Impact Assessments and the Protection of Fundamental Rights in the Processing of Personal Data*

Paola Pasqualone**

Abstract

The Data Protection Impact Assessment (DPIA) represents a pivotal instrument for safeguarding fundamental rights in the context of personal data processing, particularly in environments shaped by rapid technological innovation. Anchored in the principle of accountability enshrined in the General Data Protection Regulation (GDPR), the DPIA serves not merely as a compliance mechanism, but as a substantive tool for risk assessment and mitigation. This article examines the evolving function of the DPIA in contemporary data governance, with a specific focus on recent decisions issued by the Italian Data Protection Authority concerning the deployment of widely used chatbot technologies. These cases illuminate both the preventive and remedial dimensions of the DPIA, while simultaneously exposing a persistent lack of uniformity in its practical implementation and interpretive contours. The analysis underscores the existing tensions between formal compliance and effective protection of data subjects' rights, and advocates for a more coherent and harmonised interpretative framework to enhance the DPIA's role as a cornerstone of data protection by design.

I. The Circulation of Personal Data and its Impact on Fundamental Rights: the Vulnerability of Data Subjects

Technological progress in recent decades, particularly the development and proliferation of algorithms, has clearly highlighted the pitfalls associated with the processing of personal data, especially with regard to individuals who are in a position of greater vulnerability, as well as issues related to the respect of 'digital' rights, which are crucial for the development and protection of individuals in the virtual space.[1] In particular, Art 5 of the GDPR sets out key principles such as

* This essay, with the addition of the footnotes, constitutes further elaboration of the paper presented at the 3rd conference in the context of the project 'Digital Vulnerability in European Private Law' (DiVE), on the topic 'Remedies to Digital Vulnerability in European Law', which took place at the University of Trieste on 10 and 11 april 2025.

** PhD Student of Private Law, University of Molise.

[1] The reference is to Art 8 of the Charter of Fundamental Rights of the EU: 'Everyone has the right to the protection of personal data concerning them. Such data must be processed fairly and lawfully and for specified purposes and for the purpose for which they were originally collected. Every person has the right of access to data which has been collected concerning him or her, and the right to have such data rectified. Compliance with these rules shall be subject to control by an independent authority'.

lawfulness, transparency, minimisation, accountability and privacy by design, which are essential in the context of large-scale processing of personal data. Indeed, as authoritative scholars have reiterated, digital vulnerability is not limited to traditional categories of vulnerable individuals, but potentially affects all online users, given the digital asymmetry and ontological fragility of individuals *vis-à-vis* technological power.[2] As will be discussed in more detail below, human vulnerability is also present in discussions on data protection, privacy and data-driven technologies. The protection of *privacy* and personal data is also seen as a way of addressing the vulnerability of individuals in the face of the power imbalances created by the most innovative technologies.[3]

In the doctrinal debate, a distinction is made between risks of vulnerability related to data processing and risks of vulnerability related to the results of such processing. In the first perspective, vulnerability may emerge, for example, as a limited ability to give free consent to the collection of personal data, to understand information about data processing or to adequately exercise data protection rights. The second perspective emphasises vulnerability in the context of data protection, which emerges in the form of harm to which individuals are exposed.[4] In this context, data subjects who are 'vulnerable' to data processing are more frequently subject to profiling, resulting from the large-scale processing of personal data, which determines the classification of individuals into specific categories based on interests, preferences, habits or other distinctive elements that characterise their behaviour.[5] Moreover,

> 'this categorisation of the subject often results in an algorithmic decision being taken – for example, personalised advertising – the content of which depends precisely on the category to which the subject belongs (so-called clustering)'.[6]

In fact, the acquisition and processing of Big Data are classified as fundamental

[2] On this point P. Perlingieri, 'Sul trattamento algoritmico dei dati' *Tecnologie e diritto*, 181 (2020); see Id, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, II, *Fonti e interpretazione*, (Napoli: Edizioni Scientifiche Italiane, 4th ed, 2020), 46-47. On this point see also S. Giova and I. Prisco eds, *Il trattamento algoritmico dei dati tra etica, diritto ed economia, Atti del 14° Convegno Nazionale SISDiC* (Napoli: Edizioni Scientifiche Italiane, 2020).

[3] For an overview, see G. Carapezza Figlia, 'Vulnerabilità digitale e post-modernità giuridica' *Diritto del mercato assicurativo e finanziario*, 2 (2025); A. Bernes, 'Persona vulnerabile, ambiente digitale e obblighi di protezione' *Il diritto di famiglia e delle persone*, 163-185 (2025).

[4] G. Malgieri and N. Jedrzej, 'Vulnerable data subjects' 37 *Computer Law and Security Review*, 2-16 (2020).

[5] For an in-depth analysis of 'digital' manipulation, see A. Gorgoni, 'Vulnerability in the digital environment and the protection of freedom of will' *Persona e Mercato*, 917-918 (2024); see similary, O. Pollicino, 'Vulnerability in the Digital Age', in C. Crea and A. De Franceschi eds, *The new Shapes of Digital Vulnerability in European Private law* (Baden-Baden: Nomos, 2024) 25.

[6] As noted by G. Proietti, 'Algorithms and the interests of data controllers in the circulation of personal data' *Contratto e impresa*, 880-884 (2022); on this subject, see also E. Pariser, *The filter bubble: What the internet is hiding from you*, (London: Viking, 2012).

assets for certain purposes: thanks to predictive operations carried out using specific algorithms, they end up reducing human actions to calculable data.[7]

On this point, Regulation (EU) 2016/679 does not contain an explicit definition of vulnerable individuals, but Recital 75 expressly refers to the relevant risks to be considered when carrying out a data protection impact assessment pursuant to Art 35 (known as DPIA) 'where personal data of vulnerable natural persons, in particular children, are processed'. This definition implies that children are considered vulnerable subjects, but does not exclude other individuals from being considered as such. The introduction of the Data Protection Impact Assessment (DPIA) pursuant to Art 35 of the GDPR is therefore an essential mechanism for processing operations related to Big Data, obliging data controllers to assess and mitigate the risks to the rights and freedoms of data subjects.[8] In this regard, the Article 29 Working Party (WP29), set up to provide expert advice to Member States on data protection,[9] has noted in several opinions that vulnerability cannot be limited to minors. In particular, the WP29 argues that the key factor in identifying individual vulnerability is an imbalance of power between the data subject and the data controller. This imbalance of power means that individuals may 'not be able to easily consent or object to the processing of their data or exercise their rights'. When data controllers carry out the required balancing test if they wish to process personal data on the basis of legitimate interests (Art 6, para 1, lett f) of the GDPR), they must consider the nature and source of the legitimate interest, whether additional safeguards exist and the impact on the data subject, taking into account in particular

> 'the status of the data controller and the data subject, including any imbalance between the data subject and the data controller, or whether the data subject is a child or otherwise belongs to a vulnerable group'.

[7] On this point, the Digital Services Act (European Parliament and Council Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC [2022] OJ L 277) imposes obligations on online platforms, in particular VLOP/VLOSE, regarding algorithmic transparency, independent audits, human oversight and internal redress mechanisms, in order to safeguard users' rights to information, dignity and privacy.

[8] On the role and importance of personal data impact assessments, see, among others, D. Baldini, 'La valutazione d'impatto sulla protezione dei dati personali: quale ruolo per i diritti fondamentali degli interessati?', in A. Adinolfi et al eds, *Protezione dei dati personali e nuove tecnologie* (Napoli: Edizioni Scientifiche Italiane, 2022) 53-74; H. Janssen et al, 'Practical fundamental rights impact assessments International' 30(2) *Journal of Law and Information Technology*, 200-232 (2022); G. Georgiadis and G. Poels, 'Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review' 44 *Computer Law and Security Review*, 1-21 (2022); D. Hallinan and N. Martin, 'Fundamental Rights, the Normative Keystone of DPIA' 6(2) *European Data Protection Law Review*, 178-193 (2020); R. Bennis, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' 7(1) *International Data Privacy Law*, 22-35 (2017).

[9] The Article 29 Working Party, which had essentially advisory tasks under Directive 95/46 EC, has been replaced by the European Data Protection Board.

In particular, where data controllers are in a position of significant imbalance of power (in terms of possible impacts on fundamental rights and freedoms, significant information asymmetry based on predictive analysis, etc) *vis-à-vis* the data subject, the latter should be considered vulnerable. While the protection of fundamental rights was originally aimed at protecting individuals from interference by public authorities, the analysis of the impact of economic activities on these rights has increasingly become an essential dimension of corporate responsibility. Within the European Union, the General Data Protection Regulation now requires both economic operators and public bodies to assess the likelihood that the processing of personal data will result in a high risk to fundamental rights and freedoms, requiring a DPIA to be carried out in such cases.

II. Data Protection Impact Assessment as an Expression of the Principle of Accountability

In order to provide a coherent framework concerning those processing activities that necessarily require a data protection impact assessment, the Article 29 Working Party expressly referred, in the Guidelines adopted on 4 April 2017, to 'data relating to vulnerable data subjects'. The processing of such data constitutes a criterion that increases the imbalance of power between the data subjects and the data controller, potentially resulting in the individuals' inability to give consent freely, to object to the processing of their personal data, or to effectively exercise their rights.[10]

Within this context, the data protection impact assessment represents one of the most significant innovations introduced by Regulation (EU) 2016/679, as well as one of the principal expressions of the risk-based approach and the accountability principle, around which the interpretation of the entire regulatory framework revolves. In this regard, particular reference is made to Art 35 of the GDPR, which governs the circumstances under which the data controller[11] is required to carry

[10] See, in particular 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679', adopted on 4 April 2017, and 'Guidelines on 'Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' released in October 2017 and revised in February 2018 by the Article 29 Working Party (now the EDPB), available at www. ec.europa.eu. However, if none of these rights can be invoked, the GDPR imposes significant obligations on data controllers who use ADM, regardless of whether the decision-making process involves a human being or not. For further discussion, see L. Edwards and M. Veale, 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For' 16(1) *Duke Law and Technology Review*, 18-84 (2017); M.E. Kaminski and G. Malgieri, 'Algorithmic impact assessments under the GDPR: producing multi-layered explanations' 11(2) *International Data Privacy Law*, 125-144 (2021).

[11] Art 4, para 7, of the GDPR defines the data controller as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'.

out a DPIA,[12] although it does not provide a precise definition of the term. To address this gap, the 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation (EU) 2016/679', adopted by the Article 29 Working Party, define the DPIA as

> 'a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data, by assessing those risks and determining the measures to address them'.

The GDPR does not establish a specific threshold of risk, but it does identify certain types of processing that invariably require a data protection impact assessment, such as systematic and extensive profiling operations that produce significant effects on individuals' rights and freedoms, the large-scale processing of sensitive information, and large-scale public monitoring.[13] Moreover, a DPIA is required in cases involving the deployment of new technologies, the processing of biometric or genetic data, and operations that entail the interconnection, combination, or comparison of personal data, including the cross-referencing of digital goods consumption data with payment information. In line with the risk-based approach adopted by the General Data Protection Regulation, the obligation to carry out a DPIA does not apply to all processing activities, but only to those which are 'likely to result in a high risk to the rights and freedoms of natural persons' (pursuant to Art 35 GDPR).

Accordingly, DPIAs constitute one of the key instruments of *ex ante* governance introduced by the GDPR. They pursue the normative – albeit ambitious – objective of establishing operational tools capable of enhancing the accountability of controllers and processors, thereby giving practical effect to the legal principles and standards enshrined in the European data protection framework. During the preparatory stages of the GDPR, the European Commission conceived DPIAs as mechanisms aimed at strengthening the protection of the fundamental rights and

[12] Art 35 of the GDPR provides that, where a type of processing 'in particular through the use of new technologies', is 'likely to result in a high risk' to the rights and freedoms of natural persons, the data controller shall, 'prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data'. According to the GDPR, this assessment must include: a description of the 'processing operations' (in this case, the algorithm) and the purpose of the processing; an assessment of the necessity of the processing in relation to the purpose; an assessment of the risks to the rights and freedoms of individuals; and, importantly, the measures that a company will use to address those risks and demonstrate compliance with the GDPR, including security measures (see Art 35, para 7, and Recitals 84 and 90).

[13] As established by Art 35(3) 'A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale'.

freedoms of natural persons, by enhancing the capacity of stakeholders engaged in high-risk processing to identify potential issues in advance, anticipate their consequences, and implement appropriate remedial measures.[14] The GDPR's approach to the prevention of harm and discrimination arising from algorithmic decision-making is grounded in the principle of accountability and in the obligation of transparency on the part of data controllers and processors. Within this framework, Recital 71 plays a crucial role, requiring that profiling and automated decision-making systems be designed and implemented in such a way as to prevent the production of discriminatory effects based on sensitive data – such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or health status, or sexual orientation.[15] Precisely because of the high risk to the rights and freedoms of individuals, the European legislator has subjected this type of automated decision-making to a general prohibition that can only be overcome in specific circumstances (paras 2 and 4 of Art 22) and provided that the controller has implemented the safeguards referred to in para 3.[16] This provision is part of the broader framework of the key principles of the GDPR and, first and foremost, the principle of accountability referred to in Art 5(2) and Art 24, which requires controllers and processors to implement appropriate technical and organisational measures and to be able to demonstrate their compliance and effectiveness.[17]

It is therefore essential, in the field of personal data protection, to correctly apply the principle of accountability,[18] which is not limited to redefining the burden of assessing the lawfulness of processing in advance, but represents a new organisational criterion for those involved in the management of personal data. In fact, this principle fits perfectly with the approach of damage prevention, which is more

[14] As emphasised in N.N. Loideain and R. Adams, 'From Alexa to Siri and the GDPR: The gendering of Virtual Personal Assistants and the role of Data Protection Impact Assessments' 36 *Computer Law and Security Review*, 10 (2020).

[15] On this topic cf M.E. Kaminski and G. Malgieri, n 10 above, 129.

[16] '(...) the controller shall take appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, at least the right to obtain human intervention on the part of the controller, to express his or her opinion and to contest the decision'.

[17] In this regard, the guidelines of the EDPB (formerly the Article 29 Working Party), such as the 'Guidelines on Automated individual decision-making and Profiling', specify the responsibility of controllers to ensure transparency and oversight of algorithmic systems, to regularly monitor the accuracy and relevance of data and results, and to introduce systems for auditing and periodically reviewing the algorithmic models and data sets used.

[18] This principle is not limited to 'mere responsibility', but also includes an obligation to 'account' or demonstrate that the processing is carried out in accordance with the Regulation (Art 24 of GDPR). More precisely, accountability consists of two elements: 'adoption' of appropriate and effective measures to fulfil the obligations arising from the Regulation and 'demonstration' of compliance of the processing with the rules of the GDPR, for a detailed examination, see G. Amore, 'Fairness, Transparency and Accountability in the protection of personal data' *Studium Iuris*, 414-419 (2020); see also A. Mantelero, 'Responsabilità e rischio nel Regolamento UE n. 2016/679' *Nuove leggi civili commentate*, 147-148 (2017).

suitable for safeguarding personal rights.[19] The case law of the Court of Justice of the European Union also helps to clarify the scope and limits of automated decision-making processes and profiling systems. In the *Schrems I*[20] judgment and even more so in the *Schrems II*[21] case, the Court affirmed the need to ensure effective remedies and adequate safeguards in the context of personal data surveillance and processing systems, especially when the data involved belong to sensitive categories or are likely to have significant effects on the rights and freedoms of the data subjects. Similarly, the Meta Platforms judgment and the interpretation of Art 22 of the GDPR have further clarified the need for strict adherence to the principles of transparency, lawfulness and proportionality in the adoption of automated decision-making systems, recalling the obligation of data controllers to implement

[19] Authoritatively discussed in P. Perlingieri, 'Privacy digitale e protezione dei dati personali tra persona e mercato' *Foro napoletano*, 484 (2018), who underlines that the EU Regulation not only safeguards confidentiality but also regulates the dignity of the human person in a broader sense; see by the same author P. Perlingieri, 'Principio personalista, dignità umana e rapporti civili' *Annali S.I.S.Di.C.*, 1-5 (2020). On this topic, see L. Lonardo, 'Il valore della dignità della persona nell'ordinamento italiano' *Rassegna di diritto civile*, 773 (2011); V. Scalisi, *L'ermeneutica della dignità* (Milano: Giuffrè, 2018); M.G. Stanzione, 'La protezione dei dati personali tra «consumerizzazione» della privacy e principio di accountability' *Comparazione e diritto civile*, 13-14 (2019); B. Borrillo, 'La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR' *dirittifondamentali.it*, 326-356 (2020); E. Belmonte, 'L'autoregolamentazione per la protezione dei dati personali: tra conformità e responsabilità' *Annali S.I.S.Di.C.*, 11 (2022).

[20] Case C-362/14 *M. Schrems* v *Data Protection Commissioner*, Judgment of 6 Octobre 2015, available at www.eur-lex.europa.eu; see also P. Perlingieri, 'Sul trattamento algoritmico dei dati' n 2 above, 183-184. In this regard, the Author emphasises the centrality in the GDPR of the principles of transparency, fairness and accountability, including in relation to the circulation of data outside the EU and cases of big data that are harmful to individuals.

[21] Case C-311/18 *Data Protection Commissioner* v *Facebook Ireland Limited and M. Schrems*, Judgment of 16 July 2020, available at www.eur-lex.europa.eu. In this case, the Court invalidated the European Commission's decision that the Privacy Shield was adequate for the transfer of personal data from EU Member States to the United States. This had a significant impact on extra-EU data transfers, highlighting the need for more robust data protection mechanisms and a case-by-case assessment of their adequacy. As determined by the Court 'The first sentence of Article 45(1) of the GDPR provides that a transfer of personal data to a third country may be authorised by a decision of the Commission finding that the third country, a territory or one or more specified sectors within that third country, ensures an adequate level of protection. In this regard, without requiring the third country in question to guarantee a level of protection identical to that guaranteed by the legal order of the Union, the expression "adequate level of protection" must be understood, as confirmed by Recital 104 of that regulation, as requiring that the country in question ensures, by virtue of its domestic law or international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the Union under that regulation, read in the light of the Charter. In the absence of such a requirement, the objective referred to in the previous paragraph would be undermined'. See K. Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' 20 *German Law Journal*, 779-793 (2019). In reference to this case, the author supports the argument that where a measure imposes a limitation on the exercise of a fundamental right that is so intense and so comprehensive that it calls into question that right as such, that measure is incompatible with the Charter, as it deprives the right at issue of its essence. This is so without the need for a balancing exercise of competing interests, because a measure that compromises the very essence of a fundamental right is automatically disproportionate.

tools for reviewing and guaranteeing the rights of data subjects.[22]

Automated decision-making and profiling can pose a serious risk to fundamental rights, mainly due to a lack of transparency and the likelihood of discrimination.[23] As a result, the GDPR establishes a framework of protection aimed at minimising the negative impact that such systems may have on the entire catalogue of fundamental rights concerned. The GDPR's safeguards include: transparency and fairness requirements, specific accountability obligations, specified legal grounds for processing, rights for individuals to object to profiling and, where certain conditions are met, the need to carry out a data protection impact assessment.[24] To ensure lawfulness, fairness and transparency, the controller is required to provide data subjects with concise, transparent, intelligible and easily accessible information about the processing of their personal data (Art 12(1) of the GDPR). Furthermore, the use of big data tools increases the risk of questionable or unlawful discrimination (both direct and indirect).[25] Consequently, when assessing the impact of fundamental rights on the regulation of automated decision-making and profiling, it appears that automatic and objective safeguards play a key role, namely the restriction of processing and purpose (Art 5(1) of the GDPR), data minimisation (Art 5, para 1, lett *c)* of the GDPR), storage limitation (Art 5, para 1, lett *e)* of the GDPR).[26] They complement the set of individual protection tools (right to rectification, erasure, restriction of processing and objection) which require the data subject to actively exercise their rights. Of central importance is the regulation of automated data processing (Art 22 of the GDPR), which gives rise to personal profiling. This provision is characterised by a general prohibition of fully automated decision-making and by a core framework of protection centred on data quality and on their non-incompatibility with the permitted purposes.[27] In effect, it regulates automated decision-making in four stages: it establishes the 'right not to be subject to a decision based solely on automated processing'[28] where such decision produces legal effects or similarly significant effects; it sets out three exceptions in para 2[29] and specifies the conditions under which those

[22] Case C-252/21 *Meta Platforms Inc. and others* v *Bundeskartellamt*, Judgment of 4 July 2023, available at www. eur-lex.europa.eu.

[23] Mainly the rights to privacy and data protection, the right to an effective remedy and the right to a fair trial and to a fair trial, and prohibition of discrimination.

[24] For a more in-depth understanding of the principle of fairness, see D. Clifford and J. Ausloos, 'Data Protection and the Role of Fairness' 37 *Yearbook of European Law*, 130-187 (2018).

[25] J. Kleinberg et al, 'Discrimination in the age of algorithms' 10 *Journal of Legal Analysis*, 113 (2018).

[26] Expression of the principle of fairness referred to in Art 8 of the EU Charter of Fundamental Rights.

[27] P. Perlingieri, *Sul trattamento algoritmico dei dati* n 2 above, 184.

[28] Art 22, para 1, of the GDPR.

[29] Pursuant to Art 22, para 2, para 1 shall not apply if the decision: a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; c) is based

exceptions apply in paras 2 and 3;[30] and, finally, it contains a restriction concerning special categories of data. In this regard, it has been argued that the provision in question represents, in reality, a normative clause that takes into account not only legal concerns, but also social considerations in the design of technology. User profiling, resulting from the large-scale collection of personal data, facilitates the placement of the individual within a given category on the basis of what are presented as his or her interests, preferences, behaviours, or other specific elements. This process of categorisation is often followed by the adoption of an algorithmic decision – for example, the delivery of personalised advertising – the content of which is determined precisely by the category of affiliation (so-called cluster).[31] In this way, the acquisition of vast amounts of data through the use of social platforms and the sharing of content, as well as their subsequent processing, are regarded as fundamental assets for certain purposes; through predictive operations performed by specific algorithms, they ultimately reduce human actions to calculable data.

The doctrinal debate has primarily centred on the question of whether Art 22 GDPR establishes a genuine ex post right to an explanation of an individual decision taken by means of an automated system. Indeed, automated decisions capable of producing legal effects or otherwise significantly affecting the data subject should be rendered 'intelligible', in the sense that the individual concerned must be able to understand, to a sufficient extent, the underlying decision-making process, so as to be placed in a position to effectively exercise the other rights conferred upon him or her by the GDPR, including the right to challenge the decision itself.[32] The existing discussions on the right to an explanation under Art 22, however, largely obscure the more complex approach to algorithmic transparency adopted by the Regulation. In other words, the GDPR is better understood as 'a multi-layered system of explanations'.[33] This provision tends to be interpreted as

on the data subject's explicit consent.

[30] In the cases referred to in points a) and c) of para 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

[31] Advertising activity is not, in itself, capable of generating a legally relevant constraint, which is why doubts remain as to whether it can be classified as a decision in the strict sense. Nevertheless, it has been observed that a massive activity of this nature may be capable of having a significant impact on the data subject, within the meaning of Article 22 of the GDPR, in that it is likely to restrict users' freedom of choice, confining them to a sort of 'information bubble' in which they are exposed exclusively to content that conforms to their own beliefs, see E. Pariser, n 6 above.

[32] M.E. Kaminski and G. Malgieri, *Algorithmic impact* n 10 above, 127-128. From a systematic point of view, arguments can be derived from the context of Art 22 GDPR from the systematic position of Art 22 GDPR within the GDPR and from its context within the EU body of law. Most of these arguments support the interpretation as a data subject right, some the interpretation as a general prohibition, see F. Thouvenin et al, 'Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right?' 2 *European Data Protection Law Review*, 189-193 (2022).

[33] For an overview on the regulatory approach adopted in Art 22 of the GDPR, which reveals the nature of a legal obligation, cf C. Djeffal, 'The Normative Potential of the European Rule on

including an implicit right to an explanation, aimed at ensuring that the data subject can understand the logic underlying the automated decision and, consequently, exercise their right to object in an appropriate procedure.[34]

III. The Cases of Chatbots ChatGPT and Replika

In such a complex and dynamic context as that of personal data protection, the latest forms of algorithmic processing of information have a significant impact on the fundamental rights and freedoms of individuals in the digital society, enabling the adoption of automated decisions that are potentially capable of affecting a wide range of relevant legal situations. This issue is receiving increasing attention from national supervisory authorities, which, in their decisions, are increasingly referring to the risks that more complex processing activities – in particular those based on automated decision-making processes – may pose to the fundamental rights and freedoms recognised by European Union law.[35] In this context, the corrective and punitive measure adopted by the Data Protection Authority in November 2024 against OpenAI in relation to the ChatGPT service is noteworthy. The intervention followed an investigation launched in 2023 and concerned, among other things, the unlawful collection of personal data, the absence of a system for verifying the age of underage users and the lack of adequate information for data subjects. The Authority also highlighted the absence of a valid legal basis for the large-scale collection and storage of personal data for the purpose of training algorithms. Finally, the finding that there were no adequate mechanisms to prevent access to the service by children under the age of 13, thus exposing them to content that was potentially inappropriate for their level of development, was particularly critical.[36] In addition to imposing a fine of 15 million euros, the Authority ordered

Automated Decisions: A New Reading for Art. 22 GDPR' 80 *ZaöRV*, 856-857 (2020).

[34] For an in-depth analysis of the impact of fundamental rights on automated decision-making and profiling, see Iamiceli et al, *Casebook. Effective data protection and fundamental rights* (Roma: Scuola Superiore della Magistratura, 2022) 198.

[35] On this point, see A. Montelero and M.S. Esposito, 'An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems' 41 *Computer Law and Security Review*, 1-35 (2021). The authors focus on the analysis of numerous measures taken by supervisory authorities in various Member States (including Italy) in order to demonstrate that fundamental rights, not only the right to privacy, are taken into account in their decisions. For a similar view, see B. Borrillo, n 19 above, 354-355, which, in analysing the sanctioning model of the supervisory authorities, points out that they show a marked sensitivity towards the driving force behind the post-GDPR legislation, namely the accountability of those who process personal data with a view to carefully assessing the risks of violating the fundamental rights and freedoms of the data subjects; see 'Guidelines' n 10 above.

[36] See the press release published on 20 December 2024 on the website of the Italian Data Protection Authority; in addition, the measure issued by the Authority is based on the opinion of the EDPB, adopted on 18 December 2024, Opinion 28/2024 on certain aspects concerning data protection in the context of the processing of personal data in the context of AI models, available at www.edpb.europa.eu. With regard to DPIA, the opinion reiterates that 'data protection impact

OpenAI, using for the first time the new powers provided for in Art 166, para 7, of the Italian Privacy Code[37] to carry out a six-month institutional communication campaign on radio, television, newspapers and the Internet. The content, to be agreed with the Authority, must promote public understanding and awareness of how ChatGPT works, in particular the collection of user and non-user data for the training of generative artificial intelligence and the rights that can be exercised by data subjects, including the rights to object, rectify and erase.[38] In addition, after establishing the immediate implementation of an age verification system for registration to the service, the Authority ordered the company involved to submit an action plan providing for the implementation of an age verification system capable of excluding access to users under the age of 13 and minors without parental consent.

Similarly, the recent case of Replika is relevant to the processing of personal data by automated systems.[39] The Italian Data Protection Authority fined the US company 5 million euros for failing to provide a legal basis for the processing operations carried out through 'Replika' and for failing to provide an adequate privacy policy in various respects. As in the previous case, the company had not provided for any mechanism to verify the age of users either at the time of registration for the service or during its use, even though the company stated that it excluded minors from among its potential users. In addition, the Authority has launched a new investigation to obtain clarification on the processing of data relating to the entire life cycle of the generative AI system underlying the 'Replika' service. In particular, it highlights the need for a thorough assessment of the risks and the adequacy of the technical and organisational measures adopted to protect personal data during the various stages of development, training and refinement of the language model that forms the functional architecture of the chatbot. The development of companion chatbots involves the processing of personal data throughout the entire life cycle of the system – from initial training to deployment – as these tools are designed to establish interactive personal relationships.[40]

assessments are an important element of accountability, as processing could present a high risk to the rights and freedoms of natural persons in the context of AI models'. For more details on the case, see M.G. Riva, 'Diritto e intelligenza artificiale generativa: l'istruttoria del Garante per la protezione dei dati italiano su "OpenAI e ChatGPt" ' *Ciberspazio e diritto*, 153-176 (2024)

[37] Art 166, decreto legislativo 30 June 2003 no 196.

[38] See the provision of Italian Data Protection Authority of 11 April 2023, available at www.garanteprivacy.it.

[39] For a detailed examination, see press release of Italian Data Protection Authority of 19 May 2025, available at www.garanteprivacy.it. This particular chatbot, equipped with a written and voice interface, allows users to 'generate' a 'virtual friend' to whom they can assign the role of confidant, therapist, romantic partner or mentor. With regard to the issue of the nature of the agreements concluded between social web operators and users, which also leads to the negotiability of a person's existential attributes, see C. Perlingieri, *Profili civilistici dei social networks* (Napoli: Edizioni Scientifiche Italiane, 2014), 66.

[40] For an examination of the critical aspects of companion chatbots, see P. Dewitte, 'Better alone than in bad company: Addressing the risks of companion chatbots through data protection by design' 54 *Computer Law and Security Review*, 1-20 (2024).

IV. Personal Data Impact Assessment: a Tool for Mitigating Risks to Fundamental Rights and Freedoms and Empowering Companies

It is therefore essential, in the field of personal data protection, to ensure the proper implementation of the principle of accountability, as established by the General Data Protection Regulation. The system introduced by the GDPR is no longer based on a set of precise rules to be observed under penalty of sanctions, but rather on the accountability of the data controller. In this sense, the principle of accountability is expressed on two levels: firstly, it requires the data controller to take appropriate and specific measures to ensure effective protection of personal data; secondly, it requires the data controller to be able to demonstrate that the measures taken are effective and appropriate for this purpose. In this context, the principle in question becomes a specific tool for ensuring the legal compliance of processing on the basis of risk management, assessing the impact on the plurality of fundamental rights and freedoms of individuals. Whenever organisations consider that a particular use of automated systems does not entail high-risk processing, they are required to document the reasons underpinning such an assessment. Where a data protection impact assessment reveals a high risk to fundamental rights and no measures have been adopted to adequately mitigate that risk, the corresponding DPIA must be notified to the relevant supervisory authorities.[41] However, the absence of the conditions triggering an obligation to notify the competent authority of the outcomes of a DPIA does not relieve the controller of the overarching duty to adopt appropriate measures to ensure the effective management of the risks posed to the rights and freedoms of data subjects by the processing activities in question.[42] In practice, this entails that controllers are required, inter alia, to implement data protection by design and by default, and to carry out an ongoing assessment of the risks generated by their processing operations, including the implications for fundamental rights, irrespective of whether a DPIA is formally undertaken.

In the framework of the principle of accountability, particular significance is attributed, from the perspective of extraterritorial protection, to the provisions of Art 27 of the GDPR, which mandates that controllers and processors not established within the EU but subject to the GDPR pursuant to Art 3, para 2, must designate a representative established in a Member State. Specifically, this applies

> 'where a controller or processor not established in the Union processes personal data of data subjects who are in the Union and its processing activities are related to the offering of goods or services to such data subjects in the Union, irrespective of whether a payment by the data subject is required, or to the monitoring of their behaviour, to the extent that such behaviour takes place

[41] See H. Janssen et al, n 8 above, 207.
[42] Arts 24 and 25 of the GDPR.

within the Union'.[43]

According to the Guidelines of the European Data Protection Board, the representative acts in the interest of the controller and the processor, but may be directly addressed by supervisory authorities, including measures and sanctions.[44] It is therefore not a mere symbolic figure, but an entity vested with a specific functional responsibility within the governance framework of the GDPR. Art 27 does not provide an exhaustive list of the representative's obligations, but from a combined reading of this provision with Arts 30, 58, and 83 GDPR, it follows that they must keep the record of processing activities[45] available to the authorities and act as a point of contact for data subjects; they must cooperate with the supervisory authority. No direct and autonomous obligation to carry out impact assessments emerges, which remain the responsibility of the controller. From a systemic perspective, the representative is not vested with an autonomous duty of direct protection of fundamental rights, but becomes a nexus between legal systems, indirectly contributing to the achievement of the Union's objectives in the field of personal data protection, algorithmic accountability and the prevention of technological risks.[46]

In any event, it must be reiterated that the DPIA delineates a process aimed at identifying risks arising from the processing of personal data and mitigating them as far as possible and as promptly as possible. In this regard, the representative may be configured as a functional nexus within the European architecture of accountability for entities not established in the Union, serving as the privileged point of contact between supervisory authorities, data subjects, and extra-EU controllers. In this manner, despite the absence of a substantive obligation to conduct assessments, the representative contributes indirectly to the effectiveness of the system for the protection of fundamental rights, reinforcing the procedural and territorial dimensions of the protection afforded by the European legal order.[47]

The principle of accountability marks the transition from an essentially remedial approach, typical of previous legislation, to a preventive model focused on the accountability of the data controller. In what can be defined as a 'risk-centric' approach, it requires the adoption of appropriate technical and organisational

[43] See Recital 80 of the GDPR. Furthermore, pursuant to Art 27, para 2, of the GDPR, the appointment of a representative is not necessary where the processing is not occasional, does not include processing, on a large scale, of special categories of data referred to in Art 9, para 1, or of personal data relating to criminal convictions and offences referred to in Art 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope, and purposes of the processing; also, where the data controller is a public authority or body.

[44] Cf 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', released in November 2018 by the Article 29 Working Party (now the EDPB), available at www.edpb.europa.eu.

[45] Art 30 of the GDPR.

[46] S. Anderson, 'Article 27, the Unknown GDPR Obligation' 3 *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel*, 11-14 (2019).

[47] Cf 'Guidelines 3/2018' n 44 above.

measures from the design stage of products and services involving the processing of personal data, requiring a proactive commitment to ensure compliance with the law and the protection of the rights of data subjects. In this way, the principle of accountability makes it possible to give concrete form, with specific reference to the right to privacy and human dignity, to those proposals of modern doctrine aimed at ensuring preventive protection of personality rights. The new regulation therefore provides for the need for control based on the precautionary principle, with specific duties imposed on the data controller, which implement the principle of accountability. Privacy by design, privacy by default and accountability privacy techniques have been appropriately identified as suitable tools for rebalancing the relationship between digital service providers and users, ensuring the effective implementation of personal data protection principles and placing users at the centre of IT processes.[48] In this context, the assessment of the impact on personal data protection is undoubtedly a specific tool aimed at managing and preventing the risks inherent in data processing.

However, despite its important role in data protection, there is no uniformity of views on its content, with particular reference to the obligation of the data controller to carry out an analysis of the risks to the rights and freedoms of data subjects.[49] On this point, there are two different lines of interpretation: one, of a universalist nature, which requires the data controller to examine the potential interference of the processing activity on the entire spectrum of fundamental rights and freedoms protected by EU law, in line with the ECHR; the other, more restrictive, considers it adequate to limit the assessment of risks to the provisions contained in the GDPR, ie the protection of privacy and personal data[50]. In other words, according to the latter interpretation, the data protection impact assessment is a process intended to ensure and demonstrate compliance with the Regulation itself, without any obligation for the data controller to assess any impact on other fundamental rights, limiting itself, for example, to checking compliance with transparency obligations and the rights of the data subject. It should be noted that the provisions of the GDPR and the right to data protection enshrined in Art 8 of the European Charter of Fundamental Rights are composed of principles and rules aimed at regulating the manner in which data processing is carried out, but which essentially do not prohibit specific processing activities or purposes, with the exception of Art 22 of the GDPR concerning automated decision-making processes relating to natural persons, including profiling. In fact, as has been accurately observed in legal doctrine, the purely procedural nature of European data protection legislation means that it is not suitable or effective for identifying 'substantial' risks to the fundamental rights and freedoms of data subjects. Although

[48] As argued by M. D'Ambrosio, *Progresso tecnologico, «responsabilizzazione» dell'impresa ed educazione dell'utente* (Napoli: Edizioni Scientifiche Italiane, 2017), 23.

[49] See D. Hallinan and N. Martin, n 8 above, 182-185.

[50] For further details, see D. Baldini, n 8 above, 58-60.

compliance with the European Regulation guarantees legitimacy and fairness and brings benefits to data subjects, such as reducing information asymmetries and enabling them to exercise control over their personal data, it does not preclude the possibility of unacceptable interference with fundamental rights and freedoms. In this sense, the DPIA fits into the regulatory framework in order to remedy these structural shortcomings in the legislation and, for this reason, with reference also to the latest cases brought to the attention of the Data Protection Authority, it seems difficult to consider that the scope defined by Art 35 of the GDPR can be limited to a reference to the rights to privacy and personal data protection alone.[51]

It is worth noting that WP29 embraces this interpretative reconstruction, explaining in the aforementioned guidelines that the reference to 'the rights and freedoms of data subjects' primarily concerns data protection and privacy rights, but also includes other fundamental rights such as freedom of expression, freedom of thought, freedom of movement, non-discrimination, and the right to freedom of conscience and religion. This understanding helps to broaden the frame of reference: from the information rights of individuals as such (including privacy) to a set of values, enshrined in the language of rights and freedoms, which aim to protect the individual, their development and their dignity.[52] Although impact assessment has been defined as a process for establishing and demonstrating the compliance of personal data processing activities with the regulation, the implication is that the scope of rights and freedoms is such that it may be possible to go beyond mere compliance with the traditional set of privacy 'principles', arguing that collective interests, beyond individual interests, should be included in data protection legislation, particularly with regard to AI.[53] In the context of algorithmic decision-making processes, data protection impact assessments (DPIAs) require data controllers to carefully consider the risks associated with possible errors, unfairness, bias and discrimination, and to identify concrete measures to mitigate them. Through this tool, the GDPR guides companies' design and operational choices, outlining the values and principles they must adhere to when designing and controlling automated decision-making systems. In this sense, the DPIA can be interpreted 'as a form of commitment to protect, or even enable, individual rights to a fair algorithmic process'.[54] In this perspective, impact assessment not only embodies the principle of accountability but also appears to be closely linked to the principle of transparency (Art 5(1) of the Regulation), which is essential to

[51] ibid 70-72.

[52] It should be noted that the DPIA is an essential aspect of establishing appropriate measures to safeguard individual rights, including in accordance with the 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', adopted on 6 February 2018 by the EDPB, 34, available at www. ec.europa.eu.

[53] The provisions of the GDPR on DPIA can be interpreted as a form of commitment to protect, or even enable, individual rights to a fair algorithmic process, see M.E Kaminski and G. Malgieri, *Algorithmic impact assessments under the GDPR* n 10 above, 131-132.

[54] ibid

counteract the opacity resulting from the algorithmisation of personal data.[55] Arts 13 and 14 of the GDPR require that data subjects be informed of the existence of automated decision-making processes, including profiling, and provided with meaningful information about the logic involved, its significance and the expected consequences. The Italian Supreme Court has also ruled on this point, reiterating that consent to the processing of personal data must be freely and specifically given, with full awareness of the underlying algorithmic logic.[56] The role played by the supervisory authorities is important, as they impose financial penalties that are at the top of the pyramid of penalties that can be imposed and punish the most serious violations, when it is the principle of accountability itself that is violated. In particular, the Data Protection Authority reiterated, in the measure cited on OpenAI, the centrality of the DPIA as a substantive guarantee, highlighting how the failure to carry out a prior assessment of the risks associated with the use of advanced technologies, such as systems based on generative artificial intelligence, can cause serious harm to vulnerable individuals, in particular minors.

In support of the interpretation that the impact assessment provided for in Art 35 of the GDPR is a tool aimed at mitigating the risks to the fundamental rights and freedoms recognised by the Charter of Fundamental Rights of the European Union, there are comments highlighting the lack of clear operational guidance on how, in practice, the data controller should assess the potentially adverse effects of its processing activities. Just consider that for DPIA, despite the availability of models proposed by some supervisory authorities (such as the Italian Data Protection Authority or the *Commission nationale de l'informatique et des libertés*),[57] these are not binding and often have a more general structure, making them less suitable for particularly complex or risky treatments.

V. Conclusions

Ultimately, it is essential to emphasise the need to strengthen the guidance concerning the content and procedures of impact assessments, within a constantly evolving context that has been further accelerated by the entry into force of the AI Act. This developmental trajectory aligns with the broader process of consolidating

[55] 'To start, one can consider the DPIA risk assess ment process as one element within the context of the GDPR as an ecosystem of connected legal principles. In this regard, the DPIA risk assessment process has substantial links with other principles in the GDPR. Thus, interpretations of the content of the DPIA process should be consistent with these other principles', see D. Hallinan and N. Martin, n 8 above, 183.

[56] For further information see Corte di Cassazione 10 October 2023 no 28358, *Il diritto di famiglia e delle persone*, 1558 (2023); see also Corte di Cassazione 25 May 2021 no 14381, *Il diritto dell'informazione e dell'informatica*, 1001 (2021).

[57] The French Data Protection Authority has made templates and tools available to help organisations conduct Data Protection Impact Assessments, providing detailed guides and checklists to help organisations identify processing operations that require a DPIA, assess the risks and implement appropriate safeguards, see the website www.cnil.fr.

European constitutional traditions, which prioritise the recognition and protection of the inviolable rights of the individual. For this reason, the proper application of the principle of accountability is essential. This principle entails a prior assessment of the lawfulness of data processing activities and represents a new organisational criterion for entities involved in the management of personal data.[58] It is fully aligned with a harm-prevention approach, which proves more suitable for safeguarding personality rights[59]. However, as has been observed, the procedural nature of the GDPR, while ensuring the lawfulness of processing, is not always sufficient to protect individuals' fundamental rights from harmful interferences. The new instruments under consideration are all grounded in a careful assessment of the risks to the rights and fundamental freedoms of data subjects. On this basis, data controllers are required to implement targeted technical and organisational measures aimed at safeguarding the full spectrum of individual rights, with the ultimate goal of fostering more responsible and explainable algorithmic systems. In this sense, the DPIA should fill this gap and consider not only data protection but also other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, and the right to freedom of conscience and religion. The Article 29 Working Party endorses this interpretation, stating in its guidelines that impact assessments should consider not only the right to privacy, but also other fundamental freedoms enshrined in the Charter of Fundamental Rights of the European Union. In this light, the impact assessment not only embodies the principle of accountability, but is also closely linked to the principle of transparency (Art 5 GDPR), which is essential in addressing the opacity associated with the algorithmic processing of personal data.[60] These considerations reaffirm the crucial role of the impact assessment as a tool for mitigating risks to fundamental rights protected under EU law. However, several scholars and practitioners have pointed out the lack of clear guidance on how data controllers should assess such risks in practice. Although data protection authorities – such as the Italian Garante or the CNIL – have developed DPIA models, these are not legally binding and may lack sufficient detail when applied to high-risk processing operations. In conclusion, the data protection impact assessment constitutes a substantive and structured process of analysis and prevention, aimed at ensuring that both design and operational choices are fully compatible with the respect for

[58] In this perspective, the proposals for the adaptation of civil liability rules to AI – ranging from strict liability for damage caused by defective digital products to aggravated fault of AI system providers – seek to reconcile the competing interests involved and to move towards a more mature model of AI liability, one that is refined and deepened in the light of the principle of accountability. For a detailed examination, see M. Gambini, 'Nuovi paradigmi della responsabilità civile per l'Intelligenza artificiale' *Rassegna di diritto civile*, 1290 (2023).

[59] On the primacy of the person see P. Perlingieri, *La personalità umana nell'ordinamento giuridico* (Camerino-Napoli: Edizioni Scientifiche Italiane, 1972), 13; Id, *La persona e i suoi diritti. Problemi del diritto civile* (Napoli: Edizioni Scientifiche Italiane, 2005).

[60] See 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' adopted on 20 October 2020 by EDPB, 19-21, available at www. ec.europa.eu.

human dignity and the fundamental rights of data subjects.[61] From this perspective, and in light of the most recent guidance issued by supervisory authorities, it is increasingly evident that the scope of Art 35 of Regulation (EU) 2016/679 cannot be confined solely to the rights to privacy and data protection. Rather, it must be understood as encompassing the broader range of fundamental rights and freedoms enshrined in the Charter of Fundamental Rights of the European Union. This implies a strengthened role for the data controller, who is required to adopt a central and proactive stance in assessing and mitigating the potential impacts of their processing activities, through an approach grounded in prevention, transparency, and genuine, demonstrable accountability.

[61] D. Baldini, n 8 above, 70.