European Journal of Risk Regulation (2026), **17**, 1032–1053
doi:10.1017/err.2026.10105

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Ghost in the Shell: Inferred Groups under the AI Act and the GDPR. Concrete Solutions for System Sync

Liubomir Nikiforov

EDHEC Augmented Law Institute, IPoP, France
Email: liubomir.nikiforov@edhec.edu

Abstract

Recent advances in Artificial Intelligence (AI) reveal a mismatch between the EU's individual-centric data protection shell and automated systems' ability to affect entire groups of people, sealed within that shell. AI routinely processes data about groups, while the GDPR still allocates rights and remedies to identifiable individuals. This design produces a structural collective redress gap where injunctions may be obtained without individual mandates (GDPR Art. 80(2), RAD Art. 8), but compensation remains tied to identifiability. Here, I show how the GDPR's model (consent, data subjects' rights, Art. 80) fits in and why it fails against AI's capacity to de-anonymise and infer traits about persons whose data were never collected or volunteered. I then examine the AI Act 2024/1689. Although it repeatedly refers to "groups of persons," trilogue negotiations removed the Parliament's key collective remedy tools, leaving only *ex-ante* risk and transparency duties. The example of online behavioural advertising or affinity profiling illustrates how AI-designed groups fall outside the scope of meaningful GDPR or AI Act remedies. I argue for a right to group protection and propose four main revisions: a definition of groups, a mechanism for a group complaint and redress, group-level impact assessment requirements and group data protection by design.

Keywords: artificial intelligence act (AI Act); collective redress; group privacy; group data protection; inferred groups

I. The code of the programme

A beautiful metaphor for the lines that follow is the cyberpunk series and film, "Ghost in the Shell." Current EU data protection is the "shell" representing the individual-centric legal framework. In contrast, the "ghost" represents the inferred group data *soul* that the AI Act[1] and the GDPR[2] are struggling to rewire. This is because the dominant framework for data protection is largely individual-centric, where the General Data Protection Regulation (GDPR) focuses on safeguarding personal data at the individual level, primarily through a consent-based mechanism. While this paradigm has been in place for decades, the rapid evolution of data-driven technologies, especially Artificial Intelligence (AI), has begun to

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L 22024/1689, 12.07.2024) 2024.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119) 1.

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution-NonCommercial licence (https://creativecommons.org/licenses/by-nc/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original article is properly cited. The written permission of Cambridge University Press or the rights holder(s) must be obtained prior to any commercial use.

https://doi.org/10.1017/err.2026.10105

expose critical gaps in its protective reach. A key oversight in the current legislative architecture concerns the impact on groups of people who never consented to, nor knowingly contributed, the data that underlies automated decision-making, which may negatively affect them. Under the GDPR, personal data that is effectively anonymised is excluded from regulatory oversight, and the Regulation provides a limited legal instrument for collective redress. Yet modern AI systems can de-anonymise personal data or derive sensitive insights about entire demographics with relative ease. A paradigmatic example is the use of some service providers of "non-user's information." You may not use a service, but your personal data is still exploited as a *friendly* inference. This is how friendship requests work in practice on social media.[3]

The paper's thesis is that the GDPR's safeguards are triggered by data "relating to" an identifiable person, whereas contemporary practices can de-anonymise data or generate actionable inferences at scale that affect not only individuals but also target groups of people as such, without requiring controllers to single them out as data subjects. In that sense, the privacy harm is real, but the decisive element lies within the scope of data protection and its remedial architecture (identifiability, Articles 77–82, limits of collective standing).

This is why this paper is framed primarily in EU data protection terms because the core regulatory problem it targets is not only "privacy" in an abstract sense, but the governance of data processing and inference when datasets are treated as anonymous while still enabling personal (including sensitive) inferences about persons.

In this context, the European Union has introduced the AI Act. This new legislative tool seeks to reduce AI's risks to fundamental rights while promoting AI's beneficial uses. Among its many features, it highlights the potential relevance of "groups of persons" as subjects of rights and potential harms. Given the interconnection between the GDPR and the AI Act, the AI Regulation provides insight into the potential of collective rights in data protection. This study builds upon an earlier analysis of the draft AI Act,[4] extending that work to incorporate the final text of the legislation and situating it more firmly within existing scholarship on group privacy and data protection. This paper uses "group data protection" to describe the extension of EU data protection law's rights, obligations and remedies to groups of persons, including those constructed by AI and not individually identifiable. I reserve "group privacy" for the normative and theoretical debate that motivates such a shift.

Specifically, this paper makes two contributions. First, it identifies the need to evolve beyond a strictly individual-centric data protection framework, underscoring the unique vulnerabilities of groups, particularly when automated systems create or target them without their members' explicit awareness or permission. Second, it explores both theoretical and practical applications of such a group within existing scholarship and legislation. It reviews existing interpretations of "group privacy" in the literature. It suggests potential pathways to reinterpret existing provisions and embed group-level data protections, specifically by the AI Act and the GDPR, as a remedy before any future large-scale reform.

In this vein, there are some technical limitations to point out as well. The study is limited by the evolving nature of the legislation in question. Given that the provisions

[3] For example, see under "Information for people who don't use Meta Products" where the provider shares the collected personal data, infrastructure, systems and technology with its different platforms and retains that information "for as long as needed to provide the Contact Uploading feature to users ... including after you ask us to erase it." In <https://www.facebook.com/help/637205020878504> But also for personalisation, the same provider uses the content you create or provide through camera, metadata, etc. <https://mbasic.facebook.com/privacy/policy/printable/#2>.

[4] L Nikiforov, "Groups of Persons in the Proposed AI Act Amendments" (2024) European Journal of Risk Regulation 1 <https://doi.org/10.1017/err.2024.13>.

https://doi.org/10.1017/err.2026.10105

discussed in the text are part of the first-ever Regulation on AI, it is not surprising that there is no reference jurisprudence on which this analysis could rely. In addition, the notions of "groups of persons" or "group privacy" represent an underexplored terrain in both theory and practice, thereby demanding future research on topics beyond the scope of this analysis (e.g., the tension between group versus individual privacy, and potential negative externalities of expanding data protection to group claims).

Methodologically, I combine a literature review (doctrine and case law) with close textual analysis of the GDPR, the AI Act and the RAD, read against their historical trajectories. The paper proceeds as follows: Section 2 (The European Data Protection Individualistic Shell) provides a background on the evolution of data protection, culminating in the centrality of the GDPR, and also examines some topical critiques (through Article 80 GDPR and RAD) of the main thesis defended here. Section 3 (The Network) reframes privacy as a public good and, drawing on the group privacy literature, motivates a shift to group protection. Section 4 (Uploading to the Cloud) revisits the draft of the AI Act to show where the adopted text diverges. Section 5 (A Sealed Ghost) examines how the current AI Act treats "groups of persons." Section 6 (Hacking the Shell) uses online behavioural advertising to illustrate the loopholes that emerge from this analysis. Finally, Section 7 (Rewiring the Shell) lays out concrete recommendations, while Section 8 (System Sync) concludes.

II. The European data protection individualistic shell

In order to open the "shell" and explain this paper's emphasis on data protection, it is important to clearly distinguish it from privacy as two distinct, yet closely related rights. There has been debate over whether privacy and data protection constitute separate rights[5] and/or should be recognised as fundamental rights.[6] Whatever the scholarly discussions are, the European constitutional reality is unambiguous. Article 7 and Article 8 of the EU Charter[7] establish two fundamental rights, and this premise is fully adopted by this paper. The two rights differ primarily in their moral bases, duty bearers, scopes, and restrictions. Throughout this paper, I use privacy to mean Article 7 EU Charter and data protection to mean the distinct right under Article 8 EU Charter, operationalised primarily through the GDPR. Unless stated otherwise, the analysis proceeds in data protection terms, whereas privacy references are used only as a normative background.

Privacy is intrinsically intertwined with liberalism's core normative principle, individualism,[8] whose central claim is the individual's sovereignty over governmental

[5] A Rouvroy and Y Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy" in S Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) <https://doi.org/10.1007/978-1-4020-9498-9_2>; P De Hert and S Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action" in S Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) <https://doi.org/10.1007/978-1-4020-9498-9_1>.

[6] B Van Der Sloot, "Legal Fundamentalism: Is Data Protection Really a Fundamental Right?" in R Leenes and others (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (1st edn, Springer Cham 2017) <https://doi.org/10.1007/978-3-319-50796-5>.

[7] Charter of Fundamental Rights of the European Union 2016 [OJ C 202/389] 389.

[8] The liberal theory as formulated initially by Hobbes, Mill and Locke, advocating for a clear separation between the state and the individual, reshaped the thinking of privacy into a shield from governmental interference. This political and ethical theory, in turn, predetermined the later conceptualisation of privacy in what is celebrated in literature as the modern reading of privacy, defined as "the right to be left alone" by Warren and Brandeis in 1890 in "The Right to Privacy." There, they notice that technological development is what makes this new right so necessary in order to preserve one's own personality. With the emergence of more sophisticated technology and

https://doi.org/10.1017/err.2026.10105

interference,[9] enabling him to exercise his will freely.[10] What enables an individual to pursue freedom is his autonomy in a liberal-democratic society.[11] Thus, the "right to privacy consists essentially in the right to live one's own life with a minimum of interference,"[12] drawing a boundary between the private self and the public, the individual from society. It is not surprising that the main duty bearer is the state, which must abstain from unjustified interference and lay down the necessary positive measures in its legal order.

While privacy's moral framing may seem broad, its practical implications, compared with data protection, are narrower as interpreted by the Court of Justice of the European Union (CJEU). In Case T-194/04 Bavarian Lager, the Court explicitly stated that the scope of the right does not automatically extend to all personal data and, therefore, not all personal data falls under the notion of private life. This is not the case with data protection, where all information relating to an identifiable natural person is subject to the safeguards of the right; therefore, it encompasses virtually every kind of data falling within the definition provided in the GDPR Art. 4(1). Hence, data protection is broader in the information it covers but narrower in the persons it protects. This is why courts often do not address privacy because any assessment of interference must pass through the data protection lawfulness filter, meaning that if processing is not based on one of the legal bases set out in Article 6 GDPR, the analysis stops there and the processing is unlawful.

Despite its importance, where the analysis proceeds under the Charter, an interference with the right to respect of private life (understood as privacy, Article 7 Charter) must, where justified, satisfy the limitations clause in Article 52 (1) (legitimate aim, appropriateness, necessity and proportionality stricto sensu). The Charter provisions are addressed to the EU institutions and Member States only when they are implementing Union law (Article 51 Charter). Direct obligations of private parties are typically fulfilled through implementing secondary law, such as the GDPR, which addresses disputes at the level of lawfulness (Art. 6 GDPR).

Under the European Court of Human Rights (ECHR), the analogous review is performed under Article 8 (2) ("in accordance with the law," "legitimate aim," and "necessary in a democratic society"), typically involving contextual proportionality balancing and, importantly, systematic and temporal elements.[13]

Similar to privacy, data protection aims to introduce an equalising element by remedying power asymmetries arising from mass data processing and collection through a set of rules, grounded in principles and operationalised through tools such as consent, whose compliance is monitored by independent authorities. This architecture is anchored in the key tenet of the rule of law embodied in the principles in Article 5 GDPR, in particular, Article 5 (1)(a), lawfulness, fairness and transparency. Thus, EU data protection,

with it its new possibilities of collection and processing of data, privacy has been intrinsically linked to the liberal discourse, whose core is the individual by and for itself and where society is a sum of separate individual wills.

[9] A Roberts, "A Republican Account of the Value of Privacy" (2015) 14 European Journal of Political Theory 320 <https://doi.org/10.1177/1474885114533262>.

[10] A classic split in liberal theory between negative (right from) and positive (right to) rights.

[11] J Raz (ed), *The Morality of Freedom* (Clarendon Press 2010).

[12] Para. 16 defines privacy as living one's life with a minimum of interference and listing protected interests such as home and family life, integrity, reputation, private communications and confidential information, adding that self-"indiscreet revelations" do not grant privacy rights. In Parliamentary Assembly, "Declaration on Mass Communication Media and Human Rights, Resolution 428" 428 <https://pace.coe.int/en/files/15842/html>.

[13] J Kokott and C Sobotta, "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR" (2013) 3 International Data Privacy Law 222 <https://doi.org/10.1093/idpl/ipt017>.

https://doi.org/10.1017/err.2026.10105

and as some authors frame it, has an "essential procedural nature that makes it more objective as a right."[14]

In sum, both rights protect individuals against undue interference. Privacy should be regarded as a core right protected by a data protection filter. EU data protection exercises its filtering function through procedural rules[15] grounded in principles such as fairness, transparency, lawfulness, independent oversight, democracy, and the rule of law.

This is why this paper locates "group protection" primarily within data protection law. The problem is not *only* interference with private life but also the governance of data processing and inferences from anonymous datasets. Privacy (also, group privacy in Section 3) provides a conceptual justification, but alone it does not provide an equivalent operational toolbox for regulating large-scale processing externalities or for designing enforceable procedural safeguards. Other legal branches, such as non-discrimination, consumer and tort law, remain relevant but do not replace data protection. They offer specific answers, bound to the field's arsenal of remedies, tailored to the field's development, methods, harms and safeguards.

The following paragraphs examine specific aspects of data protection to substantiate, both theoretically and normatively, the argument that the next evolution in data protection entails a move from an individualistic approach to one that safeguards groups *as such*, and not as a bundle of individual rights or a right of organisations.[16]

This represents a potential for a shift in the current individual-centred data protection policy framework. The next paragraphs aim to expand this argument by providing an overview of the cornerstone developments that have shaped the present-day paradigm and by laying out the background for the subsequent discussion of the term "groups of persons" explored in another paper,[17] as potentially adversely affected parties by an AI system.

I identify three main factors driving the current individualistic approach to EU data protection: continuous technological evolution, led by AI; historical context; and the main law and its product, the GDPR.

1. The armour: built in the post-war for today's digital challenges

One could treat the distinction between privacy and data protection as part of a larger historical development. European data protection emerged from the post-war constitutional settlement that sought to constrain state surveillance[18] and from the

[14] See M Tzanou, "Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right" (2013) 3 International Data Privacy Law 88 <https://doi.org/10.1093/idpl/ipt004>. Importantly she adds one more, which I think is a derivative from the principle of fairness, the principle of non-discrimination, especially, in the context of profiling. Several authors note it as well. On the link fairness-discrimination in context, see G Malgieri, "The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation" *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (ACM 2020) <https://doi.org/10.1145/3351095.3372868>. on substantive fairness, see A Häuselmann and B Custers, "Substantive Fairness in the GDPR: Fairness Elements for Article 5.1a GDPR" (2024) 52 Computer Law & Security Review 105942 <https://doi.org/10.1016/j.clsr.2024.105942>.

[15] "Data protection differs from privacy by virtue of the width of its scope and of the number of individual rights it grants. It is also distinct from privacy in that it is, mostly, a tool of transparency, rather than a tool of opacity. Data protection also has a prevalently formal and procedural nature, rather than a substantive one." In LD Corte, "A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection" in D Hallinan and others (eds), *Data Protection and Privacy. Data Protection and Democracy*, vol 12 (Hart Publishing 2020).

[16] See A Westin, *Privacy and Freedom* (Ig Publishing 1967); E J Bloustein, *Individual and Group Privacy* (Routledge 1978).

[17] Nikiforov (n 4).

[18] Art. 12, UDHR (1948), establishes one of the mechanisms to protect "the inherent dignity" of people by guaranteeing the right to "arbitrary interference with his privacy, family, home or correspondence, nor to attacks

https://doi.org/10.1017/err.2026.10105

administrative possibilities opened by large-scale record-keeping,[19] while preserving persons' "inherent dignity."[20] Privacy and human-rights jurisprudence recognised that information practices can implicate private life. Still, early data protection regimes were designed to regulate the collection, storage and use of personal information by public authorities and other powerful information holders.[21]

In the late 1970s, amid rapid computerisation, European states adopted the first modern data-protection laws. A decisive development followed in 1983 with the German Federal Constitutional Court's Census judgment,[22] which framed "informational self-determination" as an autonomy interest and embedded the individual as the central point of informational control.[23] The EU translated these principles into secondary law.

Directive 95/46/EC[24] harmonised national rules and introduced consent and purpose limitation as central safeguards. The General Data Protection Regulation (GDPR) 2016/679 later modernised and strengthened that framework, making the data subject's rights directly enforceable across the Union through principles, lawfulness requirements, and accountability duties. The GDPR encapsulates Europe's data protection philosophy, emphasising citizens' rights and dignity. It prioritises individuals as the main managers of their data and rights.

Nevertheless, this individual-centric design premise is increasingly misaligned with contemporary data practices. The economic and governance significance of data now lies less in their initial collection than in their secondary uses and inferences.[25] Modern analytics can act on populations without collecting data from each member, producing

upon his honour and reputation." Also, Art. 8 ECHR (1950), although it does not reference dignity as a guiding principle for the rights it encloses, the connection with the earlier UDHR declaration is established in the text. The ECHR proclaims in Art. 8 (1) that "everyone has the right to respect for his private and family life, his home and his correspondence" in order to clarify in Art. 8 (2) that "there shall be no interference by a public authority with the exercise of this right" except after a ponderation of competing public interests and according to the law.

[19] ". . . . Data protection regimes were designed to alleviate the risks to individual self-determination that resulted from the development of information technologies." J C Buitelaar, "Privacy: Back to the Roots" (2012) 13 German Law Journal 171 <https://doi.org/10.1017/S2071832200020460>. Daniel J Solove, "The Limitations of Privacy Rights" (2022) Notre Dam Law Review <https://doi.org/10.2139/ssrn.4024790>.

[20] JQ Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 The Yale Law Journal. The tradition of dignity protected by law could be remoted even further centuries in the past, "(w)hat we see in continental law today is the result of a centuries-long, slow-maturing revolt against that style of status privilege. Over time, it has come to seem unacceptable that only certain persons should enjoy legal protections for their "dignity."

[21] In contrast to the essentially the same totalitarian ideologies of national-socialism and communism, the European legal framework stressed individual rights and liberties understood as negative rights. Negative rights or liberties could be defined as such *from* something or someone, as opposed to positive ones, which entail the right *to* do something. See I Berlin and I Harris, *Liberty: Incorporating Four Essays on Liberty* (Henry Hardy ed, Oxford University Press 2002); Roberts (n 9); P Helm, "Group Privacy in Times of Big Data. A Literature Review" (2016) 2 Digital Culture & Society 137 <https://doi.org/10.14361/dcs-2016-0209>.

[22] *Bundesverfassungsgericht (BVerfG) Urteil des Ersten Senats vom 15 Dezember 1983 (Judgement of the first senate of 15 December 1983) -1 BvR 209/83, Rn 1-215 - ECLI:DE:BVerfG:1983:rs198312151bvr020983* (Bundesverfassungsgericht); S Strömholm, "Right of Privacy and Rights of the Personality: A Comparative Survey" (Norstedts Förlag 1967).

[23] Across the continent, the notions of dignity, autonomy and the freedom to decide are practically embedded in data protection legislation. Peter Hustinx, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation" <https://www.edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en>.

[24] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281) 1995.

[25] As Solove puts it "(m)any algorithms involve finding patterns in aggregations of data about millions of people. Access, knowledge, algorithmic transparency and other rights lack much meaning for just one isolated individual. The lone individual merely seeking information about decisions affecting her and how her particular data is being used will never learn the whole story. To truly understand how these algorithms reach decisions, one must examine the data of everyone fed into the algorithm" in Solove (n 19); L Taylor, L Floridi and B Van Der Sloot

https://doi.org/10.1017/err.2026.10105

group-level predictions and effects that reach persons who never provided data or consented.[26] At the same time, techniques relied upon to neutralise the risk, such as anonymisation or differential privacy, do not reliably prevent re-identification or the extraction of meaningful inferences.[27] This mismatch frames the next subsection: the GDPR is broad in the information it covers, yet structurally narrow regarding who can trigger rights and remedies.

2. Sovereign of the GDPR: the individual in data protection

The GDPR deliberately centres the data subject as "both the object and the subject"[28] of protection. In practice, the regime is triggered by data that "relate to" an identifiable natural person and is enforced primarily through that person's rights and remedies. Doctrinally, this individual focus is built into the definition of "personal data" (Art. 4(1) GDPR) and the identifiability threshold, under which a person is not (directly or indirectly) identifiable, and in such cases, the GDPR's safeguards are not engaged. The same logic structures the rights catalogue and the remedial architecture in the Articles 77–82, which presuppose a claimant who can link themselves to a processing operation and contest its lawfulness and effects.[29] Also confirmed by the CJEU's case law.[30] A topical criticism of that conclusion involves Article 80 GDPR and the Representative Actions Directive (RAD).[31]

Article 80 GDPR allows non-profit bodies to act on behalf of data subjects, and the RAD provides collective procedures for consumer harms. But these mechanisms do not displace the identifiability premise,[32] they mainly set who litigates and which remedies are practically available.

First, Article 80 operates as a *representation* of identified or identifiable persons. Second, Article 80(2) enables mandate-free actions, but its practical function is typically to obtain injunctive relief rather than to distribute compensation to persons who cannot be identified.[33] Third, the availability and design of mandate-free collective actions remain

(eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017) <https://doi.org/10.1007/978-3-319-46608-8>.

[26] E Bougiakiotis, "The Case for Control Without Consent in Data Privacy Law" (2024) <https://doi.org/10.2139/ssrn.5019992>.

[27] A Puri, "A Theory of Group Privacy" (2020) 30 Cornell Journal of Law and Public Policy, Forthcoming 72 <https://doi.org/10.2139/ssrn.3686202>. Taylor, Floridi and Van Der Sloot (n 25). Chapter 2.

[28] More in K Nolan, "The Multi-Faceted Role of the Individual in EU Data Protection Law" <https://doi.org/10.2139/ssrn.4853540>. The individual, as object, is observed by the legislature and the courts, who adopt approaches which are said to be in their interest, and that interest comes to be identified with the normative underpinnings of EU data protection law. The individual, as subject, is engaged directly through data protection law as an actor. They are subjectified, as a participant in a new order of relationships, a rights-holder and a protected data subject in relation to the regulated data controller, as well as deputised as an agent in the enforcement of data protection law itself."

[29] For example, any collective action strategy that seeks damages for large-scale behavioural advertising must still satisfy the identifiability and mandate requirements linked to consent, a structural hurdle revisited further. In *Judgement of 04 July 2023, Meta Platforms Inc v Bundeskartellamt, C-252/21* [2023] CJEU ECLI:EU:C:2023:537. Paras. 91–112.

[30] Nolan (n 28).

[31] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409/1).

[32] Data protection or consumer organisation can, of course, initiate an injunction process, however, as analysed further, individual involvement for redress actions is obligatory.

[33] This provision is intended to act as a venue to address undue data processing liable to *affect rights*, rather than attribute compensation or liability. Recital 147 GDPR, an organisation may lodge a complaint and seek judicial remedy, but that body cannot seek compensation "on a data subject's behalf independently of the data subject's mandate". Also, Art. 80 (2) omits Art. 82 on compensations in order to prevent "commercial claims culture in the

https://doi.org/10.1017/err.2026.10105

highly dependent on national procedural and consumer-law choices, which tends to reintroduce an identification requirement once monetary redress is sought. Therefore, it could be concluded that para. 2 of Article 80 is rather an exception, "an option,"[34] which should be implemented by national governments according to their legislation,[35] rather than a feature of the legislative architecture underlining the data protection legislation, in particular, the GDPR.

The RAD makes this split explicit. Article 8 RAD involves measures to stop or prohibit infringing activity, with no consumer mandate under Article 8 (3). Redress measures under Article 9, like compensation, require consumers to identify (Article 9 (2)). Both injunctions and mass claims against GDPR infringements can be pursued under Article 2(1) and Annex I RAD.

However, given that GDPR would take precedence in data protection matters, redress without a mandate, ergo, without identification, would be unlawful because it would contradict the legislators' intention with Article 80 (2) where pursuing compensation under Article 82 GDPR without the express mandate of the damaged is prohibited with the intention to prevent frivolous claims driven by pecuniary incentives.[36] The practical consequence is that stopping an infringement can therefore benefit everyone exposed to a practice, including those who are "anonymous" to the defendant in practice. Compensation, by contrast, is confined to those who can be singled out as beneficiaries. This is why generally Member States permit mandate-free (GDPR) mass claims but confine them to injunctions. When compensation is sought, the national provisions require an opt-in mechanism, i.e., a mandate or a court-approved beneficiary list.[37]

Across Article 80 GDPR, the RAD, and broader remedies, a gap may leave affected members of inferred groups uncompensated even if an illegal practice is proven and stopped. The group privacy literature explains why harms occur at the group level, even when individual rights and remedies are the default.

In this context, it is worth situating the following paragraphs within the broader scholarly debate on groups in privacy and data protection. The next Section explains the "network" around and why the individual focus creates public-good externalities in an AI age and clarifies what kinds of "groups" any collective remedy must cover.

field of data protection", G Potjewijd and others, "Mass Damage Claims for GDPR Infringements: A Multi-Jurisdictional Perspective" (2021) D Hollander.

[34] Ibid.

[35] "... although the GDPR is a regulation intended to fully harmonise the rules applicable to the processing of personal data in the EU, Article 80(2) of the GDPR constitutes a so-called "*opening clause*". Florence D'Ath, "Meta v. BVV: The CJEU Clarifies the Scope of the Representative Action Mechanism of Article 80(2) GDPR Whereby Not-for-Profit Associations Can Bring Judicial Proceedings Against a Controller or Processor" (2022) 8 European Data Protection Law Review 320 <https://doi.org/10.21552/edpl/2022/2/21>. It goes out of the scope of this paper to provide more details, given the divergent national legislation. See, Peter Rott and others, "Comparative Legal Study on Procedural Rules and Their Impact on Collective Redress Actions in Europe" <https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-026_Study_Procedural_Rules_Impact_on_Collective_Redress_in_EU.pdf>; A Biard-Denieul, "Thunder Road: The Implementation of the Representative Actions Directive in Europe" (2024) 38 Emory International Law Review.

[36] The CJEU did not expand the provision; it simply established that Art. 80 (2) "does not preclude" national law from allowing mandate-free actions for non-compensatory relief. *Judgment of 28 April 2022, Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbunde - Verbraucherzentrale Bundesverband eV (META v BVV) C-319/20, ECLI: EU:C:2022:322.*

[37] For example, https://www.wolftheiss.com/insights/collective-redress-in-cee-see/#Bulgaria, p. 3, https://www.collectiveredress.org/documents/13_france_report.pdf, p. 6, https://www.collectiveredress.org/documents/31_the_netherlands_report.pdf, p. 6, https://www.collectiveredress.org/documents/28_spain_report.pdf, p. 8, https://www.wolftheiss.com/insights/collective-redress-in-cee-see/#Romania, p. 3.

https://doi.org/10.1017/err.2026.10105

III. The network: privacy as a public good and data protection's structural dimension

Since the inception of the European data protection framework, the focus has been on "the information regarding individuals, without distinguishing between their public and private nature."[38] In recent decades, some authors have restated the importance of privacy as a public good as well. I therefore treat privacy as a public good whose under-provision justifies group-level legal guarantees.

On privacy, Regan sustains that it functions simultaneously as a common, public and collective value,[39] one that individuals share, democracies need[40] and markets undersupply[41] of value shared by everyone. On a similar note, Fairfield and Engel argue that privacy has public-good aspects and thus externalities that spread across society and individuals, even though they may have put in place the highest levels of privacy protection.[42] Thus, the authors argue that privacy as a public good is poised to be what economists call a *tragedy of the commons* and invoke the environmental analogy.[43] This is because sharing private data yields an immediate benefit that outweighs the long-term risks or externalities (the so-called discounting effect in economics). In a world of AI, big data can infer correlations from seemingly unrelated data points that could adversely affect unaware and unidentifiable individuals whose data has never been collected.[44] This is precisely the gap this paper evidences: the traditional (individualistic) approach is insufficient, as individuals cannot properly protect themselves given the amount of information provided by third parties.[45] This is better exemplified by the example of

[38] A Mantelero, "The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics" (2014) 30 Computer Law & Security Review 643 <https://doi.org/10.1016/j.clsr.2014.09.004>.

[39] Privacy as a common value could be evidenced by the "behaviour and actions of individuals with respect to social networking sites and national security, which she deems "provide empirical support that privacy is viewed in common terms and as similarly important." In PM Regan, "Privacy and the Common Good: Revisited" in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (1st edn, Cambridge University Press 2015).

[40] " . . . the most telling evidence for the public value of privacy can be found in how candidates, political parties and interest groups are collecting, analyzing and using personal information to foster the polarization and partisanship," ibid.

[41] This is so because, first, it could not be effectively privatised; second, the market cannot provide an optimal supply thereof and finally, in today's interconnectedness it is difficult to "divide privacy." Those arguments lead to the conclusion that personal information can be regarded as a common pool resource which can be *overloaded*, driving protection costs up and *polluted* by "incorrect, irrelevant and out-of-date information," finally contributing to a state where "the volunteered information of the few can unlock the same information about the many," ibid.

[42] J Fairfield and C Engel, "Privacy as a Public Good" in R A Miller (ed), *Privacy and Power* (1st edn, Cambridge University Press 2017) <https://doi.org/10.1017/CBO9781316658888.004>.

[43] Individuals behave in a way which suits their own interests, even if that would be detrimental to both society and themselves as part of it. The typical example of overgrazing is given in G Hardin, "The Tragedy of the Commons: The Population Problem Has No Technical Solution; It Requires a Fundamental Extension in Morality." (1968) 162 Science 1243 <https://doi.org/10.1126/science.162.3859.1243>.

[44] A relevant example the authors put is the targeted advertising, where the contribution of Person A impacts A in a way he does not suspects but also Person B because "(e)ven by revealing personal interests and disinterests, users train machine-learning algorithms to predict the behavior of other people, forming the basis for targeted behavioral advertising, and creating the potential for abuse by other interested actors."

[45] The authors consider, however, that the *tragedy* need not happen if "group rules or structural conditions (called 'institutions')" are put in place in order to foster "group-empowering institutions that enable sustained cooperation" through tools such as group communication, sanction, and fostering a sense of repeat play and community.

https://doi.org/10.1017/err.2026.10105

someone who understands the significance of sharing a group picture for the people in the picture, but it is much more difficult to grasp the *spill* effect for third parties.

On data protection, Ben-Shahar draws a similar parallel between environmental damage, oil spills, data *pollution* and data *spills*, acknowledging the negative societal effect of data breaches but from the perspective of data protection. He ultimately calls for "an environmental law for data protection."[46] The "structural dimension" of data protection is extensively examined by Felix Bieker and helps explain this structural insufficiency.

In line with the author's thesis, the notion of data protection has two dimensions. On the one hand, it is the protection of "individuals and (minority) groups ... *from* the processing of data by means of individual rights and structural guarantees." On the other, the "structural" protection, which covers "systemic aspects of data protection such as institutional guarantees and organisational requirements."[47] This means according to the author that data protection has two faces, one protects individuals (and groups) through specific rights, while the other regulates the rules and requirements, the State or corporate entities should abide irrespective of whether an individual is concerned and by this preventing any adverse effects on society. This, in turn, again, benefits individuals and *groups* in society. As defended throughout those paragraphs, Bieker acknowledges that specific groups of people (e.g., minorities), "even though there is no information on one specific individual," are not protected sufficiently, if at all, despite the technological capacity to affect them adversely. This stance[48] overlaps with and confirms Malgieri's findings regarding the incomplete protection of vulnerable data subjects (and groups).[49] This is why Bieker concludes that full protection, especially with regard to profiling intended to predict behaviour, "the personal scope of the right (data protection), de lege ferenda, must be extended in order to enable groups of individuals to enforce this right collectively."

Together, these insights reveal the core flaw of the EU data protection framework: systemic data protection harms are like pollution, widespread, collectively borne, and impossible for any individual data subject to avoid. To address these externalities, the law needs a clear explanation of what types of "groups" justify collective protection.

To begin answering this question, the most comprehensive anthology of perspectives on the types of groups is the book edited by Taylor, Floridi, and van der Sloot, where they ask, "whether, and how, we may be able to move from 'their' to 'its' privacy with regard to the group" in the context of data processing practices such as profiling.[50]

Some authors refer to *self-proclaimed* and *framed* groups. Framed groups are formed voluntarily or through individual will, while self-proclaimed groups are not. Most authors describe them as designed or discovered, meaning they are identified during data processing or analytical processes based on specific datasets. The authors state most groups are "enforced," thus designed or discovered.

Closely related is the distinction between *self-aware* and *unaware* groups. Self-aware groups include professional groups, unions or interest groups formed purposefully. Not-self-aware groups comprise individuals who share genetic features and are unable to foresee the implications of analysing their genetic code, either as a group or individually. This is because genetic information identifies the group and makes each member identifiable.

A genetic code is a stable feature, which is why some focus on distinguishing *stable* and *fluid* groups. Stability comes from awareness and will to belong. However, in data

[46] O Ben-Shahar, "Data Pollution" (2019) 11 Journal of Legal Analysis <https://doi.org/10.1093/jla/laz005>.

[47] F Bieker, *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law*, vol 34 (TMC Asser Press 2022) <https://doi.org/10.1007/978-94-6265-503-4>.

[48] "... there currently is a gap in protection, especially with regard to groups who are already vulnerable." Ibid.

[49] Also discussed further in Gianclaudio Malgieri, *Vulnerability and Data Protection Law* (First edition, Oxford University Press 2023).

[50] Taylor, Floridi and Van Der Sloot (n 25).

https://doi.org/10.1017/err.2026.10105

processing, group criteria may change quickly. For example, a person going to the gym wants to be a member, but using different transport modes each day momentarily clusters him with other passengers, some regulars, some tourists. While he is aware and willing to be grouped with gym peers, he probably would not see himself as part of a short-term fluid group travelling together.

Another distinction is made based on a group's *hierarchical* or *egalitarian* structures. Legally recognised persons such as supervisors or legal representatives have a hierarchical nature, enabling them to defend collective interests before authorities, especially minority or lobbying interests. Such groups are often law-recognised due to their stability and self-proclaimed status. In contrast, horizontal groups lack legal recognition; each member must claim liability individually, even when harmed as part of a group, exemplified by LGBTQ + rights.

Finally, Floridi notes that traditionally, the distinction is made between real and fictional groups. However, he contends that groups are neither discovered nor invented but are intentionally designed. The legitimacy of these groups depends on the justification for choosing a specific level of abstraction (LoA). He claims that a group's "naturalness" merely reflects how intuitive that level is. According to him, groups exist in relation to a justified purpose (epistemological rather than ontological) and insists that the "naturalness" of a grouping depends on the context. Therefore, the key point is not whether groups are separate entities, but which particular lenses are used to perceive them. Additionally, Floridi argues that designed groups should have rights as groups, not just as the sum of their individual members. I use this to support the view that legal protection should not depend on a group's "naturalness," allowing AI-designed groups to challenge processing and seek collective redress.

The AI Act is the most prominent legislative act, containing a direct and explicit reference to "groups of persons." The following Sections analyse relevant provisions to examine how the concept of "groups," evolved since the law's proposal, how it fails *upload to the legislative cloud redress*, and how it has been *coded* into this context so to develop specific suggestions for enhancement at the end, freeing the *ghost.*

IV. Uploading to the cloud: AI groups of persons. From ambition to compromise

A brief look back at the European Parliament's draft AI Act[51] serves functional purposes. First, it reveals which tools (definition of "group," internal complaint procedures, group standing to lodge complaints) were available but finally discarded, thereby illuminating the precise gap the final Act leaves open. Second, the draft text supplies ready-made language that could be revived in the mandatory 2028 review (Article 112 AI Act), showing that stronger group protection is politically and legally feasible.

1. Groups of persons in the proposed AI Act

The EP's amendments deliberately introduced the notion of "groups of persons" in core definitional, transparency and redress provisions. This is reflected in multiple mentions of *groups* throughout the text. For example, the definitions of "significant risk,"[52] "affected

[51] European Parliament, "Amendments Adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))" <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html>.

[52] Amendment 167 to Art. 3, paragraph 1, point 1b (new) "the ability to affect an individual, a plurality of persons or to affect a particular group of persons."

https://doi.org/10.1017/err.2026.10105

person"[53] and "emotion recognition"[54] explicitly refer to the impact of AI on groups. The references to "groups" could be clustered into three main axes: potential discrimination against groups,[55] collective transparency and public trust through accuracy and impact assessments[56] and robust redress mechanisms via internal complaint procedures and a right to lodge group complaints.[57]

Despite that, the draft left open several issues inherent to that introduction, such as what counts as "group" or "groups of persons," whether providers can feasibly describe the system's logic for each affected cohort,[58] and which groups would meet admissibility thresholds for lodging complaints.

2. *The divergence in the final AI Act, and why it matters*

The Artificial Intelligence Act was finally adopted on 13 June 2024. The adopted Act preserves the draft's anti-discrimination approach but removes every binding redress device.[59]

The adopted AI Act retains several core provisions from the draft aimed at preventing discriminatory AI outcomes.[60] It upholds prohibitions on systems that distort human behaviour or exploit vulnerabilities, particularly regarding age, disability or socioeconomic status.[61] Recitals 57 and 58 and Annex IV preserve the draft's

[53] Amendment 174 to Art. 3, paragraph 1, point 8a (new) "means any natural person or group of persons who are subject to or otherwise affected by an AI system."

[54] Amendment 191 to Art. 3, paragraph 1, point 34 "means an AI system for the purpose of identifying or inferring emotions, thoughts, states of mind or intentions of individuals or groups on the basis of their biometric and biometric-based data."

[55] Amendment 78, Recital 44, and on discrimination ensuing from several technological and social contexts, where AI's development and learning stages, based predominantly on past historical data and records, play a crucial role, already pointed out in policy documents and literature: "Ethics Guidelines for Trustworthy AI" (High-Level Expert Group on AI (AI HLEG) 2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>; JJ Suh and others, "Distinguishing Group Privacy From Personal Privacy: The Effect of Group Inference Technologies on Privacy Perceptions and Behaviors" (2018) 2 Proceedings of the ACM on Human-Computer Interaction 1 <https://doi.org/10.1145/3274437>.

[56] The amendments focus on accuracy, risk assessment and transparency, introducing a collective dimension to these principles found in Art. 5 GDPR. Also, Amendment 413 proposes a new Article 29a, which introduces a requirement for a fundamental rights impact assessment for high-risk AI systems, addressing the potential harms likely to affect groups of people, particularly marginalised or vulnerable communities.

[57] Amendment 133, Recital 84a (new) urges AI system deployers to establish internal complaints mechanisms that can be used by individuals, legal entities or groups of individuals, Art. 68a grants individuals and groups of natural persons the right to lodge a formal complaint with the relevant national authority.

[58] Amendment 752 to Annex IV, paragraph 1, point 2, point b.

[59] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L 22024/1689, 12.07.2024) (n 1).

[60] Both versions emphasise the protection of human dignity and autonomy from AI's adverse effects Recital 27 refers to the AI HLEG guidelines, underscoring the connection between human dignity and personal autonomy, ensured by human oversight besides any other foreseen safeguards. More in Amendments, 37, 39, 40, 50, 56, 88, 213 and Recitals 27, 28, 31, 48, 58, 80 AI Act.

[61] Recital 29 prohibits AI systems capable of distorting human behaviour and capable of causing "significant harm to that or another person or groups of persons, including harms that may be accumulated over time". Art. 5 (1)(a) prohibits AI systems that manipulate "a person or *group of persons*"' behaviour and adds immediately after, in Art. 5 (1)(b) that systems exploiting "any of the vulnerabilities of a natural person or a *specific group of persons* due to their age, disability or a specific social or economic situation" and thus causing them harm, are prohibited. In law enforcement contexts, Recital 59 and Art. 5(1)(d) recognise the power imbalance between public bodies and individuals, requiring human oversight to mitigate risks of biased or arbitrary decisions.

https://doi.org/10.1017/err.2026.10105

transparency[62] commitment by requiring systems' instructions[63] to disclose performance accuracy[64] broken down by the persons or groups to which the AI would be applied,[65] yet the draft's stronger clause mandating group's participation in impact assessments (Article 27 (c)(d)) was moved to recitals.

Interestingly enough, where the EP draft established that human oversight should be ensured "where decisions based solely on automated processing … produce legal or otherwise significant effects on the persons or *groups of persons* on which the system is to be used,"[66] this is missing in the adopted version.

Thus, the adopted version of the AI Act follows closely the EP's proposal in the provisions acknowledging the role of AI in multiple aspects of life as well as the responsibility of third parties along the deployment chain. Nevertheless, this attestation, along with additional industry obligations, does not amount to an effective protection as much as a proper redress mechanism in case of a tort.

Crucially, however, the categorisation of provisions referring to "groups" has been modified[67] so that the recognition of the potential negative impact of AI practice on collective entities remains, while the redress mechanisms are entirely withdrawn.

Besides the Recital 96 AI Act, which recommends that deployers set up "complaint handling and redress procedures," there is no compulsory provision which operationalises complaint mechanisms as suggested in the draft. In reality, the right to lodge a complaint (Article 85 AI Act) is limited to a public authority and to the individual in question. Therefore, the wording in Amendment 628 that "every natural persons or groups of natural persons shall have the right to lodge a complaint with a national supervisory authority" has been eliminated. This deletion re-creates the exact structural gap identified previously, namely, the law acknowledges collective risk but denies collective standing and compensation.

In sum, the term "groups" has been finally introduced, and some inconsistencies have been purged.[68] The concerns related to the definition of "groups of persons," the system's description requirements, and, most importantly, the mechanism for redress in the AI Act were largely left unresolved, and, with this, the structural gap highlighted above. Injunction-level protection survives, but collective redress has been written out. How those provisions would work is a question of time and jurisprudence, however, because the Parliament's language shows that stronger protection was once regarded as feasible, those discarded clauses provide a ready blueprint for the first revision cycle mandated by Article 112 AI Act.

[62] Deployers should be provided with enough information pursuant to Art. 13 AI Act, besides the technical requirements mentioned in Art. 15 AI Act. The technical information required for the placement on the market of a high-risk AI includes "the general logic of the AI system and of the algorithms; the key design choices including the rationale and assumptions made, including with regard to persons or groups of persons in respect of who, the system is intended to be used" as well as the "capabilities and limitations in performance, including the degrees of accuracy for specific persons or groups", pursuant to Annex IV, para. 2, point 2, point b and para. 3.

[63] Art. 13 (3)(b)(ii) and (iii) AI Act, the instruction for the use should include the level of accuracy and the factors, which may challenge the correct output, apart from the performance related to groups of persons on which the system would be used.

[64] While the GDPR refers to data being up-to-date and accurately reflecting users' characteristics (Art. 5(d)), the AI Act define accuracy in terms of a system producing correct and reliable outputs.

[65] E.g., against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. While Art. 5(1)(f) prohibits emotions' analysis in these contexts, AI-based evaluation or recruitment is still permitted as "high-risk" (Annex III).

[66] Amendment 315.

[67] The AI Act not only eliminates the mentions to groups in the taxonomy of the Regulation but drops out entirely the definitions of "significant risk," "affected person" and "emotion recognition."

[68] In the draft was included the term "plurality of persons", which the final version eliminated.

https://doi.org/10.1017/err.2026.10105

V. A sealed ghost: groups in the AI Act

Groups of potentially affected people are expressly protected under Article 5 AI Act. AI systems manipulating human behaviour "by appreciably impairing their ability to make an informed decision" or by exploiting "any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation" are banned (Article 5 (1)(a) and (b)). In addition, systems, which perform evaluation or classification of "persons or groups of persons" based on their "behaviour or known, inferred or predicted personal or personality characteristics," leading to a detrimental and/or unjustified outcome in other social contexts than those for which the data was collected, are prohibited as well (Article 5 (c)). While the Regulation prohibits emotional analysis in educational or workplace contexts,[69] it allows certain AI-driven evaluations (e.g., recruitment) under a high-risk label.[70] Recitals 56 and 57 elucidate the rationale behind by both referring to concerns related to historical discriminatory patterns to "women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation." This is why high-risk AI is subject to stricter rules in order to ensure accountability, transparency and ultimately trust in users.

Furthermore, to achieve better protection in line with the previous, Article 9 (9) foresees a risk management system, which takes into account the "adverse impact on persons under the age of 18 and, as appropriate, other vulnerable groups." Recital 67 establishes that data sets should include statistical properties having into account a group dimension "in particular for persons belonging to certain vulnerable groups, including racial or ethnic groups." This requirement is reflected in Article 10 (3). As already mentioned, transparency is at the core of the Regulation. Hence, Article 13 (3)(b)(v) mandates that the instructions for use should include the performance concerning "specific persons or groups of persons on which the system is intended to be used." Article 27 establishes the requirements for the fundamental rights impact assessment for high-risk AI systems whose scope should include an evaluation of the consequences for groups. In that sense Recital 96 mandates that the objective is for the deployer "to identify the specific risks to the rights of individuals or groups of individuals." This practically means that those collective entities should be identifiable *ex-ante* and hence stable and predictable. In similar vein, go other transparency provisions.[71] The groups referred to in the Annexes, in particular, when it comes to law enforcement (Annex III (6)(d)), the logic of the AI included in the technical requirements (Annex IV (2)(b)), or the functioning of the system (Annex IV (3)). The provisions adopted by the AI Act have their critics, however, who consider them inadequate, ambiguous or even additionally harmful.[72]

It is apparent from the wording of the Articles and their corresponding Recitals mentioned here as well as those referring to discrimination throughout the Regulation, and in general, the adverse effects of AI practices that the lawmaker has specific and identifiable groups in mind. This conclusion is supported by the explicit wording of the provisions, which describe *specific, identifiable and stable* groups as well as *legally recognised* ones, following the taxonomy overviewed in Section 3. Also, multiple Recitals make express reference to age, gender and race as well as to religious, ethnic and sexual minorities.[73] All of these point out

[69] Art. 5 (1)(f) AI Act.

[70] Annex III points 3 and 4.

[71] Art. 60 (4)(g), "persons belonging to vulnerable groups due to their age or disability", Art. 90 (e) "groups of vulnerable persons, including as regards accessibility for persons with a disability, as well as on gender equality."

[72] S Wachter, "Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond" (2024) SSRN Electronic Journal <https://doi.org/10.2139/ssrn.4924553>.

[73] Recitals 29, 31, 56–9, 67.

https://doi.org/10.1017/err.2026.10105

to groups, which are identifiable, stable and even legally recognised. For the sake of this recognition, it does not matter if they are aware or not of their grouping.

Interestingly enough, the Regulation insists also on *vulnerability* as a ground for data subject's (also, groups') protection. Although, as established elsewhere, European data protection legislation does not have a coherently developed notion of "vulnerability," specific conditions or characteristics of individuals or groups make them particularly susceptible to exploitation, harm, or manipulation by AI systems because they may struggle to make informed decisions or protect their interests.[74] Thus, vulnerability is associated with dependency, weakness or being affected disproportionately from external factors, which is often perceived as deserving specifically targeted protection. Examples of vulnerable data subjects are minorities, socially or economically disadvantage people. Safeguards related to those communities are scattered in sectoral regulations.[75] Take for example asylum seekers and refugees, already labelled as vulnerable groups.[76] In this specific context of vulnerability, throughout the years, the European Data Protection Supervisor puts forward group-based arguments in order to halt data processing of "particularly vulnerable groups (e.g., asylum seekers and refugees)," which may be considered lawful but potentially exposing to risk "a group, as group ... in a way that cannot be covered by ensuring each member's control over their individual data."[77] Another paradigmatic example of vulnerable groups are minors recognised as such vulnerable group in several acts.[78]

While the exploration and analysis of the issues around vulnerable subjects go beyond this research, the term fits the concept of groups as meant in the Regulation. This is groups of persons who, by virtue of their age, condition or legal status, find themselves particularly susceptible to AI's adverse effects. When reviewing Bieker's taxonomy of data protection dimensions it has been divided in individual and structural, where the former, despite focused on single persons includes groups exemplified by minorities. Therefore, although the AI Act acknowledges that personal data may be used to harm groups, it does not go beyond the already established individual data processing dimension. Because neither Article 85 AI Act nor the GDPR's Article 80(2) regime supplies a mandate-free, compensatory remedy, the RAD remains the only (partial) venue for group redress, yet even this Directive requires identifiability (Art. 9(2) RAD), leaving anonymous and affected groups rightless.

In conclusion, the AI Act falls short of freeing the *sealed ghost*. *Other groups,* emerging from AI processing, namely, fluid, designed, unaware and/or unstable groups remain unaddressed. In order to translate this concern into practical terms, the next Section examines those challenges through the lenses of the particular, yet revealing, example of online behavioural targeting for advertising.

[74] Malgieri (n 49).

[75] Ibid.

[76] EDPS, "Opinion 02/2016 EDPS' Recommendations on the Proposed European Border and Coast Guard Regulation" <https://www.edps.europa.eu/sites/default/files/publication/16-03-18_ebcg_en.pdf>.

[77] EDPS, "Formal Consultation on EASO's Social Media Monitoring Reports (Case 2018-1083)" <https://www.edps.europa.eu/sites/default/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf>, p. 8, and EDPS, "Report on Audit Pursuant to Articles 57 (1)(a) and (f), 58 (1)(b) of Regulation (EU) 2018/1725 (Case Reference 2022-0749)" <https://www.edps.europa.eu/system/files_en?file=2024-04/405_2023-0605_001_redacted_conf.pdf>.

[78] In particular, when it comes to profiling and advertising, for example, Recitals 62, 94, 95, 104, Arts. 28, 25, 44 Regulation (EU) 2022/2065 of the European Parliament and the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) 2022 [OJ L 277/1] 3., and Recitals 38, 75 GDPR.

https://doi.org/10.1017/err.2026.10105

VI. Hacking the shell: the *unprotected* groups in profiling and online behavioural advertising

A defence and justification for a sui generis right of groups is made elsewhere,[79] and empirically.[80] This Section continues the discussion by extending and developing the arguments made earlier by evidencing where the *system is hacked* and where a shift towards group data protection, with the challenges online behavioural advertising (OBA) poses to "non-traditional groups" is needed.

OBA operationalises exactly the gap identified above. Platforms and ad-tech providers create and act upon AI-designed groups that are neither self-aware nor readily identifiable. Injunctions can stop the practice for everyone, but compensation remains unreachable for those cohorts because neither the GDPR nor the AI Act gives them collective standing.

OBA is the most widely used marketing strategy, enabling marketers and advertisers to target individuals or specific consumer groups differently.[81] It raises concerns about data protection, transparency, and societal impact.[82] While businesses and consumers benefit from targeted content,[83] risks include opacity in data collection, discrimination and adverse profiling.[84] Unlike general online personalisation, which includes both tailored pricing and advertising, OBA specifically profiles users based on their browsing behaviour and *assumed affinities*.[85] Users may voluntarily provide personal data (e.g., social media activity or consent), but much data is inferred through browsing history, location tracking, and predictive analytics.[86] Often, this information is shared with third parties through mergers or data sales, making its scope "virtually infinite."[87] Personal data collection, however, is the first step in profiling consumers. The next one is the anonymisation of the data. It has been proven that anonymised data could be de-anonymised and re-assigned with minimal input by AI.[88] Yet, there is no need to carry out complex procedures to signal

[79] L Floridi, "Group Privacy: A Defence and an Interpretation" in L Taylor, L Floridi and B van der Sloot (eds), *Group Privacy* (Springer International Publishing 2017) <https://doi.org/10.1007/978-3-319-46608-8_5>.

[80] A Majeed, S Khan and SO Hwang, "Group Privacy: An Underrated but Worth Studying Research Problem in the Era of Artificial Intelligence and Big Data" (2022) 11 Electronics 1449 <https://doi.org/10.3390/electronics11091449>.

[81] IPSOS, London Economics and Deloite consortium, "Consumer Market Study on Online Market Segmentation through Personalised Pricing/Offers in the European Union" <https://commission.europa.eu/publications/consumer-market-study-online-market-segmentation-through-personalised-pricingoffers-european-union_en#:~:text=The%20aim%20of%20this%20study%20was%20to%20explore%20the%20nature>.

[82] EDPB, "Guidelines 8/2020 on the Targeting of Social Media Users, Version 2.0" <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en>; W Wiewiórowski, "It Is Time to Target Online Advertising" (14 March 2022) <https://www.edps.europa.eu/press-publications/press-news/blog/it-time-target-online-advertising_en>; C Armitage and others, "Towards a More Transparent, Balanced and Sustainable Digital Advertising Ecosystem: Study on the Impact of Recent Developments in Digital Advertising on Privacy, Publishers and Advertisers Final Report" (2023) <https://op.europa.eu/nl/publication-detail/-/publication/8b950a43-a141-11ed-b508-01aa75ed71a1/language-en>.

[83] IPSOS, London Economics and Deloite consortium (n 81); S Aiolfi, S Bellini and D Pellegrini, "Data-Driven Digital Advertising: Benefits and Risks of Online Behavioral Advertising" (2021) 49 International Journal of Retail & Distribution Management 1089 <https://doi.org/10.1108/IJRDM-10-2020-0410>.

[84] Article 29 Data Protection Working Party, "Opinion 2/2010 on Online Behavioural Advertising" <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf>.

[85] P Rott, J Strycharz and F Alleweldt, "Personalised Pricing" <https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)734008>; IPSOS, London Economics and Deloite consortium (n 81); Zihao Li, "Affinity-Based Algorithmic Pricing: A Dilemma for EU Data Protection Law" (2022) 46 Computer Law & Security Review 105705 <https://doi.org/10.1016/j.clsr.2022.105705>.

[86] The most traditional technology behind OBA consists of placing tracking text files, also commonly known as "cookies," in user's device or browser. Article 29 Data Protection Working Party (n 84). IPSOS, London Economics and Deloite consortium (n 81).

[87] IPSOS, London Economics and Deloite consortium (n 81).

[88] "an adversary who knows only a little bit about an individual subscriber can easily identify this subscriber's record in the dataset ... we successfully identified the Netflix records of known users, uncovering their apparent

https://doi.org/10.1017/err.2026.10105

out someone, as profiling can occur without any individual identification.[89] When it comes to group's profiling, AI systems can evaluate *other* data such as third parties' data or data that does not fall within the scope of the GDPR in order to identify and target successfully groups of seemingly unrelated data subjects.

OBA's profiling practically bypasses and undermines the available data protection guarantees. This means that individuals lack effective data protection because the anonymisation techniques used in online behavioural targeting are not covered by the GDPR.[90] Even the elevated requirements in Article 9 concerning sensitive data fall short as they fail to "acknowledge a potential relationship between assumed interests and sensitive personal traits."[91] Moreover, the rights enshrined in Articles 15–22 GDPR do not apply in those cases where, after retrieving personal information, it has been anonymised.[92] In addition, all those rights are invoked solely by data subjects, and only when they establish a credible suspicion that they have been victims of some tort or discrimination. But even then, they would need to figure out a way to prove that they have been treated adversely *compared* to some others.[93] This is particularly dangerous when it comes to data collection and processing, which could be fed with diverse and unlimited sources of information, in order not only to infer opinions and tastes and profile users but also to induce a particular behaviour. Although the AI Act forbids AI uses which manipulate human behaviour, it does not backlist OBA technology.

Sandra Wachter explores how affinity profiling[94] turns out to challenge citizens' privacy and data protection rights, discriminates against marginalised groups, and most importantly, affects adversely "non-traditional groups."[95] OBA's affinity profiling is defined as a technique which infers *indirectly* users' or groups' assumed interests. By presenting two cases,[96] the author evidences that a potentially affected person need not to be part for a disadvantaged group or have any relationship with a protected group in order to suffer adverse treatment or discrimination (e.g., the content shown in advertisements or the services they are provided as it is in the *CHEZ* judgement). Even with the broadest interpretation of data protection law, its framework fails to protect "new types of groups created through inferential analytics that do not map onto historically protected attributes."[97]

political preferences and other potentially sensitive information." Arvind Narayanan and Vitaly Shmatikov, "Robust De-Anonymization of Large Sparse Datasets" *2008 IEEE Symposium on Security and Privacy (sp 2008)* (IEEE 2008) <https://doi.org/10.1109/SP.2008.33>.

[89] B Mittelstadt, "From Individual to Group Privacy in Big Data Analytics" (2017) 30 Philosophy & Technology 475 <https://doi.org/10.1007/s13347-017-0253-7>.

[90] Li (n 85).

[91] S Wachter, "Affinity Profiling and Discrimination by Association in Online Behavioral Advertising" (2020) 35 Berkley Technology Law Journal 367 <https://doi.org/10.15779/Z38JS9H82M>.

[92] W Schreurs and others, "Cogitas, Ergo Sum. The Role of Data Protection Law and Non-Discrimination Law in Group Profiling in the Private Sector" in M Hildebrandt and S Gutwirth (eds), *Profiling the European Citizen* (Springer Netherlands 2008) <https://doi.org/10.1007/978-1-4020-6914-7_13>. Interestingly enough, the authors point out to the same problem referring to the framework of the repealed Directive 95/46/EC, which leads to the conclusion that while technology evolves, legal instruments stay the same and known challenges grow.

[93] Wachter (n 91).

[94] Affinity here means the assumed interests of a consumer. For example, if a person listens to Bulgarian folk music, that person may be assumed to have *affinity* to Bulgarian culture, history, cuisine, etc. This decision is based not on any protected groups (in anti-discrimination law or data protection) but on the statistical correlation that users who like particular music would like particular food, culture, etc. This may seem trivial but has significant impact when it comes to establishing a correlation between certain groups in society and the assumed preferences they may demonstrate, which may lead to adverse treatment.

[95] Wachter (n 91).

[96] *Judgement of 17 July 2008, S Coleman v Attridge Law and Steve Law, C-303/06, ECLI:EU:C:2008:415*; *Judgment of 16 July 2015, 'CHEZ Razpredelenie Bulgaria' AD v Komisia za zashtita ot diskriminatsia, C-83/14, ECLI:EU:C:2015:480*.

[97] Wachter (n 91).

https://doi.org/10.1017/err.2026.10105

Here, the notion of "groups" comes to aid, however, not the same as the one established in the AI Act. This research calls for the protection of *non-traditional or designed, fluid and unaware groups* as autonomous entities, independent from the individual rights each person in the group holds. In this way, not only individuals who are aware and proactive in their behaviour on the Internet, not only *specific, stable and legally recognised* groups, would be protected, but also all those people who have been targeted as *perceived to* pertain to an AI designed group whose characteristics, in the end, do not fit into the GDPR or the AI Act's framework. Those groups exist and as argued throughout this paper have no protection and means to seek redress.

Potential drawbacks might be considered as well. For example, implementing group rights can be a complex in terms of fitting into the existing data protection architecture and it should be balanced against existing rights. Moreover, it could be argued that this novelty may lead to the opposite situation where individual users shielded by the collective protection engage in a frivolous conduct in which they accept whatever conditions posed by the data controller with the idea that their rights would be covered by the enhanced group protection. Also, by relying on a collective approach, the unique preferences and concerns of individual users may be overlooked, leading to a one-size-fits-all approach that may not be suitable for all individuals. The criticism may be continued even further by including proposals to curb the predictive power of AI systems.[98]

While this criticism may prove helpful for anticipating potential loopholes in establishing group rights in data protection, automatically generated groupings already occur. My intention has never been to limit technological advancements but to bring European protection of the people constituting inferred groups up to date, as they currently have no protection and no means to seek redress.

The architecture and gears of the group approach in digital legislation are the subject of another paper, which analysed "groups of persons" prior to the adoption of the AI Act.[99] This is why, in those lines, I build on it further, now that the AI Act has been adopted. The next Section provides practical suggestions for operationalising the concept of groups within existing legislation.

VII. Rewiring the shell: practical guide on operationalising groups

Although non-exhaustive, the following lines provide concrete and attainable objectives with the current legal framework for the introduction of *non-traditional* groups in the AI Act and the GDPR. Curiously enough, both Regulations receive their evaluation reports in 2028. This is a chance not to be overlooked.

1. Define "groups of persons" in the AI Act

It has already been argued that the AI Act should not only foresee provisions which protect groups of data subjects from discrimination, providing them with transparency tools and redress mechanisms, but also it should delimit the contours of those clusters. As already explored in the previous Sections, the AI Act refers to specific groups of people who, by virtue of their age, gender, or social and economic status, might be markedly *vulnerable.* Nevertheless, delimitation and interpretation of the term used in the AI Act has been done in this analysis, and not in the Regulation, which leaves the door open to regulatory and

[98] For example, R Mühlhoff and H Ruschemeier, "Regulating AI with Purpose Limitation for Models" (2024) 1 Journal of AI Law and Regulation 24 <https://doi.org/10.21552/aire/2024/1/5>; R Mühlhoff and H Ruschemeier, "Updating Purpose Limitation for AI: A Normative Approach from Law and Philosophy" (2025) 33 International Journal of Law and Information Technology <https://doi.org/10.1093/ijlit/eaaf003>.

[99] Nikiforov (n 4).

https://doi.org/10.1017/err.2026.10105

judicial interpretation and consequently legal uncertainty and inconsistencies in application and enforcement. Clarifying the interpretation of "groups" in Article 3 AI Act, recognising that groups can be machine constituted based on *assumed, inferred or designed* characteristics (e.g., inferred demographics, behavioural data) where individuals are not aware of their inclusion in the group and where those groups are ephemeral and thus distinct from those already established in the legislation would be a big step.

This raises the question and critique of whether such groups, conceived as single units distinct from the members from whom they are composed, could ever be "identifiable" or possess their *own* identity from an operational standpoint. However, "identity" is not the most appropriate term. It replicates the individualist approach described throughout this paper, implying stability and individual awareness, which does not fit impersonal groups or datasets. Modern automation *designs* groups artificially for specific goals. This design or *designation* is, most importantly, imposed rather than *naturally* arising. Therefore, groups' identity is that identity designed and designated by an external actor for a specific purpose.

2. Reintroduce the group right to complaint in the AI Act and provide guidelines

While the draft of the AI Regulation included a redress mechanism, the adopted text has forsaken it. It is not clear whether the recognition of any potential damages ensuing from biases or discrimination and the information disclosed based on the transparency provisions provided would work out, given that there is no way to claim damages as a result of a particular decision-making result, based on perceived affinities, behaviour or interests. Once again, the regulatory approach focuses on the individual action and claim before a supervisor in order to assert rights. In addition, the claimant should prove damage, which is practically impossible when inferred groups are considered, as pointed out in the cases mentioned in the preceding Section. In practice, this means that no significant change ensues for citizens except the conclusion that they may be discriminated on the grounds of their age or gender for example. Thus, a mechanism for lodging a collective complaint, defined procedural and substantive requisites and legal recognition of this right should ensure higher legal certainty and better legal protection.

Without further progress towards group data protection, realistically, a redress mechanism under the AI Act must be circumscribed to the types of groups the proper law recognises. The blueprint has already been laid out in the past by the European Parliament, which proposed Article 68a (new), establishing a right to lodge a complaint to every natural person or "groups of natural persons" with a national supervisory authority. As already mentioned, the groups in the AI Act are rather the traditionally recognised ones: stable, legally recognised and visible, which makes the reintroduction of the group right to complaint feasible, due to the existence of unions or other interest groups, which may serve as representatives of those groups in the manner of the Article 80 GDPR.

3. Group impact assessment in the AI Act

While the EU legislation is still a long way to go in order to speak about group rights impact assessment, despite Article 27 (c) and (d) AI Act, a new Article 9a would establish a specific and focused impact assessment for groups of persons. This would be a mandatory evaluation of how an AI system's operation affects groups (and their data protection and privacy rights) and whether it exacerbates biases, discrimination or collective harms. In this way, concrete and transparent rules would consolidate certain provisions for groups, facilitating the Regulation's application by deployers and its interpretation by experts.

https://doi.org/10.1017/err.2026.10105

The scholarship has already argued in favour of the reintroduction of some of the provisions proposed but ultimately dropped, as described in a previous paper.[100] For example, Mantelero calls for group representatives in fundamental rights impact assessment (FRIA) as a venue for groups' participation,[101] which was already proposed by the Parliament in Amendments 408 and 413 (Article 29 (a) new)).[102] Other authors propose a severity assessment, which includes "right-holders; their representatives, especially from groups mostly affected due to, e.g., their historical marginalisation."[103] In all those cases, FRIA is devised for recognised and visible groups, and non-iterative (Articles 27 (2 and 4) AI Act).

I operationalise group protection from the "continuous iterative process planned and run throughout the entire lifecycle"(Article 9 (2)) of an AI system. Article 9 (9) implements the risk management system considering the "intended purpose of high-risk AI system" on underaged and "other vulnerable groups." Given the current wave of simplification,[104] it is unlikely that a future reform would broaden this requirement to other than "high-risk systems." Scepticism and speculation aside, risk management systems should be required to include considerations of inferred groups, as defined in this paper. Recital 65 AI Act already contains the premises but could be expanded to cover not only "identifying foreseeable misuse" or "reasonably expected" outcomes. It should also cover adverse consequences with a rebuttable presumption of indirect liability upon deployer's evidence that the purpose behind the inference was not to infringe fundamental rights or to adversely legally or economically affect a person, identified as part of an inferred group or the group as a whole.

The previous point and this one could be introduced in the AI Act after the 2028 Evaluation and review report of the Commission, pursuant to Article 112 AI Act. More immediate remedy, although not with the same result, would be to amend accordingly the technical requirements listed in Annex IV (3) mandating that deployers should provide information on how they ensure effective redress, in particular, to affected groups as described in the Regulation.

4. *Expand the "data subject" in the GDPR*

In order to achieve a more comprehensive protection, a modification of the definition of "data subject" in Article 4 GDPR should include both individuals and groups. This would acknowledge that violations can occur at a group level and would provide legal recourse for collective harms arising from group-based profiling or targeting. The definition should cover not only vulnerable subjects and groups but also such groups which are traditionally not recognised because of their unawareness and instability, as discussed previously. Practically, this change would require a profound reconceptualisation, or rather catharsis, acknowledging the reality and therefore with significant consequences.

The dichotomy between anonymous/personal data is collapsing. No more is the question "who are you?" but "in which modelled group do you fit?" Personal data is not just *about the* person it names; it is relational and can be externally produced, false and

[100] Ibid.

[101] A Mantelero, "The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template" (2024) 54 Computer Law & Security Review 106020 <https://doi.org/10.1016/j.clsr.2024.106020>. And on a similar vein, N A Smuha, "Beyond the Individual: Governing AI's Societal Harm" (2021) 10 Internet Policy Review <https://doi.org/10.14763/2021.3.1574>.

[102] European Parliament (n 51).

[103] G Malgieri and C Santos, "Assessing the (Severity of) Impacts on Fundamental Rights" (2025) 56 Computer Law & Security Review 106113 <https://doi.org/10.1016/j.clsr.2025.106113>.

[104] "Digital Omnibus on AI" <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD%3A2025%3A0836%3AFIN%3AEN%3APDF&utm_source=chatgpt.com>.

https://doi.org/10.1017/err.2026.10105

used to make decisions that affect other people. Therefore, future reforms should adapt the concept of the data subject by broadening the criteria for identifiability by *relationalising* it, not *relativising* it.[105] This would mean personal data would be such if there is a *potential* to relate to the *same subject or another natural person*.

5. Collective transparency and rights in the GDPR

The introduction of explicit mention to groups in the GDPR would presuppose a bigger reform, which would encompass the rights and obligations enshrined therein. So, to ensure that the intended outcome of the previous modifications is achieved, several Articles such as Articles 12–14 should include a transparency mechanism that ensures individuals included in and potentially affected by group targeting are informed. For example, the most straightforward way to do it is through Article 13 (2)(f), Articles 14 (2)(g) and 15 (1)(h). Before the inclusion of a more explicit group transparency provision, those provisions could be interpreted to provide information about "the logic involved," which could include any algorithmic groups.

6. Obligations in the GDPR

An amendment to Article 25 requiring data controllers to take specific measures to protect group data protection might be useful. Controllers should be required to assess how data processing affects both individuals and groups, especially where group profiling is used to make automated decisions or generate inferred predictions about groups.

7. Collective redress mechanism in the GDPR

Extension and development of Article 80 is needed in order to allow groups to lodge complaints with supervisory authorities in cases of group-level data violations. This would enable a representative entity to act on behalf of a group, similar to class-action lawsuits, to address collective damages such as algorithmic discrimination or large-scale data breaches. This is different from the current provision as in the proposed one the defence and compensation would be in the name of a collective entity, and not in the name of a number of individuals.

8. Group data protection impact assessment in the GDPR

The previous amendments require a complex procedure to be carried out and may be better suited to a more detailed and ambitious reform. However, the text of Article 35 (4) GDPR mandates that the European data protection supervisor should adopt a list of the types of processing operations subject to a data protection impact assessment. It was done in 2019.[106] The document acknowledges multiple of the high-risk circumstances discussed here. The list of criteria could include (inferred) groups' impact as a criterion as well. It would include not only any potential adverse effect on age, gender, health, social or economic groups but also any other *unexpected* or even *unintended* groups, emerging from automated analysis.

[105] The proposed Digital Omnibus *relativises* personal data. I propose to *relationalise* it. The Omnibus proposal: <https://eur-lex.europa.eu/resource.html?uri=cellar:ebf17714-c56e-11f0-8da2-01aa75ed71a1.0001.02/DOC_1&format=PDF>.

[106] "Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA Lists Issued under Articles 39(4) and (5) of Regulation (EU) 2018/1725" <https://www.edps.europa.eu/sites/default/files/publication/19-07-16_edps_dpia_list_en.pdf>.

https://doi.org/10.1017/err.2026.10105

VIII. System sync between shell and soul

The suggested changes are nonetheless patches, if not wishes, unless a more ambitious reform of the current data protection system is undertaken. Without that system synch, EU law will keep regulating the Shell while the Ghost keeps deciding outcomes off-ledger.

Neither consent nor the notion of groups are new concepts. AI systems routinely *designs groups* of individuals, often unaware, and unidentifiable, while the GDPR and the AI Act still allocate rights and remedies to identifiable subjects. The result is a structural asymmetry where injunctions can be obtained without mandates, but compensation still requires identifiability and individual standing. That gap is not accidental because it is a legacy of an individual-centric architecture that never anticipated AI-generated groups of people.

Just as at the very beginning of the industrial revolution, Public law could not provide remedies to negative externalities caused by industry, because private bargaining was supposed to suffice. In hindsight, it seems insufficient, if not impracticable, without a further regulatory conceptual development. Just as European data protection is today, in the face of the Digital Revolution. The law already contains the pieces to fix it. The Parliament's draft AI Act supplied the missing parts: definition, transparency/participation and a group-complaint right. The 2028 reviews of both the GDPR and the AI Act are the obvious moments to re-address those concerns.

Absent those steps, the EU's data protection framework will continue to protect only the visible, recognised already individuals, while leaving the AI-constructed ghosts, the soul behind the cyborg shell, groups of people with no realistic path to a meaningful remedy. Recognising, defining, and empowering groups is not a conceptual revolution but an overdue adjustment to how AI already processes and harms people. This is why my hope is that this study contributes to the opening of new horizons in data protection and privacy by inspiring further research and discussions.

Cite this article: L Nikiforov (2026). "Ghost in the Shell: Inferred Groups under the AI Act and the GDPR. Concrete Solutions for System Sync". *European Journal of Risk Regulation* **17**, 1032–1053. https://doi.org/10.1017/err.2026.10105

https://doi.org/10.1017/err.2026.10105