REINVENTING DATA PROTECTION IN THE AI ERA: CHALLENGES FOR THE KNOWLEDGE SOCIETY

Andreea BURUIANĂ*

Abstract

The unprecedented expansion of artificial intelligence across all sectors of contemporary society calls into question the traditional normative architecture of personal data protection, built upon the premises of the classical information age and upon the paradigm of a rational, informed human subject capable of effectively exercising their digital rights. This article proposes a systematic analysis of the challenges that artificial intelligence systems — in particular large language models, facial recognition systems, automated decision-making algorithms, and predictive surveillance networks — pose to the normative framework of data protection, with particular emphasis on the European Union's General Data Protection Regulation (GDPR) and the EU Artificial Intelligence Act (AI Act). The first part examines the structural tensions between the fundamental principles of data protection law — informed consent, data minimisation, purpose limitation, and the right of access — and the intrinsic characteristics of artificial intelligence systems: algorithmic opacity, implicit knowledge transfer, large-scale data exploitation, and the capacity to infer sensitive attributes from ostensibly anonymised data. The second part analyses the normative responses developed at European and international level, critically examining mechanisms of algorithmic accountability, transparency and explainability obligations, data protection impact assessments, and the role of supervisory authorities in the AI context. The third part identifies the emerging challenges of data protection in the knowledge society: biometric and neural data, generative artificial intelligence and intellectual property rights, data sovereignty and jurisdictional conflicts, as well as the ethical dimension of AI governance. The conclusions underscore the necessity of an integrated, coherent, and adaptive normative framework capable of protecting individuals' fundamental rights in the face of the processing power of artificial systems, without stifling the technological innovation essential to the knowledge society.

Keywords: *personal data protection, artificial intelligence, GDPR, AI Act, fundamental digital rights*.

1. Introduction

The knowledge society - a concept forged at the intersection of information sociology, the digital economy, and political philosophy - is defined by its unprecedented capacity to produce, process, distribute, and valorise information as a fundamental resource underpinning social organisation and economic value creation[1]. In this society, personal data has become a strategic resource of an importance comparable to oil in the industrial economy of the twentieth century - a metaphor well-established in contemporary academic and political discourse which, however imperfect, accurately captures the dynamics of power in the current digital ecosystem[2]. Artificial intelligence (AI) constitutes the technological vector that transforms this resource into the capacity for action, prediction, and control, exponentially amplifying both the beneficial potential and the systemic risks of the data society. The normative framework for the protection of personal data, crystallised in Europe through Regulation (EU) 2016/679 - the General Data Protection Regulation (GDPR) - represented at the time of its adoption the most ambitious and comprehensive instrument for regulating personal data processing at a global level, establishing standards that have inspired similar legislation in dozens of jurisdictions. However, the GDPR was conceived within a technological paradigm that predated the explosion of deep learning systems, generative language models, and architectures of ubiquitous algorithmic surveillance. Its application to the latest generation of artificial intelligence systems reveals deep structural tensions arising from fundamental

* PhD Candidate, „Titu Maiorescu" University of Bucharest, Ștefan cel Mare University of Suceava (e-mail: buruianaandreea90@uahoo.com).

[1] Castells, M., The information age: Economy, society, and culture. Vol. I: The rise of the network society (2nd ed.), Wiley-Blackwell, 2010, p. 33.

[2] Zuboff, S., The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs, 2019, pp. 12-15.

incompatibilities between the normative logic of data protection and the technical logic of machine learning[3]. The adoption of the EU Artificial Intelligence Act (AI Act, Regulation [EU] 2024/1689) constituted a historic milestone in global digital governance: for the first time, a legally binding instrument of regional scope classifies AI systems according to their risk level and imposes specific requirements regarding transparency, robustness, human oversight, and accountability[4]. Nevertheless, the articulation of the AI Act with the GDPR and with the broader European data protection framework raises normative questions of considerable complexity, with direct implications for the design of AI systems, for organisational data processing practices, and for the exercise of individual rights in the digital space.

This article aims to critically examine the challenges that artificial intelligence poses to the normative architecture of data protection in the knowledge society, structuring the inquiry across three complementary chapters. The first chapter examines the structural tensions between GDPR principles and the technical characteristics of AI systems. The second chapter analyses the European and international normative responses, with particular emphasis on the AI Act and mechanisms of algorithmic accountability. The third chapter identifies the emerging challenges of data protection in the context of generative AI, neurotechnology, and data sovereignty. The research is grounded in a critical analysis of legal doctrine, European Union legislation, relevant jurisprudence, and reports of data protection authorities, aiming to offer a comprehensive and up-to-date perspective on one of the most dynamic and challenging fields of contemporary law.

2. Structural Tensions Between the GDPR Architecture and Artificial Intelligence Systems

The free, specific, informed, and unambiguous consent of the data subject constitutes one of the central legal bases for data processing under the GDPR [5]. This conception of consent, inherited from the Enlightenment tradition of individual autonomy and from the contractual theory of civil law, presupposes a rational, informed subject capable of evaluating the consequences of consenting to the processing of their data. Artificial intelligence systems undermine these premises in multiple and structural ways, generating what the doctrine has termed the digital consent paradox[6]. In the first place, the technical complexity of machine learning algorithms makes it practically impossible to genuinely inform data subjects about how their data will be used to train models, what inferences the system will produce, and what impact those inferences will have on their rights and interests. Privacy notices and privacy policies have reached a level of complexity that renders them unworkable as genuine instruments of information: empirical studies demonstrate that reading all the privacy policies of services used by an average American would require approximately 76 working days per year[7]. In the context of AI, this crisis of informed consent is amplified by the intrinsic opacity of deep learning models, which cannot be explained in terms intelligible to a general audience. In the second place, the dynamic nature of AI systems - which evolve continuously through incremental training, fine-tuning, and adaptation to new data - generates fundamental problems regarding the specificity and currency of consent. Consent granted at an initial moment for a particular purpose may become irrelevant or insufficient following substantial modifications to the algorithm or to the uses of the trained model. Article 7 of the GDPR provides for the right to withdraw consent; however, in the context of AI models trained on massive datasets, the withdrawal of consent and the effective erasure of an individual's data from the parameters of an already-trained model represents a first-order technical challenge, partially addressed by the concept of machine unlearning, but still far from a satisfactory normative solution[8].

In the third place, AI models may operate on ostensibly anonymised or pseudonymised data, generating inferences about identifiable individuals without the input data formally constituting personal data. Re-identification techniques applied to anonymised data have demonstrated that anonymisation guarantees are far more fragile than initially assumed: landmark studies have shown that 87% of the US population can be re-

[3] Wachter, S., Mittelstadt, B., & Russell, C. (2017). Counterfactual explanations without opening the black box: Automated decisions and the GDPR, Harvard Journal of Law & Technology, 31(2),2017, p. 860.

[4] European Parliament & Council, Regulation (EU) 2024/1689 of the European Parliament and of the Council on artificial intelligence (AI Act), Official Journal of the European Union, L, 2024, p. 1689.

[5] (Article 6(1)(a) of Regulation [EU] 2016/679).

[6] Solove, D. J., Introduction: Privacy self-management and the consent dilemma, Harvard Law Review, 126(7), 2013, pp. 1888–1903.

[7] McDonald, A. M., & Cranor, L. F., The cost of reading privacy policies, Journal of Policy for the Information Society, 4(3), 2008, p. 550.

[8] Cao, Y., & Yang, J., Towards making systems forget with machine unlearning, Proceedings of the 2015 IEEE Symposium on Security and Privacy, 2015, pp. 463–480.

identified by combining three seemingly innocuous variables - zip code, date of birth, and sex [9]In the context of AI models trained on massive datasets, the capacity for re-identification is substantially amplified, raising profound questions about the effectiveness of current anonymisation techniques as a data protection mechanism (Narayanan & Shmatikoff, 2008).

3. Data minimisation and purpose limitation in the context of machine learning

The principle of data minimisation - enshrined in Article 5(1)(c) of the GDPR, which requires that data be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed - stands in direct structural tension with the technical logic of machine learning systems. The performance of AI models is systematically and positively correlated with the volume and diversity of training data: the more data, the more robust and performant the model. This logic of data maximisation, which governs the data economy and the competitive strategies of AI companies, is diametrically opposed to the normative imperative of minimisation, generating a fundamental contradiction between legal standards and techno-economic imperatives[10].

The principle of purpose limitation - Article 5(1)(b) of the GDPR - requires that data collected for a specific purpose not be subsequently processed in a manner incompatible with that purpose. In practice, AI systems present considerable difficulties in this regard: data originally collected for a healthcare service may subsequently be exploited to train financial scoring models; behavioural data of social media users may be used to train emotional recognition systems; location data may be aggregated to produce inferences about political beliefs or religious preferences. The compatibility of a secondary use of data for AI model training with the original purpose of collection represents an issue of remarkable normative complexity, which Recital 50 of the GDPR and the guidelines of the European Data Protection Board do not resolve in a satisfactory manner[11]. The concept of privacy by design, enshrined as a legal obligation through Article 25 of the GDPR, requires the integration of data protection into the design of information systems from the initial conceptualisation phase. In the context of AI systems, privacy by design involves selecting architectures that minimise data collection - for example, through federated learning, which allows models to be trained without centralising raw data, or through differential privacy, which adds controlled statistical noise to protect individual data within aggregated datasets. Although these advanced privacy-preserving techniques represent significant advances, they entail technical trade-offs between data protection and model performance, and their voluntary adoption by the AI industry remains fragmented and insufficient[12].

4. Automated decision-making, explainability, and the right not to be subject to algorithmic profiling

Article 22 of the GDPR enshrines the right of the data subject not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them. This right, together with the right to explanations provided for in Recitals 71 and 75, has generated a remarkably intense debate in both legal and technical scholarship regarding the content and limits of the right to algorithmic explainability[13]. The Court of Justice of the European Union has not yet delivered a definitive ruling on the interpretation of Article 22; however, the jurisprudence of the German Federal Administrative Court and of French courts is beginning to trace more precise normative contours. The fundamental tension in this domain resides in the intrinsic incompatibility between explainability and performance in highly complex deep learning models. Neural networks with hundreds of millions or billions of parameters - such as GPT, BERT, and transformer-based facial recognition systems - cannot be explained in causal-effect terms intelligible to a non-specialist without significant losses in accuracy. Post-hoc explainability techniques - LIME, SHAP, Grad-CAM -

[9] Sweeney, L., Simple demographics often identify people uniquely, Carnegie Mellon University, Data Privacy Working Paper, 2000, p.10.

[10] 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, 2019(2), 2019, pp.494–620.

[11] Malgieri, G., & Comandé, G., Why a right to legibility of automated decision-making exists in the general data protection regulation, International Data Privacy Law, 7(3), 2017, p.260.

[12] Dwork, C., & Roth, A., The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3–4),2014, pp. 211–214.

[13] Wachter et al., op.cit, p.49.

provide local approximations of model behaviour, but do not furnish veridical causal explanations of the decision-making process [14].This fundamental technical limitation generates a direct conflict with the normative requirements of the GDPR regarding the transparency and explainability of automated decisions.

Algorithmic profiling - defined in Article 4(4) of the GDPR as any form of automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to a natural person - has undergone unprecedented expansion in the contemporary digital economy. Credit scoring systems, recruitment algorithms that filter candidates through the analysis of CVs and social media activity, dynamic pricing algorithms, and risk assessment systems in the context of predictive justice are examples of algorithmic profiling with a direct and significant impact on individual rights and opportunities [15]The regulation of these practices through Article 22 of the GDPR raises unresolved normative questions regarding the definition of significant effects, the possibilities for opposition, and the guarantees required for meaningful human intervention.

A landmark case in European jurisprudence regarding algorithmic profiling is the SCHUFA Holding AG case, in which the Court of Justice of the European Union held, in its judgment in Case C-634/21 (2023), that the provision of a probability score calculated on the basis of an individual's personal data constitutes an automated decision within the meaning of Article 22 of the GDPR where third parties have accorded that score decisive importance in establishing contractual relationships with the person concerned [16]This judgment substantially clarified the scope of Article 22 and generated significant normative pressure on the financial services industry and credit scoring agencies.

5. European and International Normative Responses: The AI Act, GDPR, and Algorithmic Accountability

The EU Artificial Intelligence Act (AI Act, Regulation [EU] 2024/1689), adopted by the European Parliament on 13 March 2024 and entering into force on 1 August 2024, constitutes the first legally binding instrument for the horizontal regulation of AI systems at a global level and represents a piece of legislation of paradigmatic importance for worldwide digital governance[17]. Its normative architecture is structured around a four-tier risk classification system - unacceptable risk, high risk, limited risk, and minimal risk - which generates differentiated requirements proportionate to the potential harm of AI systems to fundamental rights, health, safety, and democracy.

AI systems with unacceptable risk - including state-run social scoring, emotion recognition in workplaces and educational institutions, predictive biometrics based on protected characteristics, and individualised predictive policing - are entirely prohibited on EU territory, with strict exceptions for remote biometric identification in public spaces for law enforcement purposes. This absolute prohibition reflects a clear value choice by the European legislator: certain uses of AI are considered incompatible with the fundamental values of the Union, irrespective of technical performance or economic advantages[18]. High-risk AI systems - including those deployed in critical infrastructure, education, employment, essential services, law enforcement, migration and asylum management, and the administration of justice - are subject to a stringent regime of requirements: pre-market conformity assessment, transparency registries, detailed technical documentation, risk management systems, data quality and robustness standards for training datasets, automatic activity logs, and meaningful human oversight. These requirements are complementary to, yet not identical with, the data protection obligations imposed by the GDPR, generating a dual compliance regime for operators who use high-risk AI systems in the processing of personal data[19].

The articulation between the AI Act and the GDPR constitutes one of the central normative challenges of implementing the new European regulatory framework. The Data Protection Impact Assessment (DPIA), required by Article 35 of the GDPR for processing operations likely to result in high risks to individuals' rights, overlaps

[14] Rudin, C., Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead, Nature Machine Intelligence, 1(5), 2019, pp.206–215.

[15] O'Neil, C., Weapons of math destruction: How big data increases inequality and threatens democracy, Crown Publishers, 2016, p.33.

[16] Curtea de Justitie a Uniunii Europene. (2023). OQ v. Land Hessen (SCHUFA Holding AG), C-634/21, ECLI:EU:C:2023:957.

[17] European Parliament & Council, Regulation (EU) 2024/1689 of the European Parliament and of the Council on artificial intelligence (AI Act), Official Journal of the European Union, L, 2024, p.1690.

[18] Helberger, N., Doshi-Velez, F., & Naudts, L., Toothless and timid or bold and brave? The vision behind the AI Act, Algorithm Watch., 2022, p.22.

[19] Veale, M., & Zuiderveen Borgesius, F., Demystifying the draft EU Artificial Intelligence Act, Computer Law Review International, 22(4), 2021, pp.97–112,

partially with the conformity assessment provided for by the AI Act for high-risk AI systems. The European Data Protection Board has issued guidelines on the coordination of the two instruments; however, the practical implementation of simultaneous GDPR and AI Act requirements will substantially test the compliance capacities of organisations, in particular small and medium-sized enterprises[20].

6. Transparency, explainability, and accountability obligations in AI systems

Transparency obligations constitute a central element of both the GDPR and the AI Act, reflecting the shared conviction that individuals cannot effectively exercise their digital rights in the absence of adequate information regarding how their data are processed and the logic of automated decisions affecting them. The GDPR requires, through Articles 13 and 14, the provision of comprehensive information regarding the identity of the controller, the purposes and legal bases of processing, data recipients, and data subjects' rights. The AI Act adds specific requirements regarding the information of users about their interaction with AI systems, the obligation to label AI-generated content, and technical documentation requirements for high-risk systems[21]. The concept of algorithmic explainability - referred to in both technical and legal scholarship by the acronym XAI (eXplainable Artificial Intelligence) - has become an explicit object of regulation in the AI Act, which requires high-risk AI systems to be sufficiently transparent to permit human users and supervisors to interpret their outputs. This normative requirement has stimulated an emerging industry of XAI tools, but has also generated intense scientific debate regarding the technical feasibility of veridical explainability for deep learning models and the risk that post-hoc explanations may be misleading or incomplete [22].The tension between performance and explainability remains one of the fundamental technical limitations of the field.

Accountability - the principle enshrined in Article 5(2) of the GDPR, requiring controllers to demonstrate compliance with data protection principles - acquires additional dimensions in the AI context. The complex accountability chains in the AI ecosystem - foundation model providers, AI system providers, operators using AI systems, and data subjects - generate considerable difficulties in attributing responsibility for harms caused by automated decisions. The AI Act introduces a more precise allocation of responsibilities between providers and users of AI systems, but the relationship between AI Act liability and civil tort liability for AI-caused harm remains partially and imperfectly regulated[23].National data protection supervisory authorities - in Romania, the National Supervisory Authority for Personal Data Processing (ANSPDCP) - will acquire, under the AI Act, new competences and additional oversight tasks regarding AI systems used in personal data processing contexts. Strengthening the institutional and technical capacity of these authorities is a sine qua non condition for the effective enforcement of the new regulatory framework: the investigation of opaque AI systems, the technical assessment of algorithmic compliance, and the sanctioning of violations in highly technical domains require expertise that transcends the traditional legal training of supervisory authority staff.

7. Data subjects' rights in the context of AI-based processing

The catalogue of data subjects' rights enshrined in the GDPR - the right of access (Article 15), the right to rectification (Article 16), the right to erasure (Article 17), the right to restriction of processing (Article 18), the right to data portability (Article 20), and the right to object (Article 21) - proves insufficiently adapted to the technical realities of AI-based processing. The effective exercise of these rights presupposes the capacity of controllers to identify and extract an individual's data from large-scale processing systems - a substantial technical challenge in the context of AI models trained on datasets of billions of elements, entailing high costs and risks to the integrity of the models[24].The right to data portability - an instrument designed to stimulate competition in digital markets and to reduce lock-in effects generated by network externalities - carries significant transformative potential, but is conditioned upon the existence of interoperable technical formats

[20] European Data Protection Board, Guidelines 06/2022 on the interplay between the application of Article 3 and the provisions on international transfers, EDPB, 2023, p.15.

[21] European Parliament & Council, Regulation (EU) 2024/1689 of the European Parliament and of the Council on artificial intelligence (AI Act), Official Journal of the European Union, L, 2024, p.1689.

[22] Rudin, C., op.cit., p.210.

[23] Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., & Vayena, E., AI4People — An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations, Minds and Machines, 28, 2018,pp. 689–707.

[24] Mantelero, A., The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten'. Computer Law & Security Review, 29(3), 2014, pp.229–235.

and common data representation standards that the AI industry has not yet uniformly adopted. European initiatives to create common data spaces - in the domains of health, agriculture, mobility, and finance - seek to build data portability and interoperability infrastructures at European scale, but their implementation requires substantial investment and complex institutional coordination[25].

The right to erasure - popularly termed the right to be forgotten following the Court of Justice of the European Union's ruling in Google Spain SL v. Agencia Espanola de Proteccion de Datos[26]- acquires a specific technical dimension in the context of AI. The erasure of an individual's data from a training database does not automatically result in the elimination of knowledge acquired by the model through processing that data. Machine unlearning techniques - procedures for retraining or modifying models to eliminate the influence of specific data - are still in the research phase and have not yet attained the maturity required for industrial-scale implementation[27]. This technical gap generates an unresolved normative tension between the legal obligation to erase data and the technical reality of trained AI models. The remedial mechanism of the GDPR - comprising the right to an effective judicial remedy against controllers and supervisory authorities (Article 79) and the right to compensation for material or non-material damage suffered as a result of a breach of the Regulation (Article 82) - has generated an emerging national jurisprudence of growing impact. Administrative fines imposed by national authorities - including sanctions in the order of billions of euros imposed on companies such as Meta, Google, and Amazon - have demonstrated that the GDPR's sanctioning mechanism is capable of generating significant compliance pressures, even if its application to AI systems raises considerable challenges of proof and causation [28].

8. Emerging Challenges of Data Protection in the Algorithmic Knowledge Society

The proliferation of generative artificial intelligence systems - large language models (LLMs) such as GPT-4, Gemini, Claude, and Llama; synthetic image generation systems such as DALL-E and Midjourney; and multimodal models capable of producing text, images, audio, and video from a single prompt - has generated a set of normative challenges of unprecedented novelty and complexity for data protection law[29]. These systems are trained on colossal datasets extracted from the public space of the internet, which inevitably contain personal data - data about public figures, content published by users on digital platforms, publicly disclosed private correspondence, and identifying information present in publicly accessible documents. The collection and use of such data for the purpose of training generative models raises profound normative questions under the GDPR: what is the legal basis for processing personal data for the purpose of training LLMs? Can the legitimate interest exception provided for in Article 6(1)(f) of the GDPR be invoked for the training of commercial AI models? Does training constitute a purpose compatible with the original purposes for which data were published? Data protection authorities in several EU Member States have begun addressing these questions through investigations and sanctioning decisions: the Garante per la protezione dei dati personali (the Italian authority) ordered the temporary blocking of ChatGPT in Italy in 2023, citing the absence of a valid legal basis for processing the personal data of Italian users[30].

A specific challenge of generative AI is the phenomenon of training data memorisation - the capacity of models to reproduce, upon request, fragments of the data on which they were trained, including personal data. Landmark studies have demonstrated that large language models can, under certain conditions, reproduce email addresses, telephone numbers, fragments of private correspondence, and other personal data present in training data[31]. This capacity for memorisation transforms AI models into potential sources of personal data leakage, generating data security risks that do not easily fit into the typology of security incidents regulated by Article 33 of the GDPR. Copyright and the right to one's image in the context of generative AI represent an adjacent but

[25] European Commission, A European strategy for data. COM(2020) 66 final, Publications Office of the European Union, 2020,p.100.

[26] (C-131/12, 2014)

[27] Cao & Yang, op.cit, p.60.

[28] Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F., The European Union general data protection regulation: What it is and what it means, Information & Communications Technology Law, 28(1), 2019,1-34.

[29] Bommasani, R., Hudson, D. A., Aditi, E., Altman, R., Arora, S., Khattar, S., & Liang, P., On the opportunities and risks of foundation models, 2021, p.45.

[30] Garante per la protezione dei dati personali, ChatGPT: Il Garante riapre il caso, il gestore di ChatGPT ha fornito risposte insoddisfacenti. Garante. https://www.garanteprivacy.it. 2023,(seen at 25.04.2026.)

[31] Carlini, N., Tramer, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., & Roberts, A., Brown, T., Song, D., Erlingsson, U., Oprea, A., Raffel, C., Extracting training data from large language models, Computer Science.Cryptography and Security, 2021, pp.1-19.

deeply interconnected dimension to data protection. The images, voice, and creative style of natural persons may constitute personal data within the meaning of the GDPR, and their use for training generative models without the consent of the individuals concerned raises simultaneous issues of data protection and copyright law. European and American jurisprudence in this domain is in the process of crystallisation: American courts are examining actions in liability brought by artists against developers of image generation systems, while the Court of Justice of the European Union is expected to rule on the text and data mining exception provided for in the Directive on Copyright in the Digital Single Market[32].

9. Neural data, advanced biometrics, and the frontiers of the new digital intimacy

The expansion of neurotechnology - devices that measure, interpret, and in some cases stimulate brain activity - and its convergence with AI systems opens a domain of data protection of exceptional importance and normative urgency: that of neural data or neurodata. Brain-computer interfaces (BCIs), consumer EEG devices, neurofeedback applications, and therapeutic neurostimulation systems generate data about the cerebral activity of individuals — data that may reveal, especially after processing through AI algorithms, thoughts, emotions, cognitive predispositions, mental health states, and psychological vulnerabilities with unprecedented granularity [33]. The current GDPR framework protects neural data insofar as they fall within the special categories of data provided for in Article 9 - health data or biometric data - or insofar as AI systems processing them produce inferences about these sensitive categories. However, this protection by analogy is insufficient given the specificity and extreme sensitivity of neural data. Chile and Colombia have already adopted specific regulations on neurorights; Spain and France are discussing constitutional amendments regarding the protection of mental integrity. International legal doctrine promotes the recognition of a distinct set of neurorights - the right to cognitive liberty, the right to mental continuity, the right to mental privacy, and the right to psychological equality - as fundamental rights specific to the age of neurotechnology[34].

Biometric data - defined in Article 4(14) of the GDPR as personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person - have undergone a massive expansion of AI-based uses: facial recognition in public and private spaces, gait and gesture analysis, voice recognition, emotional analysis based on micro-facial expressions, and multimodal biometric identification systems. The AI Act prohibits the use of real-time remote biometric recognition systems in publicly accessible spaces by law enforcement authorities, with strict exceptions, but does not comprehensively regulate private uses of facial recognition, leaving significant normative gaps[35].

10. Data sovereignty, jurisdictional conflicts, and the global dimension of data protection in the AI era

The concept of digital sovereignty - the capacity of states and regional blocs to control data generated on their territory and to impose their normative standards in digital governance - has acquired growing prominence in European and international political discourse, in the context of the dominance of American and Chinese platforms in the global data economy. The European data strategy, published by the European Commission in 2020, articulates the vision of a European data space - characterised by data portability, interoperability, and security, subject to GDPR principles - as an alternative to the closed ecosystem models of major digital platforms[36]. International transfers of personal data to third countries - regulated by Chapter V of the GDPR - have generated some of the most intense legal disputes in the history of European data protection. The series of Schrems rulings - Schrems I (C-362/14, 2015) and Schrems II (C-311/18, 2020) - in which the Court of Justice of the European Union successively invalidated the Safe Harbor and Privacy Shield mechanisms for EU-US data transfers, demonstrated the fragility of the international data transfer architecture when measured against the requirements of effective protection of fundamental rights. The adoption of the EU-US Data Privacy Framework

[32] Zittrain, J., IP and the future of AI: Creative attribution and compensation, Harvard Law Review Forum, 136, 2023,pp.120–144.

[33] Ienca, M., & Andorno, R., Towards new human rights in the neurotechnology era: Cognitive liberty, mental privacy, mental integrity and psychological continuity. Life Sciences, Society and Policy, 13(5), 2017, pp.1–21.

[34] Yuste, R., Goering, S., Arcas, B. A. Y., Bi, G., Carmena, J. M., Carter, A., & Wolpaw, J., Four ethical priorities for neurotechnologies and AI. Nature, 551(7679), 2021,pp. 159–163.

[35] Terec-Vlad, L., & Rusu, A. Neuro-Cybersecurity and the Future of Cognitive Rights: Legal Foundations for the Protection of the Human Mind in the Digital Age. Revista Romanească pentru Educație Multidimensională, 18(1),2026, pp. 82-104.

[36] European Commission, op.cit., p.99.

in 2023 re-established a transfer mechanism, but the continuation of litigation by the organisation NOYB (None of Your Business) suggests that this issue is not yet definitively resolved[37].

Global regulatory fragmentation in the fields of data protection and AI generates significant risks of regulatory arbitrage - the practice whereby operators locate their data processing activities or AI system development in jurisdictions with more permissive normative standards, in order to circumvent the stricter requirements of other jurisdictions. The divergence between the European model based on fundamental rights (GDPR, AI Act), the fragmented and sectoral American model, the Chinese model grounded in state sovereignty and governmental access to data, and the emerging models of India, Brazil, and South Africa generates an incoherent global normative landscape that reduces the effectiveness of any national or regional data protection system[38].

The UN initiative to develop an international treaty on AI - discussed within the UN Human Rights Council and promoted by General Assembly Resolution A/78/L.49 of 2024 - could constitute a vector of global normative convergence, establishing minimum common standards for the protection of human rights in the AI context. Nevertheless, the experience of negotiations in the fields of internet law and electronic commerce suggests that achieving global consensus on common AI regulatory principles is a formidably challenging objective, given that technologically dominant states have structural interests in maintaining normative flexibility for their domestic AI industries[39]. Ethical AI governance - understood as the set of principles, processes, and institutional mechanisms ensuring that AI is developed and used in conformity with fundamental values and rights - is increasingly recognised as a necessary, though not sufficient, condition of effective data protection in the AI era. The ethical principles formulated by the OECD (2019)[40], the European Commission (2019), and UNESCO (2021)[41] converge around the values of transparency, accountability, non-discrimination, robustness, and human primacy, but the major criticism levelled at these principles - including by legal scholarship - is their voluntary character and the absence of concrete enforcement mechanisms. The transition from principled ethics to effective legal accountability represents precisely the central stake of the AI Act and of the European regulatory framework under construction[42].

11. Conclusions

The analysis conducted in this article demonstrates that the protection of personal data stands, in the context of the expansion of artificial intelligence systems, at a normative turning point of paradigmatic importance. The framework constructed through the GDPR in 2016 represented a major normative advance over Directive 95/46/EC, but was conceived within a technological paradigm that predated the current amplitude of deep machine learning systems. The structural tensions between data protection principles and the technical characteristics of AI - opacity, data maximisation, transferable learning, and re-identification capacity - cannot be resolved through the simple extensive application of existing norms, but require substantial normative adaptations and innovative implementation mechanisms[43].

The AI Act represents Europe's response to this challenge and constitutes the most ambitious instrument for regulating AI ever adopted by a public authority. Its normative value resides not only in its substantive content, but also in the global regulatory effect it generates - the Brussels Effect - whereby European standards become global references in the absence of comparable institutional alternatives. Nevertheless, its effective implementation will depend on the institutional capacity of national supervisory authorities, on the jurisprudential clarification of the numerous indeterminate concepts in the text of the Regulation, and on the elaboration of harmonised technical standards that translate abstract normative requirements into concrete technical specifications. The emerging challenges identified in the third chapter - generative AI, neural data,

[37] Curtea de Justitie a Uniunii Europene. (2020). Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), C-311/18, ECLI:EU:C:2020:559..

[38] Bradford, A., The Brussels effect: How the European Union rules the world. Oxford University Press, 2020, p.111.

[39] Dafoe, A, AI governance: A research agenda. Future of Humanity Institute, University of Oxford, 2018, p.60.

[40] OCDE. (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. https://legalinstruments.oecd.org (seen at 26.04.2026)

[41] UNESCO. (2021). Recommendation on the ethics of artificial intelligence. SHS/BIO/PI/2021/1. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000381137 (seen at 26.04.2026)

[42] Mittelstadt, B., Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, 1(11), 2019, pp. 501–507.

[43] Terec-Vlad, L., Ungureanu, C.G., The Rights of Artificial Intelligence: Between Ethics, Law and Normative Pragmatism, Revista Universul Juridic, 9, 2025, pp.72-83.

global normative fragmentation, and regulatory arbitrage - signal that the normative dynamics of data protection in the AI era are far from stabilised. The pace at which AI systems evolve - from text-only models to multimodal systems, from narrow AI to systems with increasingly general capabilities - exceeds the natural rhythm of normative elaboration, generating a structural gap between the technological frontier and the legal frontier. This temporal asymmetry demands the adoption of adaptive normative instruments capable of evolving alongside the technology they regulate, without sacrificing legal certainty or normative predictability. From the perspective of the knowledge society, data protection is not a bureaucratic constraint imposed on innovation, but a constitutive condition of digital trust - the fundamental resource without which the data economy cannot function sustainably. Paradoxically, robust data protection and the responsible development of AI are not competing objectives, but complementary ones: societies in which individuals trust that their data are processed lawfully and with respect for their rights are more willing to contribute to the data ecosystem that fuels AI innovation. The construction of a coherent, effective, and AI-era-adapted normative framework represents one of the fundamental missions of legal scholarship and doctrine in the knowledge society.

In conclusion, reinventing data protection in the era of artificial intelligence is not an optional or cosmetic normative project - it is an urgent necessity for safeguarding human dignity, individual autonomy, and democratic values in the face of the unprecedented processing power of artificial systems to process, interpret, and influence human behaviour at a global scale. Data protection law, alongside AI law and human rights in the digital environment, constitutes the fundamental normative stratum of the knowledge society, and its consolidation represents one of the absolute priorities of the contemporary legal agenda.

References

- Bommasani, R., Hudson, D. A., Aditi, E., Altman, R., Arora, S., Khattar, S., & Liang, P., On the opportunities and risks of foundation models, 2021.
- Bradford, A., The Brussels effect: How the European Union rules the world. Oxford University Press, 2020.
- Cao, Y., & Yang, J., Towards making systems forget with machine unlearning, Proceedings of the 2015 IEEE Symposium on Security and Privacy, 2015.
- Carlini, N., Tramer, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., & Roberts, A., Brown, T., Song, D., Erlingsson, U., Oprea, A., Raffel, C., Extracting training data from large language models, Computer Science.Cryptography and Security, 2021.
- Castells, M., The information age: Economy, society, and culture. Vol. I: The rise of the network society (2nd ed.), Wiley-Blackwell, 2010.
- Curtea de Justitie a Uniunii Europene. (2020). Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), C-311/18, ECLI:EU:C:2020:559.
- Dafoe, A, AI governance: A research agenda. Future of Humanity Institute, University of Oxford, 2018.
- Dwork, C., & Roth, A., The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3–4),2014.
- European Commission, A European strategy for data. COM(2020) 66 final, Publications Office of the European Union, 2020.
- European Data Protection Board, Guidelines 06/2022 on the interplay between the application of Article 3 and the provisions on international transfers, EDPB, 2023.
- European Parliament & Council, Regulation (EU) 2024/1689 of the European Parliament and of the Council on artificial intelligence (AI Act), Official Journal of the European Union, L, 2024.
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., & Vayena, E., AI4People — An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations, Minds and Machines, 28, 2018.
- Garante per la protezione dei dati personali, ChatGPT: Il Garante riapre il caso, il gestore di ChatGPT ha fornito risposte insoddisfacenti. Garante. https://www.garanteprivacy.it. 2023.
- Helberger, N., Doshi-Velez, F., & Naudts, L., Toothless and timid or bold and brave? The vision behind the AI Act, Algorithm Watch., 2022.
- Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F., The European Union general data protection regulation: What it is and what it means, Information & Communications Technology Law, 28(1), 2019.
- Ienca, M., & Andorno, R., Towards new human rights in the neurotechnology era: Cognitive liberty, mental privacy, mental integrity and psychological continuity. Life Sciences, Society and Policy, 13(5), 2017.
- Malgieri, G., & Comandé, G., Why a right to legibility of automated decision-making exists in the general data protection regulation, International Data Privacy Law, 7(3), 2017.

- Mantelero, A., The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten'. Computer Law & Security Review, 29(3), 2014.
- McDonald, A. M., & Cranor, L. F., The cost of reading privacy policies, Journal of Policy for the Information Society, 4(3), 2008.
- Mittelstadt, B., Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, 1(11), 2019
- OCDE. (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. https://legalinstruments.oecd.org.
- O'Neil, C., Weapons of math destruction: How big data increases inequality and threatens democracy, Crown Publishers, 2016.
- Rudin, C., Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead, Nature Machine Intelligence, 1(5), 2019.
- Solove, D. J., Introduction: Privacy self-management and the consent dilemma, Harvard Law Review, 126(7), 2013.
- Sweeney, L., Simple demographics often identify people uniquely, Carnegie Mellon University, Data Privacy Working Paper, 2000, p.10.
- Terec-Vlad, L., & Rusu, A. Neuro-Cybersecurity and the Future of Cognitive Rights: Legal Foundations for the Protection of the Human Mind in the Digital Age, Revista Romanească pentru Educație Multidimensională, 18(1),2026.
- Terec-Vlad, L., Ungureanu, C.G., The Rights of Artificial Intelligence: Between Ethics, Law and Normative Pragmatism, Revista Universul Juridic, 9, 2025.
- UNESCO. (2021). Recommendation on the ethics of artificial intelligence. SHS/BIO/PI/2021/1. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000381137 (seen at 26.04.2026)
- Veale, M., & Zuiderveen Borgesius, F., Demystifying the draft EU Artificial Intelligence Act, Computer Law Review International, 22(4), 2021.
- 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, 2019.
- Yuste, R., Goering, S., Arcas, B. A. Y., Bi, G., Carmena, J. M., Carter, A., & Wolpaw, J., Four ethical priorities for neurotechnologies and AI, Nature, 551(7679), 2021.
- Zittrain, J., IP and the future of AI: Creative attribution and compensation, Harvard Law Review Forum, 136, 2023.
- Zuboff, S., The age of surveillance capitalism: The fight for a human future at the new frontier of power, PublicAffairs,2019.