm to the health, safety or fundamental rights of natural persons» [153]. However, as in the DMA and DSA, it limits profiling within the boundaries of Article 4, point 4, of the GDPR, that is, focusing on personal data. Even if it goes beyond the mere individual protection typical of the GDPR in order to cope with risks to entire groups, it does not fully engage with the far-reaching potential pervasiveness and intrusiveness of profiling and the consequent harm to human dignity and equality that are at the basis of the enjoyment of rights and freedoms as a whole. As dealt with in the previous paragraphs, the AI Act forbids certain deceptive and manipulative practices, some of which can underlie profiling (Article 5, par. 1, points a, b); however, it bonds the prohibition in a twofold way: the objective or effect of distorting human behaviour and decisions; and the probability to cause significant harm. Along the same path, the AI Act prohibits profiling when it is addressed to social scoring practices, and in this case, it broadens the concept of profiling beyond the GDPR definition [154]. Nonetheless, it makes the prohibition conditional upon causing detri-

[153] Recital No. 53.

[154] More specifically, Article 5, par. 1, point c), refers to inferred and predicted personal or personality characteristics.

mental or unfavourable treatment that is disproportionate and unjustified or adopted in unrelated contexts (Article 5, par. 1, point c). It forbids the categorisation of people but only if based on biometric data aimed at deriving or inferring special categories of information (Article 5, par. 1, point g); furthermore, it explicitly prohibits profiling but limits this within criminal law enforcement (Article 5, point 1, d).

As such, the AI Act evidences its struggle to figure out all the different kinds of applications and harmful consequences of profiling techniques. In doing so, it creates tremendous legal uncertainty about the scope of such provisions. It could have streamlined and increased legal certainty by directly addressing profiling practices themselves, since it is the intrusiveness and pervasiveness attained by certain profiling techniques that already represents a threat to human dignity and moral agency. Along this way, the AI Act would have approached the issue upstream, at its root cause, since profiling works as an enabler of many practices forbidden under Article 5 as well as some practices qualified as high-risk by Annex III.

More specifically, the AI Act could have enshrined a clear and substantial political message: If profiling stands at the roots of many harmful AI enabled practices, the first statement should have been its prohibition. Derogation should have come secondarily and upon the fulfilment of certain conditions. Thus, the prohibition should not be considered absolute to avoid stifling positive technological developments and innovation or certain public interest and public order needs.

Stated like this, the core issue that makes profiling fall under prohibition relates to its technical features due to their potential intrusiveness against the full respect of human dignity and equality. Some quantitative parameters could be defined to be consistent with the streamlining goal and, as such, introduce legal certainty and avoid the red tape that hinders investment and businesses, as was done in the AI Act for the presumption of systemic risks for general purpose AI models when it refers to «cumulative amount of compute» (Article 51, par. 2). For profiling, the focus could shift to indicators and methodologies that take into consideration the amount of data, the combination of different data sets or sources of data, their variables, their cross use, the level of complexity of the deployed algorithms and, thus, the different techniques, parameters and metrics involved [155] and the length of the period for which they are employed. To further foster flexibility and streamlining, the

[155] For instance, regression, cluster analysis, decision tree induction or Bayesian networks. For a broad overview, see KITCHIN, *op. cit.*, p. 100 ff.

updating of such indicators according to technological developments and algorithmic improvements could be entrusted to the implementing acts of the European Commission.

In a few words, only profiling practices that are long lasting and run on sophisticated algorithms that work on combinations and the cross use of many kinds of datasets and variables should be covered by the prohibition due to their potential for intrusive insights on personal aspects of entire groups of people. The provider or deployer could be allowed to overcome the presumption of intolerable risks by proving that despite surpassing these technical and quantitative thresholds, profiling does not give rise to intrusive insights on people. In addition, explicit derogations may be introduced by national statutes provided that certain legitimate interests prevail, such as reasons of public security, public policy, public health and fundamental rights protection.

In adopting such a stance, the AI Act would have broadened Article 22 of the GDPR in scale and scope, complementing its individualistic perspective with a collective perspective, whatever data are deployed and involved (either personal or non-personal). In addition, it would have broadened the DSA scope of action as well as the market-oriented perspective of the DMA. In a nutshell, it would have implemented a more value-oriented perspective by making the forbidden cross use or combination of data not waivable by consent (Art. 5, par 2, DMA) or, in any case, not limited to designated gatekeepers (pursuant to Art. 3, DMA) or to certain kinds of targeted advertising (Articles 26, 28, DSA).

Along this way, the path back to our starting point has been traced. By scaling down the potential intrusiveness of profiling techniques to put a sort of 'brake' on the technical and quantitative variables that make them too granular in gaining insights on people, a 'humanising' process is triggered for the sake of safeguarding the anthropological basis of the «homo dignus» [156], thus preserving equality, self-determination and moral agency [157].

[156] S. RODOTÀ, *Antropologia dell'«homo dignus»*, cit.

[157] C. COLAPIETRO-A. MORETTI, *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in *BioLJ*, 3/2020, p. 359 ff.