AI LAW

INTERNATIONAL REVIEW
OF ARTIFICIAL INTELLIGENCE LAW

Streamlining EU Digital Regulation While Enforcing Human-Centric Constitutional Safeguards

Nadia Maccabiani

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

Abstract

(EN): This analysis examines selected EU digital regulations and assesses their ability to address the far-reaching legal and constitutional implications of intrusive profiling based on machine learning. Building on the EU's ongoing efforts within the Digital Omnibus Package to streamline existing digital regulations, the study aims to systematise EU provisions which, although currently dispersed across different legal acts, address various technical and legal aspects related to strong inferential processes resulting from machine learning practices. The objective is to find out a regulatory technique that enhances their effectiveness and ensures that they are better suited to providing appropriate constitutional safeguards.

(ES): Este análisis examina determinadas regulaciones digitales de la Unión Europea y evalúa su capacidad para abordar las profundas implicaciones jurídicas y constitucionales de la elaboración de perfiles basada en el aprendizaje automático. Partiendo de los esfuerzos en curso de la UE, en el marco del *Digital Omnibus Package*, por racionalizar la normativa digital vigente, el estudio pretende sistematizar las disposiciones de la UE que, aunque actualmente se encuentran dispersas en distintos actos jurídicos, abordan diversos aspectos técnicos y jurídicos implicados en las técnicas de perfilado mediante aprendizaje automático. El objetivo es reforzar su efectividad y asegurar que estén mejor adaptadas para proporcionar garantías constitucionales adecuadas.

(FR): Cette analyse examine certaines réglementations numériques de l'Union européenne et évalue leur capacité à répondre aux profondes implications juridiques et constitutionnelles du profilage fondé sur l'apprentissage automatique. S'appuyant sur les efforts en cours de l'UE, dans le cadre du *Digital Omnibus Package*, visant à rationaliser la réglementation numérique existante, l'étude entend systématiser les dispositions de l'UE qui, bien qu'actuellement dispersées dans différents actes juridiques, traitent de divers aspects techniques et juridiques liés aux techniques de profilage par apprentissage automatique. L'objectif est d'en renforcer l'efficacité et de veiller à ce qu'elles soient mieux adaptées pour offrir des garanties constitutionnelles appropriées.

(DE): Diese Analyse untersucht ausgewählte digitale Regelungen der Europäischen Union und bewertet deren Fähigkeit, den weitreichenden rechtlichen und verfassungsrechtlichen Implikationen

des auf maschinellem Lernen beruhenden Profilings zu begegnen. Aufbauend auf den laufenden Bemühungen der EU im Rahmen des *Digital Omnibus Package*, die bestehende digitale Regulierung zu straffen, zielt die Studie darauf ab, EU-Bestimmungen zu systematisieren, die – obwohl derzeit auf verschiedene Rechtsakte verteilt – unterschiedliche technische und rechtliche Aspekte betreffen, die mit *Profiling*-Techniken des maschinellen Lernens verbunden sind. Ziel ist es, ihre Wirksamkeit zu erhöhen und sicherzustellen, dass sie besser geeignet sind, angemessene verfassungsrechtliche Schutzvorkehrungen zu gewährleisten.

(PT): Esta análise examina regulamentos digitais selecionados da União Europeia e avalia a sua capacidade de enfrentar as amplas implicações jurídicas e constitucionais da definição de perfis baseada em aprendizagem automática. Com base nos esforços em curso da UE, no âmbito do *Digital Omnibus Package*, para racionalizar a regulamentação digital existente, o estudo visa sistematizar as disposições da UE que, embora atualmente dispersas por diferentes atos jurídicos, abordam diversos aspetos técnicos e jurídicos envolvidos nas técnicas de definição de perfis por aprendizagem automática. O objetivo é aumentar a sua eficácia e assegurar que estejam mais bem adequadas para proporcionar salvaguardas constitucionais apropriadas.

(IT): Lo scritto prende in esame alcuni regolamenti dell'Unione europea, valutandone l'adeguatezza giuridico-costituzionale rispetto ad intrusive tecniche di profilazione basate sul *machine-learning*. Preso atto del tentativo di razionalizzare la normativa sul digitale, intrapreso dall'UE con il *Digital Omnibus Package*, lo scritto sistematizza le esistenti disposizioni europee che, sebbene distribuite tra vari atti normativi, affrontano questioni tecniche e giuridiche dei processi inferenziali presupposti alla profilazione. L'obiettivo è di suggerire una tecnica regolatoria che rafforzi le esistenti tutele, all'insegna di adeguate garanzie costituzionali.

Summary: 1. A Brief "Technical" Introduction. – 2. From Technology to Law: What Does Machine Learning Profiling Entail? – 3. How Existing EU Regulations Deal with the Issue – 4. A Proposal for a "Re-Oriented" Regulatory Approach.

1. A Brief "Technical" Introduction

The starting point of this research is technical in nature. However, its aim is to translate technical evidence into the legal domain, not in order to assess whether the former complies with the latter, but rather to examine whether the legal framework is adequately structured and provides consistent constitutional safeguards against the risks arising from a technology-enabled evolution that cannot be reversed or erased.

The "technical" point of departure recalls some techniques that have become widespread in the last two decades. These techniques are deployed within the socio-economic and political fields: they not only focus on human cognitive

processes and consequent human behaviours but also target them, in order to steer them towards certain goals. Such techniques, which are termed nudging and neuromarketing, draw on evidence and inferences made by studies conducted within the domain of behavioural sciences and neurosciences. It is not our aim to deepen such practices, but rather to recall them for the limited purposes of the reasoning that will follow. Nudging, based on evidence given by behavioural sciences, exploits human cognitive biases in order to guide human behaviour towards certain aims [1]. Neuromarketing techniques are based on neuroscientific achievements that prove that certain stimuli, even subliminal ones, trigger certain targeted reactions in the human being [2].

Against this backdrop, it is worth recalling a further step within the field of cognitive sciences, with specific reference to computer sciences. This step has been enabled by the development of the internet, global online platforms, the business models of such platforms, and the huge amount of digital data consequently put into circulation, as well as the new artificial intelligence systems that followed, which were no longer knowledge-based and deterministic but were reliant on data and statistical correlations (and were run by machine learning algorithms, with all their sub-categories) [3]. Such machine learning systems, fed with the data, both personal and non-personal data, that people leave during their online and digitally connected experiences, have given rise to the possibility of making insightful and in-depth inferences about people's behaviour and preferences [4]. This technique has been refocused onto the more general practice of profiling. Profiling, legally defined in Article 4, point (4) of the GDPR,

[1] For the different kinds of nudging techniques, see R.H. THALER-C.R. SUNSTEIN, *Nudge. The Final Edition*, New York, 2021.

[2] For an overview of the tenets of neuromarketing and the neuroscientific techniques deployed by it, see A. JAVOR-M. KOLLER-N. LEE-L. CHAMBERLAIN-G. RANSMAYR, *Neuromarketing and Consumer Neuroscience: Contributions to Neurology*, in *BMC Neur.*, 13/2013, p. 1 ff.; E. HARRELL, *Neuromarketing: What You Need to Know*, in *Harvard BR*, January 23, 2019; L. BOJIĆ-L. TUCAKOVIĆ-N. NIKOLIĆ, *Neuromarketing Unmasked: A Review of Current State in the Field*, in *Ek. Pred.*, 2021, p. 404.

[3] For a description of machine learning systems as a subset of artificial intelligence systems, see S. RUSSELL-P. NORVIG, *Artificial Intelligence – A Modern Approach*, Hoboken, 2021.

[4] M. HILDEBRANDT, *Defining Profiling: A New Type of Knowledge?*, in M. HILDEBRANDT-S. GUTWIRTH (eds.), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Dordrecht, 2008, p. 17 ff.; A. MANTELERO, *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, in *CLSR*, 32, 2016, p. 239; L.A. BYGRAVE, *Data Protection Law, Approaching its Rationale, Logic and Limits*, The Hague, 2002, p. 306 ff.; 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*, Naples, 2017, p. 585 ff.

essentially entails inferences being extracted from data by deriving certain patterns and predictions in respect of people's behaviours, preferences, emotions and beliefs.

A clear definition of this strong inferential model was given in the 2010 Council of Europe Recommendation, which envisaged profiling as being divided into three stages: «The first stage consists of large-scale collection of data on individual behaviour … During the second stage, these data derived from individual observations undergo computer analysis to correlate certain behavioural characteristics. With statistical tools and algorithms, it thus becomes possible to identify connections between certain kinds of behaviour. Human common sense and logic play no part in establishing these correlations. It is purely the computing power and the sophistication of the algorithms that bring to light correlations often invisible to the naked eye or beyond human reason, albeit without explaining them ... In addition, statistical methods are used to determine a probability factor for the correlation made. In the third stage, the defined correlation is applied to an identified or identifiable individual in order, with a certain margin of error, to deduce some of his or her past, present or future characteristics» [5]. This technique, carried out by machine learning algorithms, improves itself in a circular way, since the system can gather the reaction of the profiled person when subjected to certain stimuli and accordingly fine-tune its inferences on the basis of this recorded reaction, putting in place what computer scientists call «real-time data analysis and optimization» and an «intelligent delivery decision» [6].

Tacking stock of this brief description of the use of machine learning to enable profiling, the "quantum leap" that machine learning has brought about in respect of the traditional inferences made by behavioural sciences and neurosciences, as well as with regard to the kind of stimuli classically offered by nudging and neuromarketing, becomes evident. The causes are multiple. First, in the same way as behavioural science and neuroscience, algorithmically-driven automated profiling is also focused on the behaviour of human beings. However, unlike traditional experiments that first collect and process their evidence "in the lab", machine learning profiling collects and processes its data "outside the lab", constantly following humans' digital interactions in disparate sectors, constantly updating the relevant available data, and constantly making

[5] Recommendation CM/Rec(2010)13 adopted by the Committee of Ministers of the Council of Europe, *The protection of individuals with regard to automatic processing of personal data in the context of profiling*, pars. 96-98.

[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 *AJST*, 9, 2, 2024, p. 216.

correlations between items of data that stem from such different domains and different human activities [7]. In addition, this is done without provoking the "filtering" conduct that people might engage in when they are aware they are being tested in a lab. Second, as a consequence of two different and intersecting factors, machine learning profiling lays the ground for strengthening the effectiveness of nudging and neuromarketing. On the one hand, the stimuli that behavioural science and neuroscience have proved are able to affect human conduct in the bricks-and-mortar world can now be fine-tuned in a personalised way, using the granular knowledge and understanding of individuals gained by in-depth and detailed machine learning profiling. On the other hand, this fine-tuning can be adapted over time in respect of each single person, according to his/her changing habits and preferences or on the basis of the feedback represented by his/her reaction to the stimuli displayed [8]. In this way, machine learning profiling boosts techniques that already exist, such as nudging and neuromarketing, by relocating them within the realm of the digital world, giving rise to what has been named, according to the terminology of computer sciences, targeting or microtargeting [9]. Unlike bricks-and-mortar nudging and neuromarketing, the pervasiveness of microtargeting stems from people's constant «onlife», and the derived possibility of impinging upon the various fields that have been colonised by the «infosphere» [10] (from the social field to the economic and political relations ones). Third, machine learning profiling can not only boost nudging and neuromarketing, but it also represents the basis and the enabler of further disparate – and potentially harmful – practices (social scoring, emotion recognition, biometric categorisation, etc.).

Bearing all this in mind, our legal and constitutional concern will indeed be focused on the scale and scope of this "quantum leap" undertaken by machine learning profiling, as the next paragraph will explain.

[7] T. COHEN, *Regulating Manipulative Artificial Intelligence*, in *scripted*, 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».

[8] K. YEUNG, *"Hypernudge": Big Data as a mode of regulation by design*, in *ICS*, 20, 1/2017, p. 118 ff.; S. MILLS, *Finding the "nudge" in hypernudge*, in *Tech. Soc.*, 71, 2022, p. 150 ff.

[9] H. JI- X. XU-G. SU-J. WANG-Y. WANG, *op. cit*., p. 215 ff.

[10] «Onlife» and «the infosphere» are terms conceived to describe the dominant virtual life of today's humans by the philosopher L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milan, 2017, p. 67 ff.

2. From Technology to Law: What Does Machine Learning Profiling Entail?

What has been briefly described until now represents the "technical" scenario. However, as promised, the purpose of this paper is to shift this scenario into the legal field. In doing so, it becomes evident that what is happening within the domain of cognitive sciences, with specific regard to machine learning enabled profiling, can be considered to be at odds with some tenets of constitutional and legal relevance [11].

This part of the cognitive sciences field (as is typical of the whole cognitive sciences domain) puts its focus on personal aspects and personality traits, and thus on something that is traditionally outside the scope of a democratic and constitutional legal system, since it is treated by such a system as a "holy" space that pertains exclusively to the person [12]. Classically speaking, a democratic and constitutional legal system consistently does not deal with the personal and personality sphere of human beings, except to safeguard it against external coercion, or to address the possibility of it expressing itself, or to allow it to be developed on an informed and fair basis. Even a regulatory technique that is intended to uphold the correct construction of a person's internal will, like disclosure and the consequent information notice as well as the underlying principles of transparency, loyalty and fairness, is aimed at rebalancing existing asymmetries within socio-economic relationships. Thus, once again, the personal sphere of an individual (his/her thoughts and preferences) is relevant for the legal system insofar as it touches upon the external dynamics of the market or of a democratic society. This approach positions the law within the realm of social phenomena, and for this reason puts it in charge of dealing with the external consequences of human behaviour [13].

Our legal concern is not so much grounded on the fact that a person and his/her personal aspects and personality traits is made the object of analysis, calculations, measurements and correlations, but rather on the way that this is

[11] For an inquiry about the impact of quantitative computation on the constitutional protection of the person, see E. DI CARPEGNA BRIVIO, *Pari dignità sociale e* reputation scoring. *Per una lettura costituzionale della società digitale*, Torino, 2024.

[12] J.C. BUBLITZ, *The Nascent Right to Psychological Integrity and Mental Self-Determination*, in A. VON ARNAULD-K. VON DER DECKEN-M. SUSI (eds.), *The Cambridge Handbook of New Human Rights. Recognition, Novelty, Rhetoric*, Cambridge, 2020, p. 387; T. ISTACE, *Protecting the mental realm: What does human rights law bring to the table?*, in *Netherlands QHR*, 41, 4/2023, p. 233.

[13] R. COTTERRELL, *The Sociology of Law. An Introduction,* Butterworths, London, Dublin, Edinburgh, 1992, p. 53 ff.

done by machine learning techniques, which is different from the way that traditional inferences are made in other cognitive science domains [14]. On the one hand, machine learning techniques chart an "inside-out" movement in relation to a person's internal interests, preferences, and emotions, making their prediction its core activity [15]. On the other hand, this understanding and these predictions are leveraged by strong inferential calculations run by machine learning algorithms. By means of these inferences, the knowledge and understanding of a person result in data that are quite detached from the data directly provided by the person or directly observed from his/her conduct. This kind of inference can unravel sensitive aspects of a person even when no special categories of personal data were fed into the machine [16], and can result in personal data even when the input data were not personal [17]. What is involved is not only the personal data that a person has directly delivered to the online platform or digital device while being aware of doing so, nor only the person's observed online conduct and consequent online tracks across different services: these represent the mere starting point of a far more complex process run by sophisticated automated algorithms.

In such cases, it is not only the inside-out movement of their preferences, interests, orientations, and beliefs that skips the will of the data subject: it is in fact the linearity of this movement that is disrupted. Specifically, this disruption occurs because of the intervention of the algorithmically-driven inferences which make the data accomplish the "quantum leap" mentioned above, completely detaching them from the source data. The European Commission has

[14] D. CORACI-I. DOUVEN-G. CEVOLANI, *Inferenza e spiegazione nelle neuroscienze cognitive*, in *Sist. Int.*, 1/2024, p. 25 ff.

[15] S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997, p. 134 ff.

[16] L. EDWARDS-M. VEALE, *Slave to the Algorithm? Why a 'Right to An Explanation' is Probably Not the Remedy You Are Looking For*, in *Duke LTR*, 2017, pp. 36-38. According to Article 29 Working Party, WP251rev.01, Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, p. 15, profiling «can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data».

[17] N. LÖLFING.-C. BISCHOFF-BRIEL-A. DIECKHOFF, *Data Protection Law*, in M. ARTZT-O. BELITZ-S. HEMBT-N. LÖLFING (eds.), *International Handbook of AI Law – A Guide to Understanding and Resolving the Legal Challenges of Artificial Intelligence*, The Netherlands, 2025, p. 309: «The autonomous learning process of AI systems can also result in the creation of personal data, where the AI algorithms infers information from anonymous data that ends up becoming personal data by inference. The data might not be considered personal data at the time of collection but is processed by an AI system that creates new connections and analyses to the point where it is possible to infer personal data».

consistently pronounced that the «use of … different types of data may have different implications for the accuracy and the fairness» of profiling practices, «in particular where the processing is opaque or relies on data points whose accuracy is more difficult to be verified» [18]. Thus, as a result of the peculiarity of this process, the distinction between personal and non-personal data is blurred, not only because these types of data are inextricably mixed within the data set, but also because, as mentioned above, even apparently insignificant data can result in personal data (and even special categories of personal data) being produced at the end of the inferential process.

In respect of such situations, the legal protection given through the pattern shaped by privacy and personal data protection rights does not seem to offer adequate safeguards, since the linearity of the connection of the person with his/her data has been broken by a strong inferential process. At the end of the inferential path, the resulting evaluation could be very far removed from the input data and, as such, from the scope of manoeuvre and control of the data subject, even if he/she has been correctly informed (pursuant to the GDPR's provisions) about the automated profiling activity, its purpose and its consequences [19].

All this being considered, it is possible to conclude at this point in time that there is "nothing new under the sun". This situation is something that doctrine has already fully described and examined [20].

Therefore, it is the substance of the inferential process triggered by machine learning profiling that should come into focus, by paying attention to what it actually entails and means in legal terms. In this respect, it should be recalled that making inferences about people implies making "evaluations", and thus "judgements", as stated by the Article 29 Working Party in reference to Article 4, point 4, of the GDPR: «the use of the word 'evaluating' suggests that profiling involves some form of assessment or judgement about a person» [21].

---

[18] EC Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), par. 159.

[19] See Articles 13, par. 2(f); 14, par. 2(g); 15, par. 1(h) and Article 22 of the GDPR.

[20] As observed by B. CUSTERS, *Profiling as inferred data. Amplifier effects and positive feedback loops*, in E. BAYAMLIOĞLU-I. BARALUIC-L. JANSSENS-M. HILDEBRANDT (eds.), *Being Profiled: Cogitas Ergo Sum. 10 Years of Profiling the European Citizen*, Amsterdam, 2018, p. 113: «The key characteristic of inferred data is that it is data inferred from other data and not data directly or indirectly provided by data subjects»; B. CUSTERS-H. VRABEC, *Tell me something new: data subject rights applied to inferred data and profiles*, in *CLSR*, 52, 2024, p. 11: «it is arguable that in applying analytical techniques data loses the direct connection with the data subject and is thus no longer considered to be 'provided by them'. Rather, it concerns data generated by the data controller».

[21] WP251rev.01 Guidelines on Profiling, cit., p. 7.

However, making judgements about people is not neutral from a legal perspective.

It is not our intention to delve into the issue of algorithmically-driven discrimination [22]: this is a slippery slope since the intrinsically discriminatory nature of profiling surely multiplies the grounds of discrimination [23], and it could lead to the conclusion that each profiled person is – as such – differentiated from others, because of the granularity of insights on people achievable by machine learning profiling [24]. Our intention is to focus on the upstream issue of the inferential process *ex se*, and to recall the "regime" usually followed by the legal system when assessments on people are allowed.

Traditionally speaking, when the legal system explicitly allows assessments and inferences to be made with respect to people, it regulates these "judgements" by means of procedural requirements and ensures that the relevant evaluations are carried out with reference to a limited set of significant, objective and evidence-based data.

More specifically, in the legal system, the assessment or "judgement" of people is usually expressly authorised in pre-established cases, and procedural safeguards are provided by the law. This implies that, before the assessment of a person is permitted, the legal system has already struck a balance between conflicting interests, in compliance with the principle of proportionality and reasonableness [25]. For instance, it is permitted to assess people when fraud, an

[22] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLJ*, 1/2019, p. 63 ff. For new algorithmically-determined categories of discrimination, beyond those provided by EU antidiscrimination law, see B.H.M. CUSTERS, *Reconsidering discrimination grounds in the data economy: an EU comparison of national constitutions*, in *CLSR*, 50, 2023, p. 10. For the distinction between disparate treatment and disparate impact, see S. BAROCAS-A.D. SELBST, *Big Data's Disparate Impact*, in *California LR*, 104, 3/2016, pp. 694-711.

[23] As evidenced by WP251rev.01 Guidelines on Profiling, cit., p. 5, automated profiling has far-reaching implications: «The widespread availability of personal data on the internet and from Internet of Things (IoT) devices, and the ability to find correlations and create links, can allow aspects of an individual's personality or behaviour, interests and habits to be determined, analysed and predicted … Profiling can perpetuate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences. This can undermine their freedom to choose, for example, certain products or services such as books, music or newsfeeds. In some cases, profiling can lead to inaccurate predictions. In other cases, it can lead to denial of services and goods and unjustified discrimination».

[24] B. PARENZO, *Profilazione e discriminazione. Dal GDPR alla Proposta di Regolamento sull'IA*, in *Tecn. dir.*, 2023, p. 106.

[25] As explained by the EC Guidelines on prohibited AI practices, cit., par. 147, a distinction is drawn between lawful and unlawful automated assessments of people: «At the same time, the prohibition is not intended to affect lawful practices that evaluate people for specific purposes

offence or an infringement of the law needs to be proved, when professional/educational competence needs to be tested, when clinical trials are carried out, or when a person's health needs to be checked by the healthcare system.

This results in the enshrinement of certain guarantees which are often composed not only of procedural and formal requirements but also of boundaries, requiring the evaluation be carried out on the basis of objective and verifiable data.

In summary, an assessment can be done by humans or, following technological development, by automated means, for legally envisaged legitimate purposes, in respect of a limited set of objective and verifiable aspects and according to legally pre-settled procedures. As a consistent rule, even when the legal system authorises a process to be automated, it ensures that it is anchored to such limited sets of verifiable and objective data as are relevant in the sector concerned. In this way, the type, scale and scope of the inferences that can be drawn are kept under control.

For instance, automated profiling is allowed to be carried out by financial institutions for anti-money laundering purposes, provided that it is based on the cases, information and procedures envisaged by Chapter III of Regulation (EU) 2024/1624 [26]. Similarly, the Consumer Credit Directive (EU) 2023/2225, when creditworthiness is required to be assessed, makes reference to certain criteria and methods whose aim is to identify relevant and accurate data on the basis of which the evaluation must be carried out [27]. Analogously, inferences made by

that are legitimate and in compliance with Union and national law, in particular where those laws specify the types of data relevant for the specific evaluation purposes and ensure that any resulting detrimental or unfavourable treatment of persons is justified and proportionate».

[26] Art. 76, par. 5 of Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[27] Recital 53 makes reference to «information provided by the consumer not only during the preparation of the credit agreement in question, but also during a long-standing commercial relationship». The following Recital 54 clarifies that the «assessment of creditworthiness should be proportionate and done in the interest of the consumer, … and should take into consideration all necessary and relevant factors that could influence a consumer's ability to repay the credit … Member States should be able to issue additional guidance on additional criteria and methods to assess a consumer's creditworthiness, for example by setting limits on loan-to-value or loan-to-income ratios». Recital 55 details that «The assessment of creditworthiness should be based on information on the financial and economic situation. Such information should be necessary and proportionate to the nature, duration, value and risks of the credit for the consumer, in line with the data minimisation principle set out in Regulation (EU) 2016/679, and should be relevant, complete and accurate. That information should include at least the income and expenses of the consumer, including giving appropriate consideration to the consumer's current obligations, inter alia the living expenses of the consumer and the consumer's household, as well as the consumer's financial liabilities. That information should not include special categories of personal

automated data processing on the name records of passengers on a flight, pursuant to Directive (EU) 2016/681, are permitted, according to the interpretation given by the ECJ, provided that they are subject to human revision and are reliant on objective criteria that are objectively linked to the serious crimes addressed by this Directive [28]. Accordingly, the AI Act allows the use of AI systems for the prediction or assessment of the risk of a person committing a crime only when the assessment of the involvement of the person in criminal activity is already based on objective and verifiable facts: in such cases an AI system is permitted to support human assessments [29]. Furthermore, the European Union Fundamental Rights Agency (the FRA), in its guide entitled «Preventing unlawful profiling today and in the future», anchors algorithmic profiling deployed in border management and checks by frontline police officers to objective evidence and reasonable grounds of suspicion [30].

It follows from the above that machine learning profiling disrupts the linearity of the guarantees usually set out by the legal system when the assessment of people is expressly allowed, for a dual reason. On the one hand, it is deeply and strongly inferential, and thus it moves a long way from the original, more objective and verifiable, data [31]. On the other hand, it is subjectively oriented: its purpose is to assess personal aspects and personality traits, and thus, once again, it is not closely linked to objective and verifiable data. In brief, it essentially consists of behavioural analysis for predictive purposes, as stated by the European Data Protection Board (the EDPB) [32].

Thus, although the legal system has usually limited, with adequate and effective safeguards, the types of assessment and judgement that are allowed to be carried out on people, which may be automated, the scale and scope of

data referred to in Article 9(1) of Regulation (EU) 2016/679, such as health data including cancer data, nor information obtained from social networks. The European Banking Authority Guidelines of 29 May 2020 on loan origination and monitoring provide guidelines on what categories of data may be used for the processing of personal data for creditworthiness purposes, which include evidence of income or other sources of repayment, and information on financial assets and liabilities or on other financial commitments».

[28] C-817/19, pars. 219-220 and 259, allows automated data processing in respect of the personal data of people suspected of planning, committing or having committed a serious crime, only where there is objective material from which it can be inferred that those data might, in a specific case, make an effective contribution to combatting such activities.

[29] Article 5, par. 1(d) of the AI Act.

[30] FRA, *Preventing unlawful profiling today and in the future: a guide*, 2018, p. 97 ff.

[31] See footnote 19.

[32] See par. 84 of the EDPB Guidelines 3/2025 on the interplay between the DSA and the GDPR.

machine learning profiling when it is deployed in cases other than those explicitly authorised and regulated skip over these guarantees. This is because the GDPR essentially roots its protection against profiling in the binomial safeguard of transparency and consent, making it possible to remove the prohibition on profiling based solely on automated personal data processing. However, as already evidenced by doctrine, the fundamental rights, freedoms and values at stake are too wide to be adequately safeguarded by means of this individual approach [33]. Therefore, a more structured and comprehensive protection is necessary in order to create an adequate defence in the fast-moving technological evolution that has made profiling algorithms so sophisticated, intrusive, and endowed with strong inferential power.

Although these concerns had been raised by scholars some time ago [34], it is only in recent times that the EU has started to struggle with the issue, complementing the individual approach to automated profiling taken by the GDPR by regulating – in a more efficient way – the high risks and systemic effects which can be triggered by this practice. This raised awareness by the EU is iconically summarised in the ECJ's *Meta Platforms* case, which describes the underlying widespread business model: «based on financing through online advertising, which is tailored to the individual users of the social network according, inter alia, to their consumer behaviour, interests, purchasing power and personal situation. Such advertising is made possible in technical terms by the automated production of detailed profiles in respect of the network users and the users of the online services offered at the level of the Meta group. To that end, in addition to the data provided by the users directly when they sign up for the online services concerned, other user- and device-related data are also collected on and off that social network and the online services provided by the Meta group, and linked to their various user accounts. The aggregate view of the data allows detailed conclusions to be drawn about those users' preferences and interests» [35].

[33] 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*, Dordrecht, 2015, p. 3 ff.

[34] The collective risks of automated profiling became well known because of the Cambridge Analytica scandals, but scholars had proclaimed the threat of the legal implications of this surveillance practice well before: see J. Van Dijck, *The culture of connectivity: A critical history of social media*, Oxford, 2013, p. 46 ff.; S. Zuboff, *Big other: surveillance capitalism and the prospects of an information civilization*, in *JIT*, 30, 1/2015, p. 75 ff.; F. Pasquale, *The black box society: The secret algorithms that control money and information*, Cambridge, 2015.

[35] C-252/21, par. 27.

However, it is worth recalling that machine learning profiling does not only underpin this clear business model consisting of algorithmically capturing, assessing and predicting the personal aspects and personality traits of people in order to increase their engagement and keep them stuck to their device as long as possible for advertising goals [36]. It also pervades all the main digital services people use, by shaping the displayed content. From recommender systems at large to newsfeeds, from digital assistants and companions to online games architecture, from cultural to political information, everything can be tailored on the basis of algorithmic inferences.

This is the reason why the legal and constitutional relevance of the great power inherent in machine learning profiling covers both the need to protect the single person and a more collective and systemic perspective. Consequently, the individual stance undertaken by the GDPR certainly represents an important starting point that calls for further complementary provisions that can tackle the collective implications of profiling.

Bearing this in mind, our attention moves now to EU legislation in order to find out how it has evolved in respect of the inferential "technical" process described above.

3. How Existing EU Regulations Deal with the Issue

In respect of automated profiling, the path followed by the EU can be briefly described as swinging between the protection of the single person "from" the market and the protection "of" the market. It can also be briefly described as a path of increasing awareness of the high risks underlying machine learning inferences, with such risks being termed "high" or "systemic".

The bedrock is obviously represented by the provisions of the GDPR, in which respect the other EU legislative acts contain a clause of conformity, usually introduced by the «without prejudice» formula. Article 22 GDPR, dealing

[36] As explained by the European Parliament's resolution of 12 December 2023 on addictive design of online services and consumer protection in the EU single market (2023/2043(INI)), par. A, «whereas in today's attention-based economy, certain technology companies use design and system functionalities to take advantage of users' and consumers' vulnerabilities in order to capture their attention and increase the amount of time they spend on digital platforms; whereas many digital services, such as online games, social media, streaming services for films, series or music, online marketplaces or web shops may be designed to keep users on the platform for as long as possible so as to maximise the data collected and the time and money they spend there as well as to maximise activity, engagement, content production, network development and data sharing».

with fully automated profiling, sets up a regulatory technique that is broadly followed by subsequent and more recent EU interventions. In substance, it enshrines a prohibition, upon the occurrence of certain conditions (i.e. a significant impact on the person), and it foresees a possible derogation upon, among other things, the data subject's consent, provided that certain transparency and due process requirements are met.

Thus, not all automated profiling crosses the threshold of the legal prohibition set out in Article 22. Furthermore, the Working Party and the EDPB explain that fully automated profiling is not considered a technique that *ex se* "significantly affects" a person, but that this judgement depends on the subsequent practices it may enable. For instance, as declared by the Article 29 Working Party, profiling overcomes the threshold (of significantly affecting a person) when it gives rise to targeted advertising based on intrusive insights, «the tracking of individuals across different websites, devices and services», or the exploitation of known vulnerabilities [37]. In this respect, the recent guidelines issued by the EDPB on the interplay between the Digital Services Act and the GDPR have upheld an analogous position [38] and have also added that «it cannot be excluded that the presentation of specific content to users of an online platform via a recommender system would be a 'decision' in the meaning of Article 22(1) GDPR, i.e. a decision which significantly affects the data subject» [39]. In

[37] WP251rev.01 Guidelines on Profiling, cit., p. 22.

[38] EDPB Guidelines No. 3/2025, cit., par. 62: «To assess whether an automated decision to present a specific advertisement to an individual produces legal effects or similarly significantly affects him or her, several (non-exhaustive) characteristics of the personal data processing activity (including at the level of each individual advertisement delivery) should be taken into account, including the intrusiveness of the profiling process, the tracking of individuals across different websites, devices and services; the expectations and wishes of the individuals concerned; the way the advert is delivered; or using knowledge of the vulnerabilities of the data subjects targeted».

[39] EDPB Guidelines 3/2025, cit., par. 84. The following par. 85 explains that «This could be the case, in particular, where the recommender system presents recommendations that cause effects that significantly affect data subjects, i.e. the 'decision' to present specific content to an individual may have an impact that is not necessarily legal but rather economic and social. Particular attention should be paid to cases where algorithmic processes could propose content, services and products that significantly affect individuals having a prolonged or permanent impact on them or significantly affect their behaviour or choices, e.g. recommender systems for housing or job offers on an online platform. The DSA underlines the implications for data subjects related to recommender systems stating that «recommender systems can have a significant impact on the ability of recipients to retrieve and interact with information online, including to facilitate the search of relevant information for recipients of the service and contribute to an improved user experience. They also play an important role in the amplification of certain messages, the viral dissemination of information and the stimulation of online behaviour».

the case of personalised advertising, the legal basis for carrying out automated profiling is narrower than that specified in Article 6, par. 1 of the GDPR. The ECJ, in the *Meta Platforms* case, excluded the performance of a contract and legitimate interest as legal bases. Profiling based solely on automated data processing, pursuant to Article 22 of the GDPR, is also relevant for credit scoring practices. According to the ECJ's adjudication, credit scoring entails the «automated establishment of a probability value based on personal data relating to a person and concerning that person's ability to repay a loan in the future» [40]. Consequently, such a practice, following the ECJ's reasoning, encompasses a profiling activity based solely on automated data processing.

It follows that in all the practices mentioned here (targeted advertising, recommender systems, and credit scoring), due process and transparency duties must be fulfilled; furthermore, meaningful information about the logic of the automated system, and the significance of, and envisaged consequences for, the data subject (Articles 13, par. 2 (f); 14, par. 2 (g); 15, par. 2(h) of the GDPR) [41] must be provided; and the possibility of the data subject expressing his/her point of view, to object the decision and to obtain human revision must be available (Art. 22, par. 3).

Furthermore, for the above-mentioned practices, the most suitable legal basis, in the same way as when special categories of personal data are involved [42],

[40] C-634/21, par. 46.

[41] B. CUSTERS-H. VRABEC, *op. cit*., p. 7, observe, in reference to Articles 13-14 of the GDPR, that «This right to meaningful information about the logic of the profiling may not entail information about the actual profiles or the categories in which data subjects are placed, but it may provide clues about what kinds of profiles or categories are established». In reference to Article 15 of the GDPR, the authors underline that «Even if the inferred data is personal data in the sense that the inferences are ascribed to individuals, it may be unclear whether the right of access can be used by data subjects to get access to such information … This provision does not, however, entail a right for data subjects to receive information about the actual profiles or categories, such as the different types of categories and the category in which the data subject is placed. The provision in Article 15.4 GDPR (stating that all this shall not adversely affect the rights and freedoms of others) could considerably restrict data subject access to categories and profiles. On the one hand, providing such information may interfere with the interests of the data controller, as such information may be considered trade secrets that provide a data controller with competitive edge. It may also create excessive business cost for the data controller to start providing details of how the data has been managed on their end, through which models it has gone and what the analysis has looked like. On the other hand, providing such information may interfere with the interests of other data subjects in the database, as such information may also reveal their characteristics».

[42] C-252/21, par. 89, specified that «where a set of data containing both sensitive data and non-sensitive data is subject to such operations and is, in particular, collected *en bloc* without it being possible to separate the data items from each other at the time of collection, the processing

relies upon the giving of information to the data subject and their explicit consent. However, for this consent to be valid, another condition has been added by the ECJ, pursuant to Article 7, par. 4 of the GDPR: «users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations [i.e. profiling]» [43].

This approach, grounded on disclosure notices and the consequent awareness of the data subject, reflects the individual stance taken by the GDPR and was adopted in a period when the scale and scope of inferences obtained by machine learning algorithms were not so pervasive and intrusive as they are nowadays.

Transparency duties and explicit consent represent the legal basis for targeted advertising and recommender systems in Regulation (EU) 2022/2065 (DSA) [44]. However, this Act recognises the amplitude of the risks implied by advertising or recommender systems based on machine learning profiling, which extend beyond the sphere of the single person [45], becoming systemic [46]. Evidence of this concern can be found in the express references in the DSA to the use and design of the algorithmic systems at the basis of both recommender systems and the selection and display of advertisements, as factors that influence the severity and probability of the systemic risks [47]. With specific regard to personalised advertisements, the DSA states that «When recipients of the service are presented with advertisements based on targeting techniques

of that set of data must be regarded as being prohibited, within the meaning of Article 9(1) of the GDPR, if it contains at least one sensitive data item and none of the derogations in Article 9(2) of that regulation applies». In addition, special categories of personal data are involved when such information is the result of linking data from different services (pars. 66 ff.).

[43] C-252/21, par. 150.

[44] 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).

[45] Recital 79 of the DSA is crystal clear about the systemic nature of the risks involved, which is also linked to the platform's business model: «Very large online platforms and very large online search engines can be used in a way that strongly influences safety online, the shaping of public opinion and discourse, as well as online trade. The way they design their services is generally optimised to benefit their often advertising-driven business models and can cause societal concerns».

[46] The DSA divides systemic risks into four categories: (1) dissemination of illegal content (Recital 80); (2) actual or foreseeable impact on the exercise of fundamental rights and freedoms (Recital 81); (3) actual or foreseeable negative effects on democratic processes, civic discourse (Recital 82); (4) «actual or foreseeable negative effect on the protection of public health, minors and serious negative consequences to a person's physical and mental well-being, or on gender-based violence» (Recital 83) and electoral processes, as well as public security.

[47] Article 34, par. 1, and par. 2, points (a) and (d), of the DSA.

optimised to match their interests and potentially appeal to their vulnerabilities, this can have particularly serious negative effects. In certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups» [48]. With specific reference to recommender systems, it has been observed that the «DSA recognizes their significant role in the amplification and viral dissemination of content as well as the stimulation of online behaviour» [49].

Taking stock of the severity of such risks, the DSA consistently prohibits the display of advertisements based on profiling using special categories of personal data (Art. 26, par. 3): this is an absolute prohibition, without the possibility of derogation, which is different from what is done in the GDPR [50]. However, a doubt remains: does this prohibition also extend to cases in which special categories of personal data are inferred from data which do not belong to this category? This extension is supported not only by the Working Party position about profiling mentioned above [51], but also by Recital 69 of the DSA, since this includes (going further than the case of profiling using special categories of personal data) the case of a resulting categorisation based on those special categories [52]. In addition, in compliance with the requirement to act in the "best interests of the child", the DSA forbids – in a similar absolute way – the display of advertising based on profiling using the personal data of the recipient of the service when (it is known with reasonable certainty) he/she is a minor (Art. 28).

The DSA has further enhanced the position of the recipient of the service: it has expressly introduced the duty of an online platform to offer an alternative choice. In particular, for targeted advertising (Art. 26, par. 1(d)) and recommender systems (Art. 27, par. 1) the online platform is charged with the duty to

[48] Regulation (EU) 2022/2065, Recital 69.

[49] EDPB Guidelines 3/2025, cit., par. 80.

[50] EDPB Guidelines 3/2025, cit., par. 67: «These special rules laid down by the DSA complement the rules laid down in Article 9(2) GDPR and Article 22(4) GDPR when they apply. The presentation of advertisements based on profiling using special categories of personal data by providers of online platforms to recipients of the service is prohibited by the DSA even in situations where the provider of an online platform or another entity would rely on an appropriate legal basis under Article 6(1) GDPR and an appropriate derogation under Article 9(2) GDPR for this processing».

[51] WP251rev.01 Guidelines on Profiling, cit.

[52] Recital 69 of the DSA states that «providers of online platforms should not present advertisements based on profiling …, using special categories of personal data referred to in Article 9(1) of that Regulation, including by using profiling categories based on those special categories».

provide meaningful information about the main parameters used to determine the recipient to whom the advertisement is presented [53] or the order of the information presented, and about the possibility for the recipient of the service to change these parameters. In addition, Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) are required to provide at least one option, for the main parameters of their recommender systems, which is not based on profiling (Article 39) [54].

However, such transparency requirements are to be fulfilled after the processing of personal data has occurred, as underlined by the recent EDPB Guidelines No. 3/2025. This is different from the information notice to be provided to the data subject under Article 13 of the GDPR, which must be given before the data processing is undertaken [55].

[53] Pursuant to Recital 68 of the DSA, such main parameters include «explanations … on the method used for presenting the advertisement, for example whether it is contextual or other type of advertising, and, where applicable, the main profiling criteria used; it should also inform the recipient about any means available for them to change such criteria».

[54] The EDPB Guidelines 3/2025, cit., par. 87, stipulates that «Providers of VLOPs and VLOSEs may only use a recommender system based on profiling after the recipient of the service has chosen this option. In addition, while the non-profiling based option is active, the provider of the online platform cannot lawfully continue to collect and process personal data to profile the user, for the purposes of future recommendations, e.g. to be prepared in case the user chooses the profiling-based option or to provide more relevant recommendations because they would be based on a more detailed profiling. In addition, where a user uses both versions of a recommender systems, for example by switching several times in the same day, i.e. the version based on profiling and the version not based on profiling, then that user should not be profiled during the use of the version not based on profiling».

[55] EDPB Guidelines No. 3/2025, cit., pars. 51-56, «Article 26(1) DSA lays down transparency rules for providers of online platforms specifically regarding advertising. This provision states that information regarding each specific advertisement should be provided to the recipients of the service in real time. Additionally, meaningful information regarding the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, information about how to change those parameters as specified in Article 26(1)(d) DSA must be directly accessible from the advertisement. It means that the elements of information mentioned in Article 26 DSA should be provided in real time, directly accessible from the advertisement, while information related to transparency obligations as set out in Articles 13 and 14 GDPR could be presented through the means of a privacy policy (e.g., one click away). It also means that information required under Article 26 DSA would be provided after a processing of personal data may have occurred. This is an important difference between Article 26 DSA and the transparency requirements under the GDPR, since the latter provides that in case of personal data collected directly from the data subject, information shall be provided at the time when personal data are obtained, as set out in Article 13(1) and 13(2) GDPR, before the processing takes place … Moreover, if processing for advertising purposes is based on consent (Article 6(1)(a) GDPR), certain information regarding processing (including profiling) must already be provided to the

When advertising falls under the scope of Article 3, point 2) of Regulation (EU) 2024/900 (TTPA) [56], which contains the definition of political advertising, the threats brought about by profiling can be extensive and impinge upon the correct functioning of democratic processes [57]. Consequently, profiling based on special categories of personal data is forbidden (Article 18, par. 1(c)). In this case, Recital 79 of the TTPA clearly specifies that «profiling using special categories of personal data encompasses profiling using special categories of personal data evaluated from personal data which are not themselves special categories of personal data. This could be the case, for instance, if a data controller uses personal data which are not special categories of personal data to categorise data subjects as having certain religious, philosophical or political beliefs, and regardless of whether that categorisation is true. It should not matter how the category is labelled if the processing of personal data reveals a special category

individual before consent is collected. Additional information pursuant to Article 26(1)DSA would later be directly and easily accessible to the recipient from the advertisement».

[56] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (the TTPA), in its Article 3, point 2), states that «'political advertising' means the preparation, placement, promotion, publication, delivery or dissemination, by any means, of a message, normally provided for remuneration or through in-house activities or as part of a political advertising campaign: (a) by, for or on behalf of a political actor, unless it is of a purely private or a purely commercial nature; or (b) which is liable and designed to influence the outcome of an election or referendum, voting behaviour or a legislative or regulatory process, at Union, national, regional or local level».

[57] The amplitude of such risks is declared in Recital 6 of the TTPA, in reference to political microtargeting: «such techniques may present particular threats to legitimate public interests, such as fairness, equal opportunities and transparency in the electoral process and the fundamental rights to freedom of expression, to privacy and the protection of personal data and to equality and non-discrimination, and the right to be informed in an objective, transparent and pluralistic way»; or, in a more extensive way, by Recital 74 of the TTPA: «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 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».

of personal data» [58]. In addition to this limit, already envisaged by the DSA for general advertisements, a further constraint is added. Profiling is reduced in scope, since only personal data directly collected from the data subject with his/her explicit consent can be processed to display targeted political advertising (Art. 18, par. 1(a) of the TTPA). The introduction of limits to the number of categories of data that can be combined for targeted political advertising is also suggested [59]. Moreover, in order to preserve the validity of consent, the data subject must be offered an equivalent alternative which allows him/her to use the online service without receiving political advertising [60]. However, there is a missed opportunity in respect of similar significant boundaries on profiling: the legislation is focused on what can be defined as political advertising and does not extend to recommender systems that manage the kind and priority of content displayed to the recipient of the service, which can have similar political relevance.

In addition to the above-described protections of data subjects and recipients of services "from" the market, Regulation (EU) 2022/1925 (DMA) [61] lays down provisions addressed to the protection "of" (the correct functioning of) the market [62]. The DMA could be deemed to deal with aspects that (directly and indirectly) draw boundaries on profiling to fulfil both of the following aims: (1) the contestability of the market; and (2) the protection of end users. The former (the contestability of the market) is safeguarded by the DMA's attempts to limit intrusive profiling, since making deep consumer profiling the industry standard would represent a barrier against potential entrants or start-ups because they cannot access data to the same extent, depth, and scale as the gatekeepers [63]. The latter (the protection of end users) is a consequence of this and is upheld by Article 5 of the DMA. More specifically, this Article prevents gatekeepers, in the absence of explicit consent given by the end user, from carrying out the

[58] Recital 79 of the TTPA.

[59] According to Recital 78 of the TTPA: «to help prevent manipulative microtargeting, it is essential that providers of political advertising services take specific measures to ensure that the personal data which is collected and processed for the purpose of targeting and ad delivery of political advertising is limited to what is necessary in relation to that purpose, for instance by restricting the availability of options for targeting and ad delivery of political advertising offered to service recipients to those which require only the combination of up to five categories».

[60] Art. 18, par. 4(b), of the TTPA.

[61] 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 (DMA).

[62] M. OROFINO, *Il* Digital Market Act: *una regolazione asimmetrica a cavallo tra diritto alla protezione dei dati e diritto antitrust*, in F. PIZZETTI (ed.), *La regolazione europea della società digitale*, Torino, 2024, p. 175 ff.

[63] See Recital 72 of the DMA.

series of personal data processing practices that are usually necessary for in-depth inferences to form the basis of both personalised advertising (Article 5, par. 1(a)) [64] and personalised content or services (Article 5, par. 1(b)(c)(d)) [65]. The «Joint Guidelines on the Interplay between the DMA and the GDPR», recently adopted by the European Commission and the EDPB, underline that the prohibition on the cross-use of personal data from core platform services in other services and vice versa covers the case of different services provided separately, not the case of services that are provided together or in a mutual supportive way, or third-party services (par. 61) [66]. In this last respect, consent is

[64] Under Article 5, par. 1(a), gatekeepers are prevented from processing, for the purpose of providing online advertising services, personal data of end users using the services of third parties that make use of the core platform services of the gatekeeper.

[65] Pursuant to Article 5, par. 1, gatekeepers are prevented from: (point (b)) combining personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services; (point (c)) cross-using personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa; and (point (d)) signing in end users to other services of the gatekeeper in order to combine personal data.

[66] According to the Joint Guidelines on the Interplay between the DMA and the GDPR, par. 61: «Article 5(2), point (c) DMA prohibits a gatekeeper from cross-using personal data from a relevant CPS [core platform service] in other services that it provides separately, including other CPSs, and vice versa, without the end user's valid consent. In contrast, Article 5(2), point (c) DMA does not require gatekeepers to obtain consent in instances of cross-use of personal data between a CPS and gatekeeper services that are provided together with or in support of a CPS, or for the cross-use of personal data with third party services». The following par. 67 states that «Article 5(2), point (c) DMA does not inhibit cross-use of personal data that is required to offer the essential functionalities of certain services», such as payment, identification services or online advertising, which «can, in principle, also be considered as services provided together with, or in support of, the gatekeeper's relevant CPS on which ads are displayed». In this last regard, the guidelines underline that a gatekeeper's online search engine CPS can, without consent, cross-use the single search query in its online advertising service, since this may be considered strictly necessary in order to display an ad on the online search engine. In that case, the search query can therefore be cross-used without end user consent under Article 5(2) DMA in order to provide an ad result (par. 70), provided that «processing … [that is] limited [to a] set of on-platform personal data, such as geography (as opposed to precise location), language and content, as well as topics of interest as actively provided by the end user, might not require consent. If processing operations do not involve intrusive measures, such as profiling and tracking, and do not go beyond the reasonable expectations of the end users, it may be possible to rely on Article 6(1), point (f) of the GDPR» (par. 75). However, «the material and temporal scope of the personal data that is cross-used should therefore be limited to what is strictly necessary to offer the interconnected functionalities to cross-use personal data without consent. As a consequence, the retention of personal data that has been cross-used by the gatekeeper should be limited to the time required to carry out the relevant functionality» (par. 69).

not a necessary requirement, and compliance with the GDPR could be achieved through other legal bases, such as the necessity to perform a contract, or legitimate interest [67]. However, «processing operations … [which] involve intrusive measures, such as profiling and tracking» [68] remain forbidden in all cases. Accordingly, when personal data gathered on a platform are cross-used in a supporting service and such processing entails deep profiling activities, consent remains the only legal basis [69]: «certain cross-uses of on-platform data in a supporting advertising service of the gatekeeper may require the latter to obtain consent under the GDPR. This may be the case where such cross-use entails the processing of high volumes and a large variety of types of personal data or involves personal data that allows information falling within Article 9(1) GDPR to be revealed about end users» [70].

The DMA, like the DSA for VLOPs, VLOSEs and their recommender systems, or the TTPA for political advertising, obliges gatekeepers to offer a less personalised alternative, stipulating that this shall not be different from or of lower quality than services provided on the basis of profiling [71].

Furthermore, in order to protect the data subject "from" the market, but also for the protection "of" the correct functioning of the market, Regulation (EU) 2023/2854 (Data Act) [72] states that gatekeepers are excluded from the right to data access and data availability (Article 5, par. 3 and Article 6, par. 2(b)). In addition, third parties who receive data from a data holder upon a request from the user of a connected product or related service are prevented from processing such data for profiling (par. 2(b)). This last prohibition narrows the scope of the

[67] Par. 72 of the Joint Guidelines, cit., underlines that «Provided that their respective conditions are effectively complied with, the lawful grounds of Article 6(1), point (b) or (f) GDPR may be appropriate lawful grounds for the cross-use of personal data between a CPS and another gatekeeper service without end user consent, where both services are provided together with or in support of each other».

[68] Par. 75 of the Joint Guidelines, cit.

[69] As specified in par. 77 of the Joint Guidelines: «certain cross-uses of on-platform data in a supporting advertising service of the gatekeeper may require the latter to obtain consent under the GDPR. This may be the case where such cross-use entails the processing of high volumes and a large variety of types of personal data or involves personal data that allows information falling within Article 9(1) GDPR to be revealed about end users, in a manner that goes beyond their reasonable expectations or that may otherwise have a significant impact on their rights and freedoms».

[70] Par. 77 of the Joint Guidelines, cit.

[71] Recitals 36 and 37 of the DMA and Article 13, par. 6 of the DMA.

[72] Regulation (EU) 2023/2854 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).

ability to carry out automated profiling envisaged by Article 22 pars. 2(a) and (c) of the GDPR, since there is no possibility of derogation. Except for this case that "cuts" profiling at its source irrespective of the consequent practice it enables, the above-mentioned legal acts (the GDPR, DSA, DMA and TTPA), when dealing with automated profiling, refer their protection to particular use-cases, primarily targeted advertising and recommender systems. In addition, they essentially build up their safeguards on the requirements of transparency and the explicit consent of the data subject.

In turn, the AI Act defines, in an absolute way and without the possibility of derogation, AI systems that perform profiling on a natural person in the domains listed in Annex III of that Act as high-risk. [73] It then prohibits AI-enabled profiling in reference to some of the listed practices, provided that certain conditions are met. This prohibition encompasses social scoring activities [74], predictive policing or justice [75], inference of emotion [76] in the workplace or an education institution [77], and individual biometric categorisation of sensitive

[73] According to Article 6, par. 3 of the AI Act, «an AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons».

[74] Article 5, par. 1(c), of the AI Act prohibits «the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following: (i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected; (ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity». As explained by the EC Guidelines on prohibited AI practices, cit., par. 154, since the definition makes reference to the concepts of "evaluation", "inferred characteristics" and "predicted characteristics", it also includes profiling activities.

[75] Article 5, par. 1(d), of the AI Act prohibits «the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity».

[76] As specified by the EC Guidelines on prohibited AI practices, cit., pars. 244-246, «The prohibition in Article 5(1)(f) AI Act does not refer to 'emotion recognition systems', but only to 'AI systems to infer emotions of a natural person'... 'Inferring' is done by deducing information generated by analytical and other processes by the system itself. In such a case, the information about the emotion is not solely based on data collected on the natural person, but it is inferred from other data, including machine learning approaches that learn from data how to detect emotions».

[77] Article 5, par. 1(f), of the AI Act prohibits «the placing on the market, the putting into

profiles [78]. The lowest common denominator of these forbidden practices is essentially strong subjective-oriented profiling. More specifically, they are cases in which a physical, physiological, behavioural or psychological analysis is carried out in order to make inferences about: (1) personal aspects for scoring (in the case of social scoring); (2) feelings and emotions (in emotion recognition); (3) beliefs and personal orientations (in biometric individual categorisation); or (4) the probability of committing future offences or repeating past offences (in predictive policing and predictive justice).

4. A Proposal for a "Re-Oriented" Regulatory Approach

The European Commission's consultations on the so-called Digital Omnibus Package ran from September 16th, 2025 to October 14th, 2025 [79], and the Commission released its consequent draft proposals on November 19th, 2025 [80]. The

service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons». As explained by the EC Guidelines on prohibited AI practices, cit., par. 249, «Recital 18 AI Act clarifies that emotions or intentions do not include 'physical states, such as pain or fatigue, including, for example, systems used in detecting the state of fatigue of professional pilots or drivers for the purpose of preventing accidents.' It further clarifies that emotion recognition systems do not include 'the mere detection of readily apparent expressions, gestures or movements, unless they are used for identifying or inferring emotions', which should be understood to also apply to Article 5(1)(f) AI Act. Those expressions can be basic facial expressions, such as a frown or a smile, or gestures such as the movement of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whispering. However, when these readily apparent expressions or gestures are used for identifying or inferring emotions or intentions, they are covered by the prohibition».

[78] Article 5, par. 1(g) of the AI Act forbids «the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise 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; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement». As specified by the EC Guidelines on prohibited AI practices, cit., par. 272: «A wide variety of information, including 'sensitive' information, may be extracted, deduced or inferred from biometric information, even without the knowledge of the persons concerned, to categorise those persons».

[79] See https://ec.europa.eu.

[80] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital

declared purpose is to streamline existing EU regulations [81] that indeed demonstrate a piecemeal approach.

We agree with this goal of simplifying the current provisions and re-ordering them in a more systematic way. However, our objective is for the multiple implications of the machine learning profiling of people to be tackled in a better way. Our first concern is its scale and scope: people are constantly within a "digital lab" made of pervasive assessments and judgements, grounded on inferences which have not only moved a long away from a limited set of objective and verifiable data but are also devoid of the traditional ethical and legal guarantees that are usually imposed on experiments conducted within a "real lab" or judgements authorised and regulated by the law. Second, this profiling uses a subjective approach, dealing with the assessment of personal aspects and personality traits, and its results may impinge upon the internal sphere of the individual, a space that a democratic legal system usually deems to be "holy" and "outside the scope" of external interference. The third aspect is its cross-cutting amplitude, since its inferences can leverage different practices (from nudging to neuromarketing to dark patterns to discriminatory decisions), as well as being addressed to different contents or services concerning different domains (from the economic field to the social and political fields).

All this considered, we propose a regulatory technique that takes the critical mass of the achievements already evident in the existing EU legislation with the purpose of fine-tuning them to the multiple challenges posed by the machine learning profiling of people.

The regulatory techniques posited by the legislative acts dealt with in the previous paragraphs, as well as belonging to the area of competition law when oriented to the protection of the correct functioning of the market, enter the

legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) - COM(2025) 837 final; Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM(2025) 837 final.

[81] See section B of the Call for Evidence – Digital Omnibus, where it is states the following as one of the objectives: «Reduce compliance costs for businesses across all sectors in relation to the access, use and sharing of data by reducing fragmentation of rules and their application and by clarifying the rules and requirements that apply and by cutting obligations where a less costly alternative exists. Reduce cookie consent fatigue, strengthen users' privacy rights online, with clear and straight-forward information and options for managing cookies; facilitate the use of cookies and other technologies for businesses for increased data availability. The initiative will pursue a stronger alignment with the general rules on the protection of personal data under the EU data protection law, potentially including modernised rules on cookies under that framework when personal data are collected through such technologies».

realm of consumer protection law when transparency, information notices, valid consent and alternative options are required. In addition, they enter the domain of the regulation of product safety, with transparency, technical requirements, technical documentation, data governance, and testing and monitoring duties being imposed for high-risk artificial intelligence systems. Moreover, they result in the conferral of rights, extending those already provided by the GDPR [82]. Last but not least, a precautionary stance has also been implemented by the EU legislator, by means of the prohibition of some AI practices or the prohibition on making use of special categories of personal data.

Taking stock of this, the proposed regulatory technique consists of an incremental but simplified approach in order to create boundaries for machine learning profiling and push this activity back to the "lowest common denominator" that usually features in the cases, expressly foreseen by the legal system, of authorised judgements and profiling of people. All this should be done without lifting the legal safeguards but by fine-tuning them to address the implications of algorithmically-driven inferences and making them more efficient and effective.

For this purpose, a preliminary consideration needs to be made. This stands on the (already mentioned) "quantum leap" and thus on the distinction between, on the one hand, data that are provided and generated by the data subject and, on the other hand, data that are inferred about people's personal aspects and traits. This is not only a technical distinction: it has received legal status. More specifically, the legal system itself has recognised a demarcation point between data provided and generated by the data subject or the users, on the one hand, and inferred or derived data, on the other. This is the stance adopted by the provisions of the GDPR, the DMA and the Data Act when dealing with the right to data portability, real-time access to data and the right to data availability. In particular, inferred data are outside the scope of these rights, since they are the outcome of an additional and complex algorithmic activity that falls under the domain of the data controller [83], the data holder [84] or the gatekeeper [85]. Consistently, it is the legal system itself that has erected a boundary beyond which data

[82] For instance, as mentioned, the Data Act extends the right to data portability (as does Article 6, par. 9 of the DMA) and introduces the right to real-time, continuous access to data and the right to data availability. The DSA extends the right to receive meaningful information on the logic involved in automated data processing (including profiling), referring to the "main parameters" used in carried out profiling and the consequent right to change them (see the clear explanation given by Recital 68).

[83] Article 20 GDPR.

[84] Articles 3, 4, 5 of the Data Act.

[85] Article 6, par. 9, DMA.

exit the domain of control of the data subject or user and enter the domain of the data holder.

Bearing this in mind, the aim of the regulatory technique we propose is to concentrate on this demarcation point, and the consequent division of the spheres of controllability of data between the data subject and the operator (to use a more neutral term than the ones used in the EU legislation mentioned above), which is the entity who decides on the inferential process for the profiling goals. In this regard, it is worth noting that, in our opinion, the traditional regulatory technique, which relies upon transparency requirements and consent, could be deemed consistent and adequate for placing safeguards to protect data subjects when the data are still within their margin of manoeuvre (and thus when we are dealing with data provided or generated by the data subject). Consequently, we hold that a regulatory technique made of prohibitions and derogations fits the purpose of regulating the procedural aspects that lead to the creation of inferred data, with specific regard to profiling, provided that the "demarcation point" mentioned above is borne in mind.

The baseline of our proposed regulatory technique consists of setting out prohibitions which limit profiling in scale and scope and in this way recover the "lowest common denominator" that makes the data more strongly required to be objective and verifiable; this is what is usually done by a democratic legal system when it explicitly authorises and regulates cases of judgements being made on people, including automated personal data processing (see section 2 above). For this goal to be attained, two intertwined factors are to be taken into consideration, since both contribute to the reduction of in-depth profiling: on the one hand, the categories of data that can be fed into machine learning algorithms; and, on the other hand, the kind of processes these algorithms are allowed to carry out.

As for the former, following the pattern laid down by Article 18, par. 1(a) of the TTPA (whose scope is limited to political advertising), profiling should only be allowed with respect to personal data directly collected from the data subject but excluding special categories of personal data, as also enshrined by the DSA and the TTPA, again in reference to advertising [86]. In this last respect, it should in particular be clearly stated in the binding part of the legal text, and not just in the recitals or in soft law as has been done until now, that the output data of algorithmic inferences are also considered one of the special categories of personal data, even when the input data do not belong to a special category.

As for the latter (the processes run by machine learning algorithms), constraints should be imposed on combining and cross-using data across different

[86] Articles 26, par. 3 and 28 of the DSA. Article 18, par. 1(c) of the TTPA.

services or third-party services, as is done by the DMA. [87] These are preliminary prohibitions, a baseline, as said. Unlike in the model followed by the DMA, the DSA and the AI Act, these constraints should be placed on the "operator", irrespective of the kind of practices triggered by the profiling (targeted advertising, personalised recommender systems, dark patterns, social scoring, emotion recognition, etc.), and irrespective of the operator's size.

This bedrock acquired, it makes sense to recover a further regulatory pattern followed by the EU legislator, which relies upon transparency and consent. Such regulatory safeguards are dispersed and disseminated in different articles in various legislative acts (the GDPR, the DSA, the DMA, the TTPA, the AI Act, and the Data Act) and it would be worth re-ordering them, since they serve the purpose of enhancing the margin of manoeuvre of the data subject *vis-à-vis* machine learning profiling. On the one hand, there is the provision to the data subject, end user or recipient of services (as they are variously called across the EU legislation) of meaningful information about automated profiling, the logic involved, its main parameters, the possibility of changing those parameters, and the significance and envisaged consequences of such processing for the person [88]. On the other hand, there are the requirements for valid consent. The conditions for valid consent have been strengthened over time (from the GDPR, to the DSA, the DMA, and the TTPA, passing through the ECJ's *Meta Platforms* case), by adding the offer to the data subject of an alternative but equivalent option devoid of profiling.

To recap what has been argued, the baseline of prohibitions mentioned above is intended to scale down machine learning profiling and shift it to a process that lies closer to the sphere of checkability, knowledge and understanding of the data subject. This step should make the protection stemming from the information notice and consent more significant and adequate, since the resulting inferences could not undertake the "quantum leap" that detaches them completely from the link with the data subject and the sphere of his/her awareness. The outcome is a closer boundary on inferences, and thus a decreased capability for in-depth insights on people by profiling them. Therefore, the streamlining could be considered to be accomplished without lifting legal safeguards: at the end of the process, automated profiling and the inferences involved would be more strictly related to the data subject, more easily monitored by him/her and also more verifiable and checkable. In this way, the rights-oriented approach

[87] Article 5, pars. 1(a), (b), (c), (d) of the DMA.

[88] See Articles 13, par. 2(f); 14, par. 2(g); 15 par. 1(h); and 22 of the GDPR; see also Article 86 of the AI Act; Articles 26, par. 1(d); 27, pars. 1-2; and 38 of the DSA; Article 18 of the TTPA; Article 5, par. 2 of the DMA.

featured in the GDPR would be recovered in its entire significance.

However, this could not be considered to bring us to the end of the path: a further step should be taken. More specifically, the suggested solution needs to be tested against the principle of necessity and proportionality, and we need to show that a legitimate aim is pursued. The legitimate aim of the above-described prohibition is evident, because of both the individual and the high systemic risks involved in machine learning profiling, which leads to evaluations involving people's personal aspects and personality traits, and in this way impinges upon well-known fundamental freedoms and rights. The means identified to tackle the issue, which are aimed at scaling down the power of inferences, are composed of both the reduction of the set of data fed into a machine learning algorithm and limits on how these data can be processed, as such making the process more verifiable. By acting in this way, the legal system recovers the protections usually erected in permitted cases of judgements and assessments on people.

However, in order to make this solution proportionate, a possibility should be given of a margin of manoeuvre of the data controller, the digital service provider or the provider or deployer of an artificial intelligence system (which have briefly been named "operators"), since they may hold overriding interests underpinning the necessity of in-depth profiling. Therefore, the legal system should provide them with the possibility of lifting the prohibitions erected around machine learning profiling but impose on them the burden of proof. As a result of their technological, economic and/or socio-political power, they occupy the most suitable position to bear this burden of proof. Thus, the choice seems to be reasonable and proportionate and to aim to strengthen the accountability principle, already enshrined in the GDPR [89]. In particular, if they believe they hold a legitimate interest in carrying out machine learning profiling on the basis of huge amounts of data (not only data directly provided by the data subject, but also data observed, derived and inferred, cross-used and combined throughout different services and sources and being personal data of different categories), they should first bear the proof that their interests are of an overwhelming nature as against the rights and freedoms of the data subjects. It is only in this case that judgements and evaluations by strong inferential processes based on personal aspects and personality traits would be permitted. In addition, the preventive authorisation should be given on a case-by-case basis by a competent and independent supervisory authority, which would follow quickly-

[89] S. CALZOLAIO-L. FEROLA-V. FIORILLO-E.A. ROSSI-M. TIMIANI, *La responsabilità e la sicurezza del trattamento*, in L. CALIFANO-C. COLAPIETRO (eds.), *Innovazione tecnologica e valore della persona – Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, p. 137 ff.

evolving technological developments and fast-changing socio-economic conditions and avoid the rigidity of a legally enshrined list of practices. This means that the solution is different from that adopted by both the GDPR, under which the assessment of the overriding legitimate interest of the data controller is left to the data controller themselves, and the AI Act, under which the evaluation of a high risk in order to mitigate that risk is left to the provider and deployer of the system.

In this way, the challenging path initiated by the AI Act of listing out forbidden use-cases would be reversed and streamlined: it is not for the legislator to struggle to draft and keep updated such a list, with the implied risk of ineffective provisions due to overinclusive or underinclusive lists or interventions made too late or too early [90]. This is instead a task for the "operator", who holds the necessary technical competences, as well as a more comprehensive knowledge and understanding, to cope with the burden of proving the usefulness, for a specific goal, sector or for society at large, of the automated and in-depth inferences it wishes to undertake on people. Obviously, all the principles that make personal data processing lawful must be respected, including the carrying out of a Data Protection Impact Assessment (DPIA, Article 35 of the GDPR) and a Fundamental Rights Impact Assessment (FRIA, Article 27 of the AI Act) [91], as well as all the requirements set out in Chapter III, Section 2 of the AI Act for high-risk systems.

Last but not least, the legislator obviously retains what is already in place: the pre-emptive right to declare that in certain cases automated inferences are permitted, when the dominance of the public and collective interests has already

[90] In this respect, M. EBERS, *Truly Risk-Based Regulation of Artificial Intelligence. How to Implement the EU's AI Act*, in *The European Union Law Working Paper Series*, Stanford-Vienna, No. 101, 19th June 2024, p. 15, observes that «The AI Act provides a broad and rather abstract classification of high-risk systems under Annex III. Instead of providing a risk classification on a case-by-case basis, the Act uses a pre-defined, closed list of typical high-risk applications. Whether an AI system used in a specific sector for specific purposes poses a high risk to health, safety and/or fundamental rights, is not assessed for the *concrete* risk, but is pre-defined for typical cases in Annex III … The choice of such a top-down regulation raises several issues. First, this approach leads to over-regulation where, for instance, an AI system falls into one of the eight categories listed in Annex III, but in reality does not pose a significant risk of harm. Second, the list of typical high-risk AI systems (albeit with broad definitions and open to updating) may not be easy for the European Commission to keep up to date in a timely manner, given how rapidly AI technology is evolving. Moreover, the decision to delegate (to the Commission) the power to amend Annex III by adding, modifying and removing high-risk AI systems (Art. 7 AI Act) raises concerns in terms of power allocation».

[91] As for the different scopes of, and the consequent relationship between, a DPIA and a FRIA, see O. POLLICINO, *DPIA e FRIA: guida completa alla valutazione del rischio nell'IA*, in *agendadigitale.eu*, 10 November 2025; N. LÖLFING.-C. BISCHOFF-BRIEL-A. DIECKHOFF, *Data Protection Law*, cit., pp. 362-365.

been balanced by the regulator itself, provided that adequate procedural safeguards, as well as relevant, objective and verifiable data to feed the machine learning algorithms, are identified.

In conclusion, since regulatory techniques are not only formal and procedural safeguards but are also substantial guarantees of the effectiveness of constitutional principles, rights and freedoms, it is deemed that the proposed regulatory approach is able to streamline existing EU digital regulations, making them more effective without reducing the legal protection.