11.
Algorithmic Profiling and Targeting: Between European Law and Constitutional Boundaries

by *Nadia Maccabiani*[*]

Content: 1. A matter of fact. - 2. A matter of constitutional relevance. - 3. EU legal provisions relevant for profiling and targeting techniques. - 4. A de facto vicious cycle and a virtuous de jure safeguard.

1. A matter of fact

Our point of departure is represented by a matter of fact: since the beginning of the new millennium we have increasingly been faced with certain techniques that span different scientific domains but share the same subject and goal[1]. As for the former (the subject), the focus of the techniques is on human cognitive processes through the study of how they function. As for the latter (the goal), the purpose of the techniques is the exploitation of the knowledge and understanding gained about human cognitive processes in order to steer our behaviour towards certain pre-set aims.

These techniques are commonly known as neuromarketing and nudging, but also profiling and targeting based on machine learning; while they share the same subject and goal, their underlying means are different. Neuromarketing rests on evidence from the biological functioning of our neural processes, obtained from neuroscientific studies that make use of

* University of Brescia.

1. The Conference on Cognitive Computational Neuroscience stimulated interaction and cross-feeding between cognitive science, neuroscience and artificial intelligence, by underscoring their common goal by; see T. Naserlaris *et al.*, *Cognitive Computational Neuroscience: A New Conference for an Emerging Discipline*, in *Trends Cogn. Sci.*, Vol. 5, No. 22, 2018, pp. 365 ff.

fMRI (functional magnetic resonance imaging, electroencephalography, and physiological tracking (the tracking of facial expressions, eye movements, pupil dilation, heart rate and other physical manifestations of people's emotions and feelings), and it presents stimuli that can leverage human preferences and desires[2]. Nudging relies upon behavioural studies and experiments carried out on groups of people: these studies evidence the different cognitive biases that affect human decisions, refuting the theory that people behave in a rational way and showing that it is possible to leverage these cognitive biases in order to 'gently push' people towards certain behaviours[3]. Machine learning is a subset of artificial intelligence systems; it relies upon computer and data science studies that have developed different learning functions and feedback techniques (by means of sophisticated algorithms that are trained on huge amounts of data)[4] and that (among other things) enable the system to gain in-depth knowledge and understanding of people's habits, interests, thoughts and emotions (i.e. profiling)[5] and to target them with personalised content in order to steer

2. For the impact of neuroscience on legal studies, with specific regard to private law and free consent, see L. Tafaro, *Neuromarketing e la tutela del consenso,* Edizioni Scientifiche Italiane, 2018. For an overview of the tenets of neuromarketing and the neuroscientific techniques deployed by it, see A. Javor *et al.*, *Neuromarketing and Consumer Neuroscience: Contributions to Neurology*, in *BMC Neurology*, No. 13, 2013, pp. 1 ff; E. Harrell, *Neuromarketing: What You Need to Know,* in *Harvard Business Review,* January 23, 2019.

3. For a detailed overview of the object and the aim of nudging techniques, see R.H. Thaler, C.R. Sunstein, *Nudge. The Final Edition,* Penguin Books, 2021.

4. For a detailed description of the different functions and approaches of machine learning techniques, see W. Meert, T. De Laet, L. De Raedt, *Artificial Intelligence. A Perspective from the Field,* in N.A. Smuha (ed.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence,* Cambridge University Press, 2025, pp. 17 ff.

5. Article 4(4) of the GDPR lays down a legal definition of profiling: «"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements». Regarding the legal implications of profiling, 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,* Editoriale Scientifica, 2017, pp. 573 ff.; S. Calzolaio, *Protezione dei dati personali,* in *Digesto disc. pubbl.,* Utet Giuridica, 2017, pp. 598 ff.; L.A. Bygrave, *Article 22 Automated Individual Decision-making, Including Profiling,* in C. Kuner *et al.* (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary,* Oxford Academic, 2020, pp. 522 ff.; F. Bosco, N. Creemers, V. Ferraris, D. Guagnin, B.J. Koops, *Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities*, in S. Gutwirth, R. Leenes, P. De Hert (eds.), *Reforming European Data Protection Law,* Book Series: Law, Governance and Technology, Springer Science, Vol. 20, 2015, pp. 9 ff.

their choices[6]. Artificial intelligence systems, and in particular machine learning techniques, have been enabled by the digitalisation of people's daily lives. Philosophers and historians have iconically framed this change by speaking about the infosphere, 'inforgs', 'onlife'[7], and 'dataism' as a new faith or religion[8]. The substance is that we can no longer conceive of our lives without the interaction with digital devices, and as a consequence of this interaction our activities are constantly tracked and monitored through our online experience. This has led to the circulation of an increasing amount of personal and non-personal data, which feed new sophisticated machine learning algorithms, empowered by increasing computing power, allowing more detailed insights on people to be gained and their preferences or interests predicted from the patterns extracted from complex correlations among the data.

These three kinds of scientific evidence and achievement act and react on one another, in a circular way. On the one hand, machine learning techniques have made it possible for behavioural and neuroscientific studies to gather, process and correlate, in an more efficient way, huge amounts of data to give more granular and individualised insights about people[9]. On the other hand, the digital environment represents a conducive framework in which neuromarketing, profiling, targeting and nudging techniques can thrive, by displaying stimuli that are shaped and re-shaped in real time on the basis of the individual specificities of the targeted person. This allows these techniques to perform their steering purposes in a better way[10].

6. H. Ji, X. Xu, G. Su, J. Wang, Y. Wang, *Utilizing Machine Learning for Precise Audience Targeting in Data Science and Targeted Advertising*, in *Academic Journal of Science and Technology*, Vol. 9, No. 2, 2024, pp. 215 ff; J.A. Choia, K. Lim, *Identifying Machine Learning Techniques for Classification of Target Advertising*, in *ICT Express*, No. 6, 2020, pp. 175 ff.

7. L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo,* Raffaello Cortina Editore, 2014, pp. 27 ff.

8. Y.N. Harari, *Homo Deus. A Brief History of Tomorrow,* Penguin Random House UK, 2017, p. 428: «Dataism declares that the universe consists of data flows, and the value of any phenomenon or entity is determined by its contribution to data processing».

9. T. Cohen, *Regulating Manipulative Artificial Intelligence*, in *scripted*, No. 20, 2023, p. 216: «a machine learning system may have access to, or may construct, granular and dynamic behavioural profiles to identify and exploit a vulnerability in the manipulee's decision-making processes. These capabilities are the product not only of machine learning techniques but other features and functionality of digital environments».

10. K. Yeung, *'Hypernudge': Big Data as a Mode of Regulation by Design*, in *ICS*, No. 1, 2017, pp. 118 ff.; D. Susser, *Invisible Influence: Artificial Intelligence and the Ethics of Adaptive Choice Architectures*, in *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, New York, 2019, pp. 404 ff.

2. A matter of constitutional relevance

In respect of the matter of fact described briefly above, which constitutes our point of departure, our concern is a question of legal and constitutional relevance. First, we ask whether, and, if so, how, the above-mentioned practices align with fundamental constitutional values and freedoms. Secondly, we ask whether the legal protection that the European Union has set out in recent times is adequate. Our final question is whether something is missing from a legal and constitutional perspective.

Neuroscience, behavioural science and artificial intelligence achievements revolve around a premise that is different from the building block on which the whole legal system stands. More specifically, the legal system rests on the freedom of the human will, while neuroscience and behavioural science evidence how the human will is bounded, by biological factors (the former) or heuristics (the latter). Similarly, artificial intelligence stands on the mathematical representation, by means of different approaches, of human cognitive processes. However, it is not this dichotomy that raises concerns. Rather, there is a constitutional concern when the tools offered by neuroscience, behavioural science and machine learning are exploited in order to delve into our cognitive processes with the aim of influencing, distorting and manipulating them.

As is well known, constitutionalism is centred on the person, and on his/her human dignity. As such, its aim is to support a person's full development, not only as an individual subject but also as part of an organised community made of social relationships within which the person grows and thrives[11]. For this purpose, constitutional provisions set out fundamental rights and freedoms, and, as their reverse side, pose limits on public powers and duties of solidarity on private powers[12]. There are legal safeguards to preserve the integrity of moral agency[13], and thus the submission of a person to stimuli that exploit human fragility or vulnerability (emotions, feelings and cognitive biases) is at odds with the human dignity that represents the core value of constitutionalism[14]. As a consequence, it is not the evidence given by neuroscience, behavioural science or machine learning profiling and targeting that encroaches upon constitutional values, but their potential

11. A. Baldassarre, *Diritti della persona e valori costituzionali,* Giappichelli, 1997; S. Rodotà, *Il diritto di avere diritti,* Editori Laterza, 2012.

12. L. Carlassare, *Solidarietà: un progetto politico,* in *costituzionalismo.it,* No. 1, 2016, p. 66.

13. G. Resta, *Autonomia privata e diritti della personalità. Il problema dello sfruttamento economico degli attributi della persona in prospettiva comparatistica*, Jovene, 2005.

14. S. Rodotà, *Antropologia dell'«homo dignus»,* in *Riv. crit. dir. priv.,* No. 4, 2010, pp. 547 ff.

goals. Once again, as usual, it is not science and technology *per se* that are bad, but rather the way in which their achievements are exploited.[15] Neuromarketing, nudging, and political microtargeting capitalise on such achievements in order to shape human decisions.

If persuasion is part and parcel of trade relationships, political relationships, and social relationships at large, what is currently troublesome is the potential empowerment of the traditional tools of persuasion using the evidence given by neuroscience, behavioural science and machine learning techniques. This is because these techniques can delve deeply into cognitive processes and leverage cognitive biases, emotions, and subconscious perceptions in real time and in a personalised way, and in so doing strongly increase their effectiveness. In other words, when profiling carried out by automated algorithms is able to give a very detailed picture of a single person, the results of neuromarketing, nudging and targeting are strengthened because the suggested messages can not only be individualised, giving rise to tailored stimuli, granular targeting and boosted nudges, but can also be continuously adapted in real time to the detected subjective state or specific cognitive biases of the individual person, through the constant screening and monitoring allowed by digitalisation and automated profiling algorithms[16].

Against this backdrop, it is not difficult to figure out the multiple and intertwined constitutional principles that are being challenged[17]. Plenty of doctrinal studies and EU documents have underlined them. As already mentioned, at the root lies the person with his/her human dignity, as well as the principle of equality, since profiling implies putting people together in clusters and treating the clusters differently according to the features of their specific profiles[18]. In addition, the right to privacy and personal data protection can be infringed as a result, because of the correlations and patterns delivered by machine learning algorithms that allow the information enclosed in the secrecy of people's minds to be figured out[19].

15. M. Kranzberg, *Technology and History: "Kranzberg's Laws"*, in *Technology and Culture*, Vol. 27, No. 3, 1986, pp. 544 ff.

16. Cf. *supra*, footnotes 9-10.

17. For an in-depth understanding, see M. Ienca, O. Pollicino, L. Liguori., E. Stefanini, R. Andorno (eds.), *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights,* Cambridge University Press, 2022, especially pp. 125 ff.

18. V. Molaschi, *Algoritmi e nuove schiavitù*, in *federalismi.it*, No. 18, 2021, pp. 210 ff.

19. M. Kosinski, D. Stillwell, T. Graepel, *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, in *Proceedings of the National Academy of Sciences*, Vol. 110, No. 15, 2013, p. 5802: «People may choose not to reveal certain pieces of information about their lives [...], and yet this information might be predicted in a statistical sense from other aspects of their lives that they do reveal [...]. Human migration to digital environment

As a consequence, it is our freedom of thought that can be undermined, because this algorithmic knowledge can be leveraged (on the basis of evidence given by behavioural science and neuroscience) by stimuli that exploit people's cognitive biases, emotions and feelings and in this way target their moral agency in order to steer it towards pre-established goals[20]. In addition, and closely related to freedom of thought, it is the right to vote and the implied political freedom that can suffer an impact when nudging, and more specifically what has been called political microtargeting, is carried out[21]. These are some of the many constitutional principles and rights that can be considered to be touched upon.

However, if it is not a demanding task to identify the constitutional principles or rights that are affected by such techniques, it is a more daunting one to draft adequate legal safeguards, within boundaries that align with the principle of necessity and proportionality[22]. This difficulty is due to the fact that placing limits on profiling, neuromarketing, nudging and political microtargeting could – in turn – have an impact on other freedoms, such as the freedom to conduct a business, freedom of expression, and freedom to conduct research and science. Consequently, a balance must be struck among conflicting interests, according to the guidelines set out by the EU Better Regulation approach[23], in both directions: by testing not only whether a legal rule pursues a legitimate objective but also whether the rule is necessary and proportionate to this purpose.

In this respect, it is obvious that legal intervention could not be put in place to forbid neuroscience or behavioural science research or machine learning profiling and targeting as such, since these activities can support multiple goals, including those which produce useful results for socio-economic and technological development, for instance for the health of

renders it possible to base such predictions on digital records of human behavior. It has been shown that age, gender, occupation, education level, and even personality can be predicted from people's Web site browsing logs».

20. P. O'Callaghan, B. Shiner, *The Cambridge Handbook of The Right to Freedom of Thought,* Cambridge University Press, 2025, especially pp. 305 ff.

21. In this regard, A. Cardone, *"Decisione algoritmica" vs Decisione politica? A.I. Legge Democrazia,* Editoriale Scientifica, 2021, p. 72 ff, speaks about a lack of articulation of the political representative relationship and a commercialisation of the political message. For a broad overview on the matter, see also M. Calamo Specchia (ed.), *Processi politici e nuove tecnologie*, Giappichelli, 2024.

22. As evidenced by G. Azzariti, *Internet e Costituzione,* in *Politica del Diritto,* No. 3, 2011, p. 371. The author deems that the online environment represents both an economically relevant and a politically decisive space, and as such is in need of constitutional guarantees that protect against the abuse of power by states and corporations.

23. *Better Regulation Guidelines*, SWD(2021) 305 final.

people or the environment. The focus of regulation should rather be on the means deployed, in conjunction with relevant use-cases and the goals pursued (as is done in Article 5 of the AI Act, which lays down prohibited artificial intelligence practices).

Consequently, regulation can tackle the matter by acting at two different but strictly interrelated levels.

First, it should act at the individual level, pursuant to the personalistic principle. In this respect, it should be borne in mind that profiling people, and thus segmenting them into different groups on the basis of granular insights gained from their online behaviour, can be deemed to be an intrinsically discriminatory practice[24]. Moreover, when this practice is used to target people in order to manipulate their free choices, it encroaches upon their moral agency and thus impinges upon human dignity[25]. Even if neuromarketing is a widespread practice, upheld by freedom of expression and the freedom to conduct a business, it can be deemed to cross the boundaries traced by Article 41 of the Italian Constitution, since an economic private initiative cannot be conducted in a way that harms freedom and human dignity. Similarly, although persuasion is an essential part of the political debate, when it is strengthened by in-depth insights into people's thoughts and leveraged by the exploitation of people's cognitive biases, it can be deemed to be impinging on the freedom and personal character of the right to vote (Article 48 of the Italian Constitution).

Secondly, it can act at the collective level, pursuant to the pluralistic principle. When the complex dynamics of the economic and political market are put at stake, it is the principle of loyal and fair competition and the democratic functioning of the system as a whole that are affected.

Following this dual-level perspective, the EU has set out some provisions to tackle the challenges posed by the machine learning profiling and targeting that, as mentioned, can underlie neuromarketing, hyper-nudging and political micro-targeting practices. These provisions will be briefly considered in the next paragraph.

24. B. Parenzo, *Profilazione e discriminazione. Dal GDPR alla Proposta di Regolamento sull'IA,* in *Tecnologie e Diritto,* Vol. IV, No. 1, 2023, p. 335.

25. Moral agency has been described as being grounded on Article 2 of the Italian Constitution, which underlies the right to self-determination, and Article 21, since freedom of expression underlies freedom of thought: in this respect see A. Lamberti, *Costituzionalismo digitale, poteri delle piattaforme, intelligenza artificiale e democrazia,* in *Consulta Online,* No. 2, 2025, p. 1113.

3. EU legal provisions relevant for profiling and targeting techniques

Making rules on technology means ensuring that the technology serves freedoms and not control[26]. Hailing this premise, the European Union has recently laid down boundaries to activities carried out within the digital environment, by means of the AI Act[27], the DSA[28], the DMA[29] and the TTPA[30]. With reference to this broad framework, our focus will be on some of the provisions enacted by these recent pieces of EU legislation that can be deemed to deal with digital interaction when it results in actors being able to gain deep knowledge about people's interests, preferences, thoughts and emotions, and in this way to perform better targeting to affect people's cognitive processes and moral agency. In pursuing this objective, the EU has enacted two kinds of provision: on the one hand, provisions directly addressed to upholding the personalistic principle, and, on the other hand, provisions that directly protect collective and pluralistic interests, like the interest of fair and loyal competition as well as the correct functioning of the economic and political markets, while indirectly also implementing individual safeguards on moral agency.

Even before the above-mentioned EU legislation, the GDPR had prohibited decisions based exclusively on automated personal data processing, including profiling «which produces legal effects concerning ... [the person] or similarly significantly affects him or her» (Article 22). However, in a way that is consistent with the individual stance taken by the GDPR, this prohibition can be waived with the explicit consent of the data subject or when profiling is necessary to carry out a contract with them.

Broadening the ban on certain machine learning profiling or targeting practices, the AI Act has, since 2 February 2025, forbidden the following: social scoring; emotion recognition in the workplace and places of

26. M.C. Carrozza, O. Pollicino, *L'«umano» deve essere il perno della normativa nel digitale*, in *Il Sole 24Ore,* 30 luglio 2025.

27. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act, AI Act).

28. 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, DSA).

29. 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, DMA).

30. Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (TTPA).

education; AI systems that subliminally interfere with or manipulate or deceive in order to distort «the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm» (Article 5, para 1(a)); and any AI system «that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm» (Article 5, para 1(b)). In addition, AI systems are also forbidden when their purpose is predictive justice or policing, or the creation or expansion of «facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage» (Article 5, para 1(d), (e)). In a similar vein, AI systems are forbidden if their purpose is to carry out «biometric categorisation ... that categorise[s] individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation' (Article 5, para 1(g)), or when they carry out «"real-time" remote biometric identification ... in publicly accessible spaces for the purposes of law enforcement» (except for certain excluded cases: Article 5, para 1(h)).

Such prohibitions are aimed at reducing the margin of manoeuvre of artificial intelligence systems run by powerful machine learning algorithms; as such they limit both the scope and the scale of the profiling, controlling and monitoring of human activities or features. As a consequence, they also put limits on the power of targeting, in order to protect human dignity and moral agency.

Following the same prescriptive stance, the DSA prohibits online platforms from displaying deceptive online interfaces: «Providers of online platforms shall not design, organise or operate 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). It also prohibits the display of advertisements on the basis of profiling that uses special categories of personal data (Article 26, para 3), and «advertisements ... based on profiling ... using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor» (Article 28, para 2). In addition, it should be borne in mind that, according to the ECJ, a legitimate interest does not represent

a suitable legal basis for intrusive profiling and consequent personalised advertising[31]. Furthermore, with specific regard to political advertising and with reference to targeting techniques and ad-delivery techniques that involve the processing of personal data, the TTPA limits the scope of such techniques to personal data collected directly from the data subject when explicit consent has been obtained (Article 19, para 1(a), (b)). It also prohibits profiling on the basis of special categories of personal data (Article 19, para 1(c)) and – in any circumstances – the profiling of minors (Article 19 para 2) for political advertising goals.

In addition to this prescriptive and mainly individual stance, some of the prohibitions set out in the AI Act as well as some of those in the DSA are also functional to pluralistic interests, by supporting loyal and fair competition in the market. In this respect, such provisions ban practices that could be exploited by an economic operator in order to take advantage of its competitors. In line with the principle of individual protection but also with pluralistic objectives, the AI Act and the DSA provide some transparency requirements. More specifically, under the AI Act notice should be provided when an artificial intelligence system is in action, and meaningful information should be given about the functioning of high-risk artificial intelligence systems, with reference to «the role of the AI system in the decision-making procedure and the main elements of the decision taken» (see, respectively, Articles 50 and 86). As for the DSA, transparency is required when an advertisement is displayed, with «meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters» (Article 26, para 1(d)); similar provisions are set out when recommender systems are in action (Article 27). In the same light, the TTPA sets out clear transparency duties for providers and publishers of political advertising about the identification of the political advertising service (Article 7) and each political advertisement published (Articles 11-12), including notice of the deployment of targeting techniques or ad-delivery techniques based on the processing of personal data (Article 12, para 1(l)) and record-keeping for the services provided (Article 9). In addition, when targeting and ad-delivery techniques, including through the use of artificial intelligence systems, are deployed in the context of political advertising, meaningful information must be given about the personal data involved, as well as the mechanisms and main parameters used (Article 19).

31. Case C-252/21, *Meta Platforms Inc and Others v Bundeskartellamt* paras. 115 ff.

The DMA follows a reverse path. Its point of departure is represented by a market-oriented approach, and thus it starts from a pluralistic perspective, focusing on loyal and fair competition; however, this does not prevent it from also having the function of protecting the individual subject. On the one hand, recognising that gatekeepers have a potential advantage in terms of the accumulation of data, which thereby raises barriers to entry to the market, the DMA limits the possibility of combining and cross-using end users' personal data obtained from different services, included third parties' websites and applications that make use of services provided by gatekeepers (Article 5). Furthermore, it prevents gatekeepers from using, in competition with business users, aggregated or non-aggregated data that is not publicly available, when the data are generated by these business users or are inferred from, or collected through, the commercial activities of the business users or their customers (Article 6). In addition, the gatekeeper must grant business users, end users and third-party undertakings providing online search engines access to some data generated by their activity[32]. On the other hand, the DMA imposes an obligation on gatekeepers to enable end users to freely choose whether or not to opt in to personal

32. Article 6, paras 8-11: «8. The gatekeeper shall provide advertisers and publishers, as well as third parties authorised by advertisers and publishers, upon their request and free of charge, with access to the performance measuring tools of the gatekeeper and the data necessary for advertisers and publishers to carry out their own independent verification of the advertisements inventory, including aggregated and non-aggregated data. Such data shall be provided in a manner that enables advertisers and publishers to run their own verification and measurement tools to assess the performance of the core platform services provided for by the gatekeepers. 9. The gatekeeper shall provide end users and third parties authorised by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service, including by providing, free of charge, tools to facilitate the effective exercise of such data portability, and including by the provision of continuous and real-time access to such data. 10. The gatekeeper shall provide business users and third parties authorised by a business user, at their request, free of charge, with effective, high-quality, continuous and real-time access to, and use of, aggregated and non-aggregated data, including personal data, that is provided for or generated in the context of the use of the relevant core platform services or services provided together with, or in support of, the relevant core platform services by those business users and the end users engaging with the products or services provided by those business users. With regard to personal data, the gatekeeper shall provide for such access to, and use of, personal data only where the data are directly connected with the use effectuated by the end users in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end users opt in to such sharing by giving their consent. 11. The gatekeeper shall provide to any third-party undertaking providing online search engines, at its request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on its online search engines. Any such query, click and view data that constitutes personal data shall be anonymised».

data processing and sign-in practices, by offering a less personalised but equivalent alternative, and does not permit them to make the use of the core platform service or certain functionalities thereof conditional upon the end user's consent. In this last respect, «the less personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or signing in end users to a service ... it should be as easy to withdraw consent as to give it. Gatekeepers should not design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent» (recital 37). In a similar vein, the ECJ, in the *Meta* case, has stated that (irrespective of the size of the digital service provider), an equivalent alternative option, devoid of profiling and consequent personalised services, must be offered by the data controller (if necessary subject to an appropriate fee)[33]. The cookies pledge principles drafted by the European Commission in collaboration with stakeholders has added a further option to the acceptance of personalised advertising on a pay or leave model, asking for «an additional choice of another less privacy intrusive form of advertising»[34].

In addition, gatekeepers are charged with certain transparency duties in respect of profiling activities in order to «put external pressure on [them] ... not to make deep consumer profiling the industry standard, given that potential entrants or start-ups cannot access data to the same extent and depth, and at a similar scale» (recital 72). Reinforcing such an individual but also market-driven perspective, the ECJ has stated that inconsistencies with the GDPR provisions can be taken into consideration by the competent authorities when assessing whether there is an abuse of dominant position[35].

33. Case C-252/21, para 150: «users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations».

34. Draft Pledging Principles, para D, in https://commission.europa.eu/document/download/8eb6358b6c5df4997aa92d254dde910b6_en?filename=Draft%20pledging%20principles.pdf (last accessed August 18th, 2025).

35. Case C-252/21, paras 48 and 51: «It follows that, in the context of the examination of an abuse of a dominant position by an undertaking on a particular market, it may be necessary for the competition authority of the Member State concerned also to examine whether that undertaking's conduct complies with rules other than those relating to competition law, such as the rules on the protection of personal data laid down by the GDPR [...] access to personal data and the fact that it is possible to process such data have become a significant parameter

4. A de facto vicious cycle and a virtuous de jure safeguard

Many EU documents and acts, as already mentioned, follow a human-centric approach in order to strike a balance between the need to allow technology, innovation and economic growth to thrive and the safeguarding of human dignity as well as fundamental rights and freedoms. However, this statement risks remaining mere rhetoric when there is an awareness that a widespread online 'model' lacks adequate legal safeguards. We are used to arguing about a 'business model'[36] that rests on tracking-based advertising to enable what is defined as behavioural or personalised advertising[37]. This tracking system for users' online navigation is not limited to the economic market. The digital environment has become a sort of constant and continuous 'survey' of our habits, behaviours, interests, preferences, and beliefs or, in a single word, of 'us': experiments, similar to those carried out in behavioural science or neuroscience within a protected environment and following pre-settled legal and ethical guidelines, are now conducted continuously, in real time and 'outside the lab'[38], by exploiting people's digital interactions in order to profile them. The recent evidence in a MIT report on the Data Comp Common Pool dataset is telling about this. It shows how web-scraped machine learning datasets (built on the basis of web-scraping activities from 2014 to 2022) contain significant personally identifiable information, despite sanitisation efforts[39]. This shows the high potential created by digital devices in respect of people's personalities.

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 competition 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». This position is in line with what is already suggested by the doctrine: see G. De Minico, *Libertà* in *Rete. Libertà* dalla *Rete,* Giappichelli, 2020, p. 248; M. Betzu, *I poteri privati nella società digitale: oligopoli e antitrust,* in *Diritto Pubblico,* No. 3, 2021, pp. 739 ff.

36. S. Zuboff, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, Profile Books, 2019, pp. 27 ff.

37. *EDPB reply to the Commission's initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices – Draft Principles (Ref. Ares(2023)6863760).*

38. T. Cohen, *Regulating Manipulative Artificial Intelligence*, in *scripted*, No. 20, 2023, p. 205: «Outside the lab, millions of people interact daily with complex machine learning systems designed to "learn" their behavioural patterns and adapt stimuli (such as newsfeeds and ads) to induce choices which align with the systems' objectives».

39. R. Hong, J. Hutson, W. Agnew, I. Huda, T. Kohno, J. Morgenstern, *A Common Pool of Privacy Problems: Legal and Technical Lessons from a Large-Scale Web-Scraped Machine Learning Dataset*, at https://arxiv.org/abs/2506.17185v1 (last accessed August 18th, 2025).

This widespread 'model' challenges highly sensitive constitutional values, principles, rights and freedoms. It is not profiling activities *per se* that raise concern. It is rather their scale and scope, as well as their consequent targeting potential, when they are carried out by artificial intelligence techniques, and more specifically machine learning algorithms, that raises worries. This is due to the fact that machine learning algorithms empower in-depth profiling that – in turn – can strongly enhance targeting capabilities, by hiding them behind people's daily online experiences. More specifically, the more granular, detailed and insightful is a person's 'digital profile' (processed and built by machine learning algorithms that enrich this profile with inferences and predictions about people's behaviour, preferences, interests etc.), the more deep and profound is the consequent knowledge and understanding gained about that person, and the more personalised (also over time) are the messages (of whatever kind and format) that can be displayed to them by leveraging their individual cognitive biases or, in any case, their personal feelings and emotions. Following this model, even the most innocent persuasion becomes a powerful 'weapon' against personal cognitive processes, and personal perceptions, emotions and feelings, due to the improved performance and effectiveness stemming from the alliance between algorithmic profiling and targeting, which in turn improve the evidence given by behavioural science and neuroscience. It is a circular mechanism that takes the stock of behavioural science and neuroscientific results and reinforces them, since it is addressed at leveraging people's cognitive biases (more specifically, their confirmation bias and limited attention) or people's feelings and emotional reactions to certain stimuli. In addition, such a circular and mutually improving mechanism affects not only the dynamics of the economic market, but also those of the political debate or – broadly speaking – political messages and communication, as well as the design of online interfaces and the methods of artificial intelligence systems with which people interact: all can be tailored to the detailed profile of the user, carrying out more effective targeting aimed at persuasion, manipulation, and deception.

Bearing in mind the arguments made in this paper, it seems to us that making the legal protection adequate and significant implies, because of the fundamental rights and freedoms involved, tackling the root cause of the issue. Doing this means taking the protections already adopted by the recent above-mentioned pieces of EU legislation a step further. These further steps can be briefly summarised as the enactment of regulatory measures different from prohibitions, for the protection of fundamental rights and freedoms; or the typical safeguards of consumer protection laws or, else, the defences usually erected by product safety law or competition law.

Starting with prohibitions, those set out in the AI Act and the DSA deal with some of the more relevant manifestations of the problem, but they do not solve the problem at its source. Thus, this regulatory technique is only apparently prescriptive and coercive. In this respect, for instance, it does not prove to be an adequate regulatory safeguard to prohibit (as is done by Article 5, para 1(a) and (b) of the AI Act) any artificial intelligence system that deploys subliminal, deceptive or manipulative techniques or exploits a particular vulnerability of people (when it causes or is reasonably likely to cause significant harm to people by distorting their behaviour). Similarly, it does not prove to be an adequate safeguard to prohibit deceptive or manipulative online interfaces (as is done by Article 25 of the DSA). These prohibitions risks being empty prohibitions because of their ill-defined boundaries, since it is too difficult to establish in an objective way what is subliminal, deceptive or manipulative – the terms depend on many subjective and contextual factors which also change over time. It is also not easy to establish the threshold of what can be deemed a significant harm, since, again, subjective and contextual factors make this threshold flexible.

In reference to the measures adopted by the EU legislator that follow the model of consumer protection regulation, it is transparency requirements and informed consent that come into play in order to re-balance the power asymmetries within the contractual relationship. However, because of the pervasiveness and intrusiveness that profiling practices achieve today, the depth of the knowledge about people they enable to be obtained, which leverages the evidence delivered by behavioural science and neuroscience, and the consequent tailored and individualised targeting, the imbalance mentioned above becomes too huge. There is a double reason for this: on the one hand, the 'cognitive' supremacy gained by one party over the other is 'artificially' multiplied and fostered; on the other hand, the interests involved are important and sensitive, affecting constitutional rights and freedoms. In this last regard, as previously said, it is not difficult to identify many constitutional values, principles, rights and freedoms that can be strongly and significantly infringed by deep and granular profiling and targeting practices that impinge upon both the individual and the collective life. Consequently, the struggle to re-balance the wide asymmetries should not be uniquely borne on the 'shoulders' of the weakest parties by means of transparency safeguards and consent.

As regards product safety laws, the security and procedural requirements set out in the AI Act are certainly useful; however, they do not define the boundaries of the mechanisms that make the interaction with an artificial intelligence system too intrusive in respect of people's habits, thoughts, preferences, and so on.

As for competition law safeguards, their market-oriented approach needs to be improved with an approach oriented towards fundamental rights.

Bearing all this in mind, in order to adequately protect people and make the human-centric model not merely rhetorical, a new step should be implemented[40] by tackling the 'roots' of the matter, instead of limiting the legal intervention to the external manifestations of the whole mechanism (by forbidding manipulative and deceptive AI systems or online interfaces, or implementing transparency duties or procedural requirements).

To tailor such legal provisions, a balancing assessment should be carried out in order to adopt a reasonable and proportionate stance that balances the conflicting interests in a fair way, pursuant to the EU Better Regulation approach. On the one hand, there are the interests of the market, with the relevant and well-known business model developed by digital service providers that relies upon deep profiling and consequent personalised and behavioural advertising as well as recommender systems. There are also the interests of political parties or other subjects who undertake political activity and political communication (political actors, as defined by the TTPA), who similarly tend to target people on the basis of their profiles (political microtargeting). On the other hand, there are the interests of the targeted people, who hold fundamental rights and freedoms, grounded on the fundamental values of human dignity and equality. These rights include not only the right to privacy and to data protection, and not only the right not to be discriminated against in ways that also go beyond the classical categories of discrimination set out in EU anti-discrimination laws (since algorithmic data processing allows new kinds of discrimination)[41], but also the right to freedom of thought, the right to vote (with its implications in terms of a personal and free vote), the right to personal identity and the relevant rights of the personality[42]. It turns out that this balancing operation involves both individual and collective interests to avoid massive, intrusive and pervasive distortions of personal opinions and information, for the sake of both the correct functioning of the market and democratic processes. Because of the dysfunction that these practices provoke at the collective level, within the economic and political system at large, such legal safeguards

40. In this respect, see also the position upheld by the 'digital constitutionalism' doctrine, G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society,* Cambridge University Press, 2022.

41. As evidenced by B.H.M. Custers, *Reconsidering Discrimination Grounds in the Data Economy: An EU Comparison of National Constitutions,* in *Computer Law & Security Review,* Vol. 50, 2023, p. 10.

42. M. Ienca, O. Pollicino, L. Liguori., E. Stefanini, R. Andorno (eds.), *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights,* cit.

should not be limited to the ill-defined prohibitions mentioned above, should not be limited to transparency notices, due process and consent, should not be limited to procedural or safety requirements to be fulfilled by online service providers, providers or deployers of artificial intelligence systems, and should not be limited to fair and legal competition.

The new step must add something different to these kinds of protection.

It is necessary, according to the precautionary principle[43], to adopt a preventive and pre-emptive approach that puts limits on profiling (and consequently cuts down the potential power of targeting) in the two sectors mentioned above (economic and political). To achieve more effective regulatory protection implies tackling what lies at the origin of these manipulative or distorting online strategies, by scaling down the capabilities that allow such techniques to become detailed and individualised and, thus, dangerous. More specifically, it implies making a reduction in the margin of manoeuvre of the profiling and the consequent granular and personalised targeting practices. In this regard, the hints stemming from the DMA and the TTPA are useful and should be broadened in their objective and subjective scope.

One can refer to the provisions of the former (the DMA), which imposes limits on the possibility of gatekeepers combining, cross-using and gathering data from end users or business users, and also on the provisions of the latter (the TTPA), which limits profiling and the consequent targeting to data directly collected from the data subject that excludes special categories of data.

On the one hand, profiling should be carried out on the limited basis of personal data directly collected from the individual, after excluding personal data that indirectly stem from him/her, such as derived or inferred data that are extracted by machine learning algorithms from tracks left by his/her online activity[44]. Moreover, it should not include special categories

43. A. Simoncini, *L'impatto dell'IA sul diritto e i diritti*, in *BioLaw Journal*, No. 1, 2020, p. 498 claims that the precautionary principle should be applied when regulating AI systems.

44. The relevant risks are well described by recital 74 of Regulation EU 2024/900: «Personal data collected directly from individuals, or indirectly such as observed or inferred data, when grouping individuals according to their assumed interests or derived through their online activity, behavioural profiling and other analysis techniques, are increasingly used to target political messages to groups or individual voters or individuals, and to amplify their impact. On the basis of the processing of personal data, in particular special categories of personal data under Regulations (EU) 2016/679 and (EU) 2018/1725, different groups of voters or individuals can be segmented and their characteristics or vulnerabilities exploited, for instance by disseminating the advertisements at specific moments and in specific places, designed to take advantage of the instances where they would be sensitive to a certain kind of information or a message. Such processing of personal data has specific and detrimental

of personal data. In this way, the objective scope of the path started by Article 18 of the TTPA would, as a result, be enlarged beyond the political advertising domain[45]. On the other hand, consistently with this perspective of limiting the data used in profiling to data directly collected from the data subject, the use (by combination or cross-use) of personal data gathered from third parties or from different services provided by the same digital services provider should be prohibited[46], thus widening the subjective scope of Article 5 of the DMA by enlarging its boundaries beyond gatekeepers and by waiving the possibility of escaping from the prohibition by obtaining the end user's consent. Consequently, it is not a question of obliging gatekeepers to offer «a less personalised but equivalent alternative ... [that] should not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or signing in end users to a service»[47], but it is rather a question of making the less personalised option the standard one, when economic or political messages are at stake, irrespective of the size of the digital services provider.

The paths mentioned above would lead to profiling being limited in scope and in scale, thus avoiding intrusive profiling activities that enable, support, and strengthen the capability and effectiveness of targeting

effects on individuals' fundamental rights and freedoms, such as to be treated fairly and equally, not to be manipulated, to receive objective information, to form their opinion, to make political decisions and exercise their voting rights. Furthermore, it negatively impacts the democratic process as it leads to fragmentation of the public debate about important societal issues, selective outreach and, ultimately, the manipulation of the electorate. It also increases the risk of the spreading of information manipulation and foreign interference. Misleading or surreptitious political advertising is a risk because it influences the core mechanisms that enable the functioning of our democratic society».

45. Article 18(1), Regulation EU 2024/900, states that «Targeting techniques or ad-delivery techniques that involve the processing of personal data in the context of online political advertising shall be permitted only when the following conditions are fulfilled: (a) the controller collected the personal data from the data subject [...]».

46. As explained by recital 36 of the DMA, «The processing, for the purpose of providing online advertising services, of personal data from third parties using core platform services gives gatekeepers potential advantages in terms of accumulation of data, thereby raising barriers to entry. This is because gatekeepers process personal data from a significantly larger number of third parties than other undertakings. Similar advantages result from the conduct of (i) combining end user personal data collected from a core platform service with data collected from other services; (ii) cross-using personal data from a core platform service in other services provided separately by the gatekeeper, notably services which are not provided together with, or in support of, the relevant core platform service, and vice versa; or (iii) signing-in end users to different services of gatekeepers in order to combine personal data».

47. Cf. recitals 36 and 37 of the DMA.

practices within the economic market and the political debate[48]. This seems to be a proportionate measure aimed at avoiding the distortion or, in any case, the flattening of people's behaviours and opinions by algorithmically driven models or patterns extracted from past data, information and inputs[49]. Thus, irrespective of whether these targeting messages are true or false, what risks being undermined is the human capability of developing a critical perspective, of thinking 'outside the box', or of opening the mind to messages that would be discarded from algorithmically driven models that, in turn, are filtered on the basis of personal profiling and enclosed within the consequent individualised targeting[50]. Such a mechanism risks impoverishing novel and forward-looking insights, thus restricting the boundaries of individual cognitive freedoms, the full development of human beings and the complete unfolding of democratic processes.

In conclusion, the suggested regulatory approach can be read through the lens of the Italian Constitution, by giving an updated implementation to the goals set out in Articles 2 and 3: the removal of obstacles to individual and collective freedom and development, for the sake of people's full participation in economic, political and social life. This implies that, following an economic and socio-technological evolution, the nature of the obstacles to be removed, as well as the regulatory remedies enacted for their removal, has undergone a change. Along this path, consumer protection law and product safety regulations, as well as the competition-oriented perspective, as enacted in the pieces of EU legislation mentioned above, should be complemented. More specifically, they need to be complemented by a (not only proclaimed but effective) rights-driven dimension which aims to reduce the power of the 'technological weapons' mentioned above[51], to decrease their potential to grab, push, manipulate and shape people's thoughts, interests, preferences, and emotions, acting on the boundaries of their triggers (through profiling and consequent targeting), and to scale them down.

48. E. Caterina, *La comunicazione elettorale sui* social media *tra autoregolazione e profili di diritto costituzionale,* in G. Di Cosimo (a cura di), *Processi democratici e tecnologie digitali,* Giappichelli, 2023, p. 33, suggests the prohibition of more intrusive forms of microtargeting in political advertising.

49. C. Pinelli, *Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale,* in *Diritto Pubblico*, No. 1, 2022, p. 185.

50. As regard filter-bubbles and polarisation, see E. Pariser, *The Filter Bubble: What the Internet is Hiding From You*, Penguin, 2011; C. R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, 2017.

51. To paraphrase C. O'Neil, *Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy,* Crown Publishers, 2016.

Bibliography

G. Azzariti, *Internet e Costituzione*, in *Politica del Diritto*, No. 3, 2011, p. 371.

A. Baldassarre, *Diritti della persona e valori costituzionali*, Giappichelli, 1997.

M. Betzu, *I poteri privati nella società digitale: oligopoli e antitrust*, in *Diritto Pubblico*, No. 3, 2021, pp. 739 ff.

F. Bosco, N. Creemers, V. Ferraris, D. Guagnin, B.J. Koops, *Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities*, in S. Gutwirth, R. Leenes, P. De Hert (eds.), *Reforming European Data Protection Law*, Springer Science, Vol. 20, 2015, pp. 9 ff.

L.A. Bygrave, *Article 22 Automated Individual Decision-making, Including Profiling*, in C. Kuner *et al.* (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford Academic, 2020, pp. 522 ff.

M. Calamo Specchia (ed.), *Processi politici e nuove tecnologie*, Giappichelli, 2024.

S. Calzolaio, *Protezione dei dati personali*, in *Digesto disc. pubbl.*, Utet Giuridica, 2017, pp. 598 ff.

A. Cardone, Decisione algoritmica *vs Decisione politica? A.I. Legge Democrazia*, Editoriale Scientifica, 2021, p. 72 ff.

L. Carlassare, *Solidarietà: un progetto politico*, in *costituzionalismo.it*, No. 1, 2016, p. 66.

E. Caterina, *La comunicazione elettorale sui social media tra autoregolazione e profili di diritto costituzionale*, in G. Di Cosimo (a cura di), *Processi democratici e tecnologie digitali*, Giappichelli, 2023, p. 33.

J.A. Choia, K. Lim, *Identifying Machine Learning Techniques for Classification of Target Advertising*, in *ICT Express*, No. 6, 2020, pp. 175 ff.

T. Cohen, *Regulating Manipulative Artificial Intelligence*, in scripted, No. 20, 2023, p. 205 ff.

B.H.M. Custers, *Reconsidering Discrimination Grounds in the Data Economy: An EU Comparison of National Constitutions*, in *Computer Law & Security Review*, Vol. 50, 2023, p. 10.

G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022.

G. De Minico, *Libertà in Rete. Libertà dalla Rete*, Giappichelli, 2020, p. 248.

L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, 2014, pp. 27 ff.

Y.N. Harari, *Homo Deus. A Brief History of Tomorrow*, Penguin Random House UK, 2017, p. 428.

E. Harrell, *Neuromarketing: What You Need to Know*, in *Harvard Business Review*, January 23, 2019.

R. Hong, J. Hutson, W. Agnew, I. Huda, T. Kohno, J. Morgenstern, *A Common Pool of Privacy Problems: Legal and Technical Lessons from a Large-Scale Web-Scraped Machine Learning Dataset*, at https://arxiv.org/abs/2506.17185v1.

M. Ienca, O. Pollicino, L. Liguori, E. Stefanini, R. Andorno (eds.), *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights*, Cambridge University Press, 2022, especially pp. 125 ff.
A. Javor *et al.*, *Neuromarketing and Consumer Neuroscience: Contributions to Neurology*, in *BMC Neurology*, No. 13, 2013, pp. 1 ff.
H. Ji, X. Xu, G. Su, J. Wang, Y. Wang, *Utilizing Machine Learning for Precise Audience Targeting in Data Science and Targeted Advertising*, in *Academic Journal of Science and Technology*, Vol. 9, No. 2, 2024, pp. 215 ff.
M. Kranzberg, *Technology and History: "Kranzberg's Laws"*, in *Technology and Culture*, Vol. 27, No. 3, 1986, pp. 544 ff.
M. Kosinski, D. Stillwell, T. Graepel, *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, in *Proceedings of the National Academy of Sciences*, Vol. 110, No. 15, 2013, p. 5802.
A. Lamberti, *Costituzionalismo digitale, poteri delle piattaforme, intelligenza artificiale e democrazia*, in *Consulta online*, No. 2, 2025, p. 1113.
W. Meert, T. De Laet, L. De Raedt, *Artificial Intelligence. A Perspective from the Field*, in N.A. Smuha (ed.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge University Press, 2025, pp. 17 ff.
V. Molaschi, *Algoritmi e nuove schiavitù*, in *federalismi.it*, No. 18, 2021, pp. 210 ff.
T. Naserlaris *et al.*, *Cognitive Computational Neuroscience: A New Conference for an Emerging Discipline*, in *Trends Cogn. Sci.*, Vol. 5, No. 22, 2018, pp. 365 ff.
P. O'Callaghan, B. Shiner, *The Cambridge Handbook of The Right to Freedom of Thought*, Cambridge University Press, 2025, especially pp. 305 ff.
C. O'Neil, *Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy*, Crown Publishers, 2016.
E. Pariser, *The Filter Bubble: What the Internet is Hiding From You*, Penguin, 2011.
B. Parenzo, *Profilazione e discriminazione. Dal GDPR alla Proposta di Regolamento sull'IA*, in *Tecnologie e Diritto*, Vol. IV, No. 1, 2023, p. 335.
C. Pinelli, *Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale*, in *Diritto Pubblico*, No. 1, 2022, p. 185.
G. Resta, *Autonomia privata e diritti della personalità. Il problema dello sfruttamento economico degli attributi della persona in prospettiva comparatistica*, Jovene, 2005.
S. Rodotà, *Antropologia dell'«homo dignus»*, in *Riv. crit. dir. priv.*, No. 4, 2010, pp. 547 ff.
S. Rodotà, *Il diritto di avere diritti*, Editori Laterza, 2012.
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*, Editoriale Scientifica, 2017, pp. 573 ff.
A. Simoncini, *L'impatto dell'IA sul diritto e i diritti*, in *BioLaw Journal*, No. 1, 2020, p. 498.
C.R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, 2017.

D. Susser, *Invisible Influence: Artificial Intelligence and the Ethics of Adaptive Choice Architectures*, in *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, New York, 2019, pp. 404 ff.
R.H. Thaler, C.R. Sunstein, *Nudge. The Final Edition*, Penguin Books, 2021.
K. Yeung, *'Hypernudge': Big Data as a Mode of Regulation by Design*, in *ICS*, No. 1, 2017, pp. 118 ff.
S. Zuboff, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, Profile Books, 2019, pp. 27 ff.