THE PROTECTION OF INDIVIDUALS AGAINST PRIVACY-INVASIVE AND DISCRIMINATORY INFERENCES UNDER EUROPEAN LAW: FROM THE GENERAL DATA PROTECTION REGULATION AND THE DIGITAL CONTENT AND SERVICES DIRECTIVE TO THE ARTIFICIAL INTELLIGENCE ACT

*Prof. Gina Gioia**
*Sofia Maria Lener, LL. M.***

UDK: 347.121:004.7/.8
347.71:004.7/.8
342.738(4)EU
339.923:061.1>(4)EU
DOI: 10.3935/zpfz.74.56.6
Pregledni znanstveni rad
Primljeno: veljača 2024.

Inferences are information relating to an identified or identifiable natural person generated using machine learning techniques, allowing probabilistic correlations between input data to be discovered and predictions made in new cases. Inferences carry many risks: they are inherently uncertain, predictions are only as reliable as the data on which they are based, and inferences can be used to nudge and manipulate individuals. It is essential to prevent these risks, and where they materialise, provide appropriate protection. This paper examines whether current European legislation adequately addresses these issues. The first task is to classify inferences to

* Gina Gioia, Ph. D., Associate Professor, University of Tuscia, Department of Legal, Social, and Educational Sciences, Via Santa Maria in Gradi 4, 01100 Viterbo, Italy; gina.gioia@unitus.it;
ORCID ID: orcid.org/0000-0002-4542-9711

** Sofia Maria Lener, LL. M., Ph. D. candidate, University of Tuscia, Department of Legal, Social, and Educational Sciences, Via Santa Maria in Gradi 4, 01100 Viterbo, Italy; sofiamaria.lener@leplex.it;
ORCID ID: orcid.org/0000-0003-1980-9152

determine whether they fall within the concept of personal data and are this covered by European personal data laws. This analysis considers both possibilities – treating inferences as personal and non-personal data – and evaluates the relevant regulatory frameworks, including the General Data Protection Regulation, the Proposal for a Regulation on Privacy and Electronic Communications, Digital Content and Services Directive, and the Artificial Intelligence Act.

Key words: Italian consumer law; termination of the contract; privacy-invasive and discriminatory inferences; protection of individuals

1. INTRODUCTION

The relentless advancement of technology makes it increasingly challenging to ensure the effective protection of information about individuals, particularly when such information is gathered using artificial intelligence (AI). The recent enforcement of the Directive (EU) 2019/770 (Digital Content and Services Directive, DCSD)[1] prompts reflection on a topic that remains underexplored in the literature. Among these concerns, inferences made by AI merit special attention. AI systems identify probabilistic correlations between personal data collected from various sources and process these to produce new personal information. Such inferences are inherently uncertain, as they are generated by unknown automated processes – sometimes in violation of privacy rights and, in some cases, with discriminatory outcomes. The use of inferences is expanding exponentially and increasingly forms the basis of decisions impacting individuals' economic and social lives. Yet, no EU legislation directly addresses the protection of individuals from unlawful inferences. This paper analyses relevant EU legislation, both currently in force and still in the drafting stage, to assess its applicability in governing inferences and its adequacy in providing individuals with protection. To begin this analysis, it is essential to define what is meant by "inferences" and to clarify how AI is used to generate them.

[1] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, Official Journal, L 136, 22 May 2019.

2. ARTIFICIAL INTELLIGENCE, INFERENCES, AND RISKS

Despite its widespread use, no universally accepted definition of AI currently exists.[2] Over time, AI has been described in various ways[3], with numerous definitions even at the European level. Notably, the European Commission aims for a technologically neutral definition. In the Proposal for a Regulation laying down harmonised rules on AI (AI Act)[4], an AI system is defined as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".[5]

Today, we are experiencing a period of great diffusion and development of AI, driven by hardware with vast computational capabilities, immense volumes of globally produced data, and machine deep learning techniques.[6] The shift from "expert systems", capable of solving problems based on specific, structured knowledge ("knowledge-based systems"), to adaptive systems with autonomous learning capabilities based on experience (machine learning) underpins the current success of AI.[7]

[2] See Angelini, R., *Intelligenza Artificiale e governance: Alcune riflessioni di sistema*, in: Pizzetti, F. (ed.), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, pp. 293–318.

[3] The AI-Watch, developed by the Joint Research Centre in December 2018 following the publication of the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Coordinated Plan on Artificial Intelligence, COM(2018) 795 final, 7 December 2018, has compiled definitions of AI used between 1955 and 2021 in academic, industrial, and corporate perspectives: Samoili, S.; Lopez Cobo, M.; Gómez, E.; De Prato, G.; Martínez-Plumed, F.; Delipetrev, B., *AI Watch: Defining Artificial Intelligence 2.0: Towards an operational definition and taxonomy of artificial intelligence*, Publications Office of the European Union, Luxembourg, 2021.

[4] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM(2021) 206 final, 21 April 2021.

[5] Article 3(1) AI Act.

[6] Gabbrielli, M., *Dalla logica al deep learning: una breve riflessione sull'intelligenza artificiale*, in: Ruffolo, U. (ed.), *XXVI lezioni di diritto dell'intelligenza artificiale*, Giappichelli, Torino, 2021, pp. 26–27.

[7] Sartor, G., *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, European Parliamentary Research Service, Brussels, 2020, pp. 8–9; Casadei, T.; Pietropaoli, S., *Intelligenza artificiale: fine o confine del diritto?*, in: Casadei, T.;

There are three primary methods of machine learning: supervised learning, reinforcement learning, and unsupervised learning. In supervised learning, the system uses a data set – the training set – comprising input-output pairs to form a function it applies to new inputs, as seen in recruitment systems where a candidate's profile is associated with application outcomes and then the correlation between the two is applied to all new candidates. In reinforcement learning, the system deduces data by observing the environment and adjusting its actions to achieve a set goal, using feedback in the form of rewards, such as a game system refining strategies based on previous results. Unsupervised learning resembles supervised learning but lacks defined inputs and outputs, so the system groups data based on similarity or proximity.[8]

From this brief description, two points emerge: first, some AI systems require data to form a model; second, using the model, other data can be inferred. Specifically, machines use probabilistic correlations among input data to derive predictors and make predictions, thus arriving at a "target".[9] To infer data, therefore, means to make automated predictions and evaluations based on a set of data.

To give a few examples, an AI system can estimate the probability of recidivism for convicted offenders based on characteristics such as mental health, education, or family circumstances, or asses a potential borrower's creditworthiness using data on previous borrowers and their creditworthiness.[10] The more input data available, the higher the accuracy of the inferred data. Hence, the enormous relevance of Big Data[11], which is defined in the scientific literature

Pietropaoli, S. (eds.), *Diritto e tecnologie informatiche: Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters Kluwer CEDAM, Padova, 2021, pp. 222–223.

[8] D'Acquisto, G., *Intelligenza artificiale*, Giappichelli, Torino, 2018, p. 127; High-Level Expert Group on Artificial Intelligence, *A Definition of AI: Main Capabilities and Disciplines*, European Commission, Brussels, 2018, p. 4.

[9] Sartor, *op. cit.* (fn. 6), p. 15.

[10] See, for example, the *Compas* software, which can assess an individual's risk of reoffending and social dangerousness: Zaccaria, G., *Figure del giudicare: calcolabilità, precedenti, decisione robotica*, Rivista di diritto civile, *vol.* 66, no. 2, 2020, p. 291; Carratta, A., *Decisione robotica e valori del processo*, Rivista di diritto processuale, *vol.* 75, no. 2, 2020, p. 511; Signorato, S., *Giustizia penale e intelligenza artificiale: Considerazioni in tema di algoritmo predittivo*, Rivista di diritto processuale, *vol.* 75, no. 2, 2020, p. 611.

[11] Statista predicts that the global Big Data market will grow to 103 billion U.S. dollars by 2027: *Big data market size revenue forecast worldwide from 2011 to 2027*, Statista, March 2018, https://www.statista.com/statistics/254266/global-big-data-market-forecast/ (12 December 2022).

with the “4 Vs”: the Volume of data collected, Variety of sources, Velocity with which data analysis can take place, and Veracity of the data that could (presumably) be achieved through the analytical process or, alternatively, Value that the data take on when analysed.[12]

Among the input data used to train AI systems there can be – and, indeed, often are – personal data. However, personal information can also be inferred through machine learning methods: we are talking, in this case, about inferences, data from data[13], or information inferred from data[14], i.e., information about an identified or identifiable natural person created by deduction or reasoning rather than simple observation or collection from the person concerned.[15] Inferences may also form the basis of automated decisions, i.e., decisions made by an AI system without human intervention.[16]

The use of inferences brings substantial benefits and opportunities. AI systems can considerably reduce the risk of unequal treatment, discrimination, and errors inherent in human decision-making, offering far more accurate and unbiased predictions than humans can make, and benefiting disadvantaged groups.[17] Algorithms on which AI systems are based, for instance, can be designed to disregard distinctions based on ethnicity, census, or gender.[18]

While these benefits are significant, potential risks are equally numerous. As noted, AI systems derive conclusions from data, using machine learning

[12] Sicular, S., *Gartner’s Big Data Definition Consists of Three Parts, Not to Be Confused with Three “V”s*, Forbes, 27 March 2013, https://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/ (12 December 2022); *Big Data*, Gartner, https://www.gartner.com/en/information-technology/glossary/big-data (12 December 2022).

[13] Pizzetti, F. (ed.), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, p. 42.

[14] Finocchiaro, G., *Riflessioni su intelligenza artificiale e protezione dei dati personali*, in: Ruffolo, U. (ed.), *Intelligenza artificiale: Il diritto, i diritti, l’etica*, Giuffrè, Milano, 2020, p. 245.

[15] Wachter, S.; Mittelstadt, B., *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, Columbia Business Law Review, no. 2, 2019, p. 515.

[16] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 17/EN, WP251rev.01, 2018, p. 8.

[17] Kleinberg, J.; Ludwig, J.; Mullainathan, S.; Sunstein, C. R., *Discrimination in the Age of Algorithms*, Journal of Legal Analysis, *vol.* 10, 2018, p. 154.

[18] Sunstein, C. R., *Algorithms, Correcting Biases*, Social Research: An International Quarterly, *vol.* 86, no. 2, 2019, p. 508.

techniques, resulting in knowledge that is probable but inherently uncertain. Typically, neither the training data set (and their provenance and quality) nor the process used by the system is transparent, creating the problem of *explainability* and complicating the individual's ability to understand how data used by a machine learning system contribute to reaching certain conclusions. Consequently, the accuracy of such predictions is inextricably dependent on the input data; predictions can be reliable only if the underlying data is accurate.[19] Furthermore, the training set of an AI system may contain biases that are amplified through machine learning.[20] If an AI system is trained on discriminatory human judgments, the algorithm will likely reflect these flaws, producing decisions that are at least incorrect. Finally, there is a risk of individual stereotyping classified according to automated predictions. Emblematic is the case where an AI system infers an unfavourable prognosis from health data and uses this to deny insurance coverage or employment opportunities.[21]

3. INFERENCES AND EUROPEAN LEGISLATION

The aforementioned risks associated with inferences must be prevented, and where they materialise, appropriate protection must be provided. It is therefore necessary to assess whether current European legislation is adequate in this regard.

To this end, the first issue to be addressed is the classification of inferences, specifically whether they fall under the notion of personal data, defined in Article 4 of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR)[22] as "any information relating to an identified or identifiable natural person", and therefore within the scope of European personal data laws.

Although the Court of Justice of the European Union (CJEU) has not yet ruled on inferences generated by AI systems, it has recently considered information inferred from human assessments in two notable cases.[23] In the

[19] Mittelstadt, B. D.; Allo, P.; Taddeo, M.; Wachter, S.; Floridi, L., *The ethics of algorithms: Mapping the debate*, Big Data & Society, *vol.* 3, no. 2, 2016, pp. 4–5.

[20] Gabbrielli, *op. cit.* (fn. 6), p. 266.

[21] Sartor, *op. cit.* (fn. 7), p. 27.

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal, L 119, 4 May 2016.

[23] CJEU, *YS v Minister voor Immigratie, Integratie en Asiel, Minister voor Immigratie, Integratie en Asiel v M, S,* Joined Cases C-141/12 and C-372/12, ECLI:EU:C:2014:2081; CJEU, *Peter Nowak v Data Protection Commissioner,* Case C-434/16, ECLI:EU:C:2017:994.

first case, the Court examined the legal analysis contained in the reasoning given by an immigration officer to support a decision on a residence permit application, finding that this analysis does not qualify as information relating to an identified or identifiable person[24], unlike the personal data that it may contain.[25] According to the Court, the protection of the right to privacy implies that individuals should be able to ensure that their personal data is accurate and lawfully processed. To facilitate this, they have a right of access to their data, but this right does not extend to a legal analysis whose accuracy cannot be verified and, therefore, rectified.[26]

In a second case, however, the Court of Justice adopted a broader interpretation of personal data, concluding that it "potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject".[27] It includes, therefore, an examiner's comments on a candidate's written response during a professional exam, since these comments are intended to document the candidate's evaluation and may impact their rights and interests.[28]

This broader perspective is also supported by the – non-binding – Opinion 4/2017 of the Article 29 Working Party, which states that "the concept of personal data includes any sort of statements about a person. It covers 'objective' information, such as the presence of a certain substance in one's blood. It also includes 'subjective' information, opinions or assessments".[29] The Article 29 Working Party thus noted that the definition of personal data "lives up to its potential to become an all-encompassing notion"[30] and explicitly recognised so-called inferred data as personal data.[31]

The divergent views in these two decisions of the Court of Justice, along with the distinctive nature of inferences compared to information inferred by

[24] *YS v Minister* (fn. 23), paras. 39–40.

[25] *Ibid.*, para. 38.

[26] *Ibid.*, paras. 44–45.

[27] *Nowak* (fn. 23), para. 34.

[28] *Ibid.*, paras. 42–43.

[29] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN, WP136, p. 6.

[30] Purtova, N., *The law of everything: Broad concept of personal data and future of EU data protection law*, Law, Innovation and Technology, *vol.* 10, no. 1, 2018, p. 45.

[31] Article 29 Data Protection Working Party, *Guidelines on the right to "data portability"*, 16/EN, WP 242 rev.01, 2017, p. 10; Article 29 Data Protection Working Party, *op. cit.* (fn. 16), p. 8.

humans, suggest that the issue of their qualification remains unresolved. As such, doubts persist regarding the GDPR's applicability to inferences. In the following sections, both possibilities – classifying inferences as personal data or as non-personal data – will be explored to assess whether the relevant laws in each case provide sufficient protection for individuals.

3.1. Inferences as personal data: the GDPR and the Proposal for a Regulation on Privacy and Electronic Communications

If inferences were classified as personal data, the primary legislation applicable would be the GDPR, which was implemented in Italy through Legislative Decree No. 101/2018, adapting relevant national legislation (Legislative Decree No. 196/2003) to GDPR provisions. By guaranteeing individuals whose data are processed by third parties both appropriate information notice and the possibility to influence the processing, the GDPR stands as the most effective legislative instrument at European level for protecting privacy, personal identity, and reputation of individuals. Yet, even the safeguards provided by the GDPR appear insufficient.

A primary issue lies in the possibility of re-identification: machine learning methods can link various data, including anonymised or pseudonymised data, to identify subjects who otherwise would not be identifiable. Starting from anonymous data, which falls outside GDPR's scope, AI systems can infer personal data. Similarly, by applying machine learning techniques to non-sensitive data, inferences can be drawn in the form of special categories of personal data, which, as is well known, cannot be processed.[32]

Another core requirement for GDPR safeguards to be effective is awareness of the processing itself. Articles 13 and 14 GDPR mandate that controllers provide specific information to the data subject.[33] Since inferences are not directly collected from the data subject, Article 13, which applies when personal data is collected directly from the data subject, is inapplicable. Article 14, however, applies where data have not been obtained from the data subject, as in cases

[32] Article 9 GDPR.

[33] The Italian Supreme Court recently ruled on the required content for informing the data subject to ensure valid consent in relation to data processing by an automated reputation system (Corte di Cassazione, 24 March 2021, no. 14381). See Comandé, G., *Leggibilità algoritmica e consenso al trattamento dei dati personali, note a margine di recenti provvedimenti sui dati personali*, Danno e responsabilità, *vol.* 27, no. 1, 2022, pp. 141–150.

where inferences are generated by third parties and subsequently transferred. Under Article 14, controllers must inform the data subject of various elements, including the "categories of personal data" processed – a broad term likely referring to abstract data categories rather than specific descriptions. Additionally, controllers are exempt from providing information if "the provision of such information proves impossible or would involve a disproportionate effort"[34], a standard left undefined and open to broad interpretations. Moreover, if inferences are generated directly by the controller, there is no obligation to inform the data subject, as the data were not collected directly or from third parties. In this context, individuals may not even know about inferences concerning them, limiting their ability to exercise other rights, starting with the right of access under Article 15 GDPR. The right of access, in any case, is not absolute: it "shall not adversely affect the rights and freedoms of others"[35], including trade secrets, intellectual property, and the copyright protecting the software[36], as well as the personal data protection rights of third parties.[37]

Furthermore, some argue that, contrary to the Article 29 Working Party's opinion[38], the right of rectification under Article 16 GDPR relies on verifiability and therefore excludes predictive inferences, which by nature are unverifiable. The right to erasure under Article 17 GDPR is similarly challenging to apply to inferences[39] because it requires balancing against the data controller's interest on a case-by-case basis[40], according to criteria that remain undefined.[41]

Finally, Article 22 GDPR prohibits decisions based solely on automated processing, including profiling[42], if they have legal or otherwise significant effects on individuals.[43] While many current AI-driven activities fall within this prohibition (such as in recruitment, loans, and insurance systems), exceptions in

[34] Article 14(5)(b) GDPR.

[35] Article 15(4) GDPR.

[36] Recital 63 GDPR.

[37] Wachter; Mittelstadt, *op. cit.* (fn. 15), pp. 543–547.

[38] Article 29 Data Protection Working Party, *op. cit.* (fn. 16), pp. 17–18.

[39] Some scholars argue that Article 17 GDPR applies only to data provided by the data subject: Edwards, L.; Veale, M., *Slave to algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*, Duke Law & Technology Review, *vol.* 16, no. 1, 2017, pp. 68–69.

[40] Article 17(1)(b) and (c) GDPR.

[41] Wachter; Mittelstadt, *op. cit.* (fn. 15), pp. 548–556.

[42] Article 4(4) GDPR.

[43] Recital 71 GDPR.

Article 22(2), particularly those in (a) and (c), significantly limit the prohibition. These exceptions allow decisions based on automated processing when they are necessary for entering into or performing a contract with the data subject or based on the data subject's explicit consent.[44] Controllers must still implement suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests, including the right to obtain human intervention by the data controller, to express their opinion, and to contest the decision.[45] However, the CJEU's interpretation in previous cases described above suggests that challenging such decisions would require that input data be incorrect or incomplete, or that other data protection rights or principles be violated, making the right to contest the decision a mere procedural than substantive.[46]

The GDPR not only fails to provide adequate protection against inferences, but moreover risks facilitating their creation. Accepting that inferences are statistical[47] could trigger multiple exemptions[48], and Member States may provide exceptions to rights under Articles 15, 16, 18 and 21 GDPR per Article 89(2) GDPR.[49]

Although the GDPR seems the most appropriate place to regulate inferences, additional European laws may help protect individuals from misuse. Chief among these is the proposed "ePrivacy" Regulation, which would complement the GDPR by governing the respect for private life and the personal data protection in electronic communications.[50]

[44] Sartor, *op. cit.* (fn. 7), p. 59–61.

[45] Article 22(3) GDPR.

[46] Wachter; Mittelstadt, *op. cit.* (fn. 15), pp. 568–571.

[47] Mayer-Schönberger, V.; Padova, Y., *Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation*, The Columbia Science & Technology Law Review, *vol.* 17, no. 2, 2016, p. 330.

[48] Provided for in Articles 9(2)(j), 14(5)(b) and 17(3)(d) GDPR.

[49] It is true that, according to Recital 162 GDPR, "The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person". However, recitals are not legally binding according to the CJEU's established interpretation.

[50] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 10 January 2017 (ePrivacy), whose latest version was approved by the Council on 10 February 2021.

In fact, one of the e-Privacy recitals specifically acknowledges inferences, stating that metadata (i.e., data processed via electronic communications services for the purposes of transmitting, distributing, or exchanging electronic communications content)[51] "includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc."[52] Alongside metadata, the regulation also applies to the content of electronic communications, including text, voice, video, images, and sound[53], which together are referred to "electronic communications data".[54] In general, electronic communications networks and services providers may process electronic communications data for technical and security needs[55], but processing the electronic communications content requires data subject consent[56], while processing metadata is permissible in six cases, including data subject consent or for scientific, historical, or statistical purposes.[57] Since consent is often given without full knowledge of the subsequent processing and, as noted, some attribute a statistical nature to processing for the purpose of drawing inferences, the ePrivacy Regulation might not prevent providers of electronic communications networks and services from inferring data about individuals.[58] Article 7 ePrivacy mandates that providers erase or anonymise electronic communications content when no longer needed for processing, but this only applies to data provided or observed directly by the data subject, therefore excluding inferences.

[51] Article 4(3)(c) ePrivacy.

[52] Recital 2 ePrivacy.

[53] Article 4(3)(b) ePrivacy.

[54] Article 4(3)(a) ePrivacy.

[55] Article 6 ePrivacy.

[56] Article 6a ePrivacy.

[57] Article 6b ePrivacy.

[58] Notably, Recital 17b ePrivacy states the processing metadata for statistical purposes should result in aggregated data only and should not be used to support measures or decisions about any particular natural person, i.e., to determine the nature or characteristics of the end-user, to build an individual profile, or to draw conclusions concerning the end-user private life. However, recitals, as mentioned, do not carry binding legal force.

3.2. Inferences as non-personal data: the Digital Content and Services Directive

The analysis above suggests that European data protection laws fall short from protecting individuals from the misuse of inferences. It remains to consider the alternative scenario where inferences are not classified as personal data. In this regard, the recent adoption of the DCSD may impact the treatment of inferences.

On 11 December 2021, Legislative Decree No. 173/2021 took effect in Italy, implementing the DCSD and introducing amendments to the Italian Consumer Code.[59] Specifically, Chapter I-*bis*, entitled "With regard to contracts for the supply of digital content and digital services", was added. These amendments became effective on 1 January 2022, and apply to all contracts for the supply of digital content and digital services concluded on or after that date.

Of particular relevance here is the addition of Article 135-*noviesdecies* (4) and (5) to Italian law, which faithfully reproduces Article 16(3) and (4) DCSD. It states that, upon termination of the contract for the supply of digital content and services, the trader must refrain from using any content, other than personal data, provided or created by the consumer during the use of the digital content or service, while also allowing the consumer to retrieve such content. Thus, if the conditions set forth in Article 14 DCSD (transposed in Article 135-*octiesdecies* of the Italian Consumer Code) entitling the consumer to exercise the right to terminate the contract are met, the consumer gains a right to have the content they provided or created deleted. If this "created content" includes inferences, Article 16 DCSD could effectively provide the right to erase inferences after contract termination.

Importantly, unlike the right under Article 17 GDPR, this right to erasure does not require balancing with the data controller's interest on a case-by-case basis. This could provide the data subject with a straightforward means to eliminate inferences, regardless of any legitimate interest of the controller, thus avoiding the risks discussed previously.

To assess whether this right could include inferences, it is crucial to interpret the phrase "content other than personal data, which was provided or created by the consumer when using the digital content or digital service".[60] Consequently, inferences would fall within Article 16 DCSD only if they do not qualify as personal data – an eventuality, as noted earlier, that remains unresolved. Recital 69 of the DCSD adds that "such content could include digital images, video and

[59] Legislative Decree No. 206/2005.

[60] Articles 16(3) and (4) DCSD.

audio files and content created on mobile devices", an open-ended definition that might extend to inferences generated by AI. However, a strict interpretation suggests they should be excluded, as inferences are typically generated by the trader, not the consumer, even if through AI.

Furthermore, the DSCD's prohibition against using this content is subject to exceptions under Article 16(3) DCSD, one of which states that content "has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts". Aggregation forms the basis of automated processing, and "disproportionate efforts" remain undefined: it is clear that, even if inferences were part of the content to be deleted, the economic operator could invoke the exception in question in their favour, without having to provide any other justification.

Given these considerations, the applicability of Article 16 DCSD to inferences remains debatable even if they are classified as non-personal data. Additionally, even if Article 16 were to apply, its effectiveness would likely be significantly diminished by the existing exceptions.

4. AI ACT

The AI Act aims "to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values".[61] The proposed regulation adopts a risk-based approach to health, safety, and fundamental rights, categorising risks as low, high, and unacceptable. AI practices that fall within the third category of risk are either prohibited or heavily restricted. This category includes AI systems that use subliminal techniques outside a person's awareness, exploit specific vulnerabilities of certain groups to influence behaviour, rank the trustworthiness of individuals based on social behaviour or personal characteristics, and conduct "real-time" remote biometric identification in publicly accessible spaces for law enforcement purposes.[62]

High-risk AI systems, addressed in Title III of the proposal, are classified based on their functions, specific purposes, and methods. These include AI systems used as products or safety components of products requiring *ex ante* conformity assessment under existing European laws, as well as stand-alone

[61] Recital 1 AI Act.

[62] Article 5 AI Act.

AI systems listed in Annex III[63] – a list that the Commission may update according to Article 7 AI Act. Systems in the latter category include many of those previously mentioned, such as those used "for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests", as well as "to evaluate the creditworthiness of natural persons or establish their credit score", or "for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences".[64]

These systems can be placed and used within the EU market only if certain conditions are met. First, they must adhere to the requirements outlined in Articles 8–15 AI Act.[65] In addition to meeting those requirements[66], providers of high-risk AI systems must also implement a quality management system ensuring compliance with the AI Act[67], complete a conformity assessment, either through internal control or with the involvement of a notified body[68] who must meet the requirements of Article 33 AI Act.[69] The procedure based on internal control is carried out directly by the supplier for all high-risk AI systems listed in Annex III, except for those used for the "real-time" and "post" remote biometric identification of natural persons. Before being placed on the market, however, the AI systems listed in Annex III must be registered in the EU database established by Article 60 AI Act.[70] Additionally, providers must establish a post-market monitoring plan which analyses data provided by users or collected through other sources and enables the provider to evaluate the continuous compliance with the above-mentioned requirements.[71]

[63] Article 6 AI Act.

[64] No. 4, 5 and 6 Annex III AI Act.

[65] The explanatory memorandum clarifies that the requirements in Articles 8–15 AI Act are based on the ethics guidelines of the High-Level Expert Group on AI: High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, European Commission, Brussels, 2019.

[66] Article 16 AI Act.

[67] Article 17 AI Act.

[68] Article 43 AI Act.

[69] Under Article 30 AI Act, Member States must establish "a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring".

[70] Article 51 AI Act.

[71] Article 61 AI Act.

The AI Act not only represents the first broad attempt to regulate AI systems horizontally, but also contains many innovative and valuable elements, such as the risk-based categorisation, provision for both *ex ante* and *ex post* controls, and the creation of a public database. However, early commentators have identified some limitations, warning that the AI Act may, by allowing too much leeway to Member States, lead to problematic fragmentation within the European market.[72]

Regarding the data protection implications of the AI Act, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) issued a joint opinion on the proposed regulation, suggesting several textual improvements. They recommend clarifying "risk to fundamental rights" to align with the GDPR and Regulation (EU) 2018/1725.[73] Additionally, they propose that compliance with legal obligations under EU legislation, including data protection legislation, should be a prerequisite for European market authorisation, suggesting an explicit requirement for AI systems to align with GDPR and Regulation (EU) 2018/1725. They further recommend the certification scheme to be unrelated to European data protection legislation and therefore propose incorporating the principles of data minimisation and data protection into the certification process before obtaining the CE marking.[74]

One concern raised by academics but not addressed by the EDPB and EDPS is the lack of direct judicial and extrajudicial remedies (redress mechanisms[75]) available to individuals whose personal data is processed by AI systems in the event of erroneous or discriminatory automated decisions. This concern is particularly pressing given the minimal role of notified bodies in the conformity assessment procedure; almost all high-risk stand-alone AI systems rely on

[72] Finocchiaro, G.; Floridi, L.; Pollicino, O., *Sull'intelligenza artificiale Ue indecisa tra armonizzazione e margini di libertà*, Il Sole 24 ore, 3 March 2022, https://www.ilsole24ore.com/art/sull-intelligenza-artificiale-ue-indecisa-armonizzazione-e-margini-liberta-eccessivi-AEOLm5GB (12 December 2022).

[73] European Parliament and Council Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, Official Journal, L 295, 21 November 2018.

[74] EDPB/EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 June 2021.

[75] Pollicino, O.; De Gregorio, G.; Bavetta, F.; Paolucci, F., *Regolamento AI, la "terza via" europea lascia troppi nodi irrisolti: ecco quali*, Agenda digitale, 21 May 2021, https://www.agendadigitale.eu/cultura-digitale/regolamento-ai-la-terza-via-europea-lascia-troppi-nodi-irrisolti-ecco-quali/ (12 December 2022).

providers' self-assessment to determine compliance, which may not adequately protect individuals' health, safety, and fundamental rights.[76]

5. CONCLUSION

A study of the current European legal framework on data and AI reveals a significant gap in remedies that could adequately address issues posed by inferences. On one hand, neither the European legislator nor the courts have yet directly addressed inferences – even in the proposed AI Act – and on the other, the rights and tools currently available, or potentially forthcoming under the AI Act and ePrivacy Regulation, do not appear to sufficiently protect individuals against risks associated with automated processes, even with broad interpretation and application.

A legislative intervention could help to resolve many of these issues. The AI Act, as it remains under proposal, could be revised to include provisions directly addressing inferences and to introduce protections for affected individuals, following suggestions from scholars and legal experts.

Nevertheless, the GDPR remains the most appropriate instrument for incorporating a targeted framework by expressly including inferences within the definition of personal data and adapting data subject rights to address the unique challenges posed by inferences, or by introducing specialised provisions. Personal data, after all, enjoy the strongest level of protection under European law – a protection that is particularly crucial with regard to inferences, as these can form the basis for major decisions affecting individuals, such as denial of insurance coverage, employment, or loans.

It is worth noting that the GDPR, although came into force in 2016 and applicable throughout the EU since 2018, does not mention either AI or inferences. When the regulation was drafted, the primary concern was the growing sharing and collection of personal data[77], an issue that logically predates the risks posed by AI-driven data processing, which has only recently become a central topic.

Thus, the first step should be to amend the GDPR to include explicit references to AI, specifying, *inter alia*, the purposes for which processing of personal data to draw inferences should be deemed lawful and whether it qualifies as processing for statistical purposes. Additionally, data controllers should be

[76] Veale, M.; Zuiderveen Borgesius, F., *Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach*, Computer Law Review International, *vol.* 22, no. 4, 2021, p. 106.

[77] Recital 6 GDPR.

obligated to inform data subjects when inferences are drawn about them or when inferences are received from third parties. In both cases, the notification should include a clear description of the inferences' content, the data used to draw them, and, above all, the intended or possible uses of inferences. Individuals should be provided with opportunities to challenge such decisions and to influence outcomes accordingly. Finally, a specific right to delete inferences should be introduced, modelled closely after Article 16(3) and (4) DCSD, to strengthen the protection of individuals.

Despite the current challenges, the AI Act and other European and national initiatives inspire cautious optimism: the time has come to regulate AI, hopefully, in a forward-looking way, and it seems that the European legislator recognises this need.

BIBLIOGRAPHY

Angelini, R., *Intelligenza Artificiale e governance: Alcune riflessioni di sistema*, in: Pizzetti, F. (ed.), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, pp. 293–318

Carratta, A., *Decisione robotica e valori del processo,* Rivista di diritto processuale, *vol.* 75, no. 2, 2020, pp. 491–514

Casadei, T.; Pietropaoli, S., *Intelligenza artificiale: fine o confine del diritto?*, in: Casadei, T.; Pietropaoli, S. (eds.), *Diritto e tecnologie informatiche: Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters Kluwer CEDAM, Padova, 2021, pp. 219–232

Comandé, G., *Leggibilità algoritmica e consenso al trattamento dei dati personali, note a margine di recenti provvedimenti sui dati personali*, Danno e responsabilità, *vol.* 27, no. 1, 2022, pp. 141–150

D'Acquisto, G., *Intelligenza artificiale*, Giappichelli, Torino, 2018

Edwards, L.; Veale, M., *Slave to algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*, Duke Law & Technology Review, *vol.* 16, no. 1, 2017, pp. 8–84, DOI: 10.2139/ssrn.2972855

Finocchiaro, G., *Riflessioni su intelligenza artificiale e protezione dei dati personali*, in: Ruffolo, U. (ed.), *Intelligenza artificiale: Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, pp. 237–250

Finocchiaro, G.; Floridi, L.; Pollicino, O., *Sull'intelligenza artificiale Ue indecisa tra armonizzazione e margini di libertà*, Il Sole 24 ore, 3 March 2022, https://www.ilsole24ore.com/art/sull-intelligenza-artificiale-ue-indecisa-armonizzazione-e-margini-liberta-eccessivi-AEOLm5GB (12 December 2022)

Gabbrielli, M., *Dalla logica al deep learning: una breve riflessione sull'intelligenza artificiale*, in: Ruffolo, U. (ed.), *XXVI lezioni di diritto dell'intelligenza artificiale*, Giappichelli, Torino, 2021, pp. 21–30

High-Level Expert Group on Artificial Intelligence, *A Definition of AI: Main Capabilities and Disciplines*, European Commission, Brussels, 2018

High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, European Commission, Brussels, 2019

Kleinberg, J.; Ludwig, J.; Mullainathan, S.; Sunstein, C. R., *Discrimination in the Age of Algorithms*, Journal of Legal Analysis, *vol.* 10, 2018, pp. 113–174, DOI: 10.1093/jla/laz001

Mayer-Schönberger, V.; Padova, Y., *Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation*, The Columbia Science & Technology Law Review, *vol.* 17, no. 2, 2016, pp. 315–335, DOI: 10.7916/stlr.v17i2.4007

Mittelstadt, B. D.; Allo, P.; Taddeo, M.; Wachter, S.; Floridi, L., *The ethics of algorithms: Mapping the debate*, Big Data & Society, *vol.* 3, no. 2, 2016, pp. 1–21, DOI: 10.1177/2053951716679679

Pizzetti, F. (ed.), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018

Pollicino, O.; De Gregorio, G.; Bavetta, F.; Paolucci, F., *Regolamento AI, la "terza via" europea lascia troppi nodi irrisolti: ecco quali*, Agenda digitale, 21 May 2021, https://www.agendadigitale.eu/cultura-digitale/regolamento-ai-la-terza-via-europea-lascia-troppi-nodi-irrisolti-ecco-quali/ (12 December 2022)

Purtova, N., *The law of everything: Broad concept of personal data and future of EU data protection law*, Law, Innovation and Technology, *vol.* 10, no. 1, 2018, pp. 40–81, DOI: 10.1080/17579961.2018.1452176

Sartor, G., *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, European Parliamentary Research Service, Brussels, 2020

Samoili, S.; Lopez Cobo, M.; Gómez, E.; De Prato, G.; Martínez-Plumed, F.; Delipetrev, B., *AI Watch: Defining Artificial Intelligence 2.0: Towards an operational definition and taxonomy of artificial intelligence*, Publications Office of the European Union, Luxembourg, 2021, DOI: 10.2760/382730

Sicular, S., *Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three "V"s*, Forbes, 27 March 2013, https://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/ (12 December 2022)

Signorato, S., *Giustizia penale e intelligenza artificiale: Considerazioni in tema di algoritmo predittivo*, Rivista di diritto processuale, *vol.* 75, no. 2, 2020, pp. 605–616

Sunstein, C. R., *Algorithms, Correcting Biases*, Social Research: An International Quarterly, *vol*. 86, no. 2, 2019, pp. 499–511, DOI: 10.1353/sor.2019.0024

Veale, M.; Zuiderveen Borgesius, F., *Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach*, Computer Law Review International, *vol*. 22, no. 4, 2021, pp. 97–112, DOI: 10.9785/cri-2021-220402

Wachter, S.; Mittelstadt, B., *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, Columbia Business Law Review, no. 2, 2019, pp. 494–620, DOI: 10.7916/cblr.v2019i2.3424

Zaccaria, G., *Figure del giudicare: calcolabilità, precedenti, decisione robotica*, Rivista di diritto civile, *vol*. 66, no. 2, 2020, pp. 277–294

Sažetak

Gina Gioia[*]
Sofia Maria Lener[**]

ZAŠTITA POJEDINACA OD INFERENCIJA KOJE UGROŽAVAJU PRIVATNOST I DISKRIMINATORNIH INFERENCIJA U EUROPSKOM PRAVU: OD OPĆE UREDBE O ZAŠTITI PODATAKA I DIREKTIVE O DIGITALNOM SADRŽAJU I USLUGAMA DO AKTA O UMJETNOJ INTELIGENCIJI

Inferencije su informacije koje se odnose na identificiranu ili prepoznatljivu fizičku osobu generirane uporabom tehnika strojnog učenja koje omogućuju vjerojatnosne korelacije između otkrivenih ulaznih podataka i predviđanja za buduće slučajeve. Inferencije nose mnogobrojne rizike: inherentno su neizvjesne, predviđanja su pouzdana samo koliko su pouzdani i podatci na kojima se inferencije temelje, a one se mogu rabiti za poticanje i manipulaciju pojedincima. Ključno je spriječiti te rizike, a gdje se pojave, pružiti odgovarajuću zaštitu. Ovaj rad ispituje je li postojeće europsko zakonodavstvo adekvatno razriješilo te probleme. Prvi je zadatak klasificirati inferencije kako bi se utvrdilo ulaze li u pojam osobnih podataka i jesu li stoga obuhvaćene europskim pravom zaštite osobnih podataka. Ova analiza razmatra obje mogućnosti – tretiranje inferencija i kao osobnih i kao neosobnih podataka – te ocjenjuje relevantni regulatorni okvir, uključujući Opću uredbu o zaštiti osobnih podataka, Prijedlog uredbe o privatnosti i elektroničkim komunikacijama, Direktivu o digitalnom sadržaju i uslugama te Akt o umjetnoj inteligenciji.

Ključne riječi: talijansko potrošačko pravo, raskid ugovora, inferencije koje ugrožavaju privatnost, diskriminatorne inferencije, zaštita pojedinaca

[*] Dr. sc. Gina Gioia, izvanredna profesorica, University of Tuscia, Department of Legal, Social, and Educational Sciences, Via Santa Maria in Gradi 4, 01100 Viterbo, Italija; gina.gioia@unitus.it;
ORCID ID: orcid.org/0000-0002-4542-9711

[**] Sofia Maria Lener, mag. iur., doktorandica, University of Tuscia, Department of Legal, Social, and Educational Sciences, Via Santa Maria in Gradi 4, 01100 Viterbo, Italija; sofiamaria.lener@leplex.it;
ORCID ID: orcid.org/0000-0003-1980-9152