Palmerini E., 'Data protection law and the regulation of artificial intelligence: a two-way discourse' (2025) Special Issue EJPLT.
DOI:

EJPLT
ISSN 2704-8012

Data protection law and the regulation of artificial intelligence: a two-way discourse

Protezione dei dati e regolazione dell'intelligenza artificiale: discipline in dialogo

ERICA PALMERINI
Associate Professor of Private Law
Scuola Superiore Sant'Anna di Pisa

The paper aims to analyse the relationship between the law on the protection of personal data and the regulation of artificial intelligence, in search of synergies and with a view to a complementary application to automated processing and decision-making. In particular, in anticipation of the possible development of a European regime of civil liability for damage caused by AI systems, it turns to the compensatory remedy provided by the GDPR as a means of protecting the interests violated by abusive algorithmic practices.

Il contributo si propone di analizzare il rapporto tra le discipline della protezione dei dati personali e dell'intelligenza artificiale, alla ricerca di sinergie e in vista di un'applicazione complementare ai trattamenti e alle decisioni automatizzate. In particolare, in attesa degli eventuali sviluppi di un diritto europeo della responsabilità civile per i danni causati dai sistemi IA, ricorre al rimedio risarcitorio previsto dal GDPR quale dispositivo di tutela delle situazioni di interesse offese da pratiche algoritmiche abusive.

Keywords: data protection; artificial intelligence; public and private governance.

Summary: Introduction – 1. Regulatory approaches of the GDPR and the AI Act: similarities and differences. – 2. Overlaps, interactions, clashes. – 3. Privacy harms and AI harms.

Introduction.

There are significant similarities between the regulatory fields of data protection, on the one hand, and artificial intelligence, on the other, especially when the latter consists of machine learning and deep learning techniques. Such correspondences appear both in the phenomenological reality that is the target of regulation and in the approaches that the European legislator has chosen to address it.

From the first point of view, a complementarity is undoubtedly to be found in the fact that learning algorithms need to be fed with large amounts of data, which will often include personal data. It is widely agreed that the most advanced developments in artificial intelligence would not have been possible without the massive availability of information in digital form, which adds up to the growth in computational power of machines.

A convergence, often problematic, between privacy and artificial intelligence exists with reference to both the inputs and outputs of algorithmic computation. [1] The collection of data is essential to the functioning of algorithms; the subsequent processing by artificial intelligence systems leads to the generation of new data, production of knowledge, classifications and predictions, as well as to decisions affecting the data subjects themselves.

From the second perspective, that of the regulation of the two phenomena, we can detect as many convergences as, admittedly, a few discontinuities. The most important of the former is the prominent role assigned to public regulation, which leaves less room for the deployment of instruments of private governance. However, while in the European data protection model, we can find a combination of rules of a preventive nature that organise and conform the processing activity, as well as a wide set of individual rights, in the regulation of artificial intelligence the latter are almost completely missing.

We can now provide a general understanding of these regulatory approaches, which in both cases have taken the form of a European regulation; also, given the inevitable overlap between the two bodies of law, attempt to reconcile potential contradictions; and finally, suggest ways in which their interaction can be exploited to fill any gaps in protection.

1. Regulatory approaches of the GDPR and the AI Act: similarities and differences.

[1] DJ Solove, 'Artificial Intelligence and Privacy' (2025) 77 Florida Law Rev. 1, 5 f., 26 ff.

In the area of data protection, a regulatory environment has been created that surrounds and informs the collection and use of personal data, including in the case of algorithmic processing.

Although private law instruments such as tort and contract could also play a regulatory role, they cannot systematically address the phenomenon of data exploitation.

The obstacles to an adequate allocation of the risks inherent in data processing activities through the mechanisms of private agreements or tort law have been thoroughly explored and underlined. Personal data, once released, become dispersed and data subjects inevitably lose control over them. Consent as an individual control device is inadequate to grasp the complexity of the operations that take place on data, especially in the digital environment, and loses much of its protective scope in this reality.[2]

The system of data collection, use and distribution is too complex to be managed by contractual agreements or similar instruments that require rational and informed choices by the consenting party.[3]

The recovery of damages in tort law, on the other hand, suffers from difficulties of a different nature, although they are more evident outside the European context.

This is why, in addition to relying on individual consent as a control mechanism, the GDPR sets out a wide range of precautionary measures that apply to all types of processing and do not depend on the initiative of the data subject to consent, such as data minimisation, purpose limitation, privacy by design, and the obligation to carry out a data protection impact assessment under certain conditions.

These rules may have a predominant procedural value, with companies complying with them without substantively protecting the rights of individuals; and often these measures turn out to be over-regulatory, creating barriers to useful and harmless data processing that burden SMEs in particular, or even individuals, and the public sector, for example in the area of health research. However, they do create a certain and defined framework within which the processing activity can take place safely and with reduced risk of harm.

Moreover, the GDPR also resorts to some general principles designed to steer the behaviour of economic operators, at the same time endowing them with the necessary suppleness and elasticity.

The principle of accountability, expressed in particular in Art. 24, and the explicit inclusion of fairness among the parameters of lawfulness of the processing (Art. 5(1)(a))[4] make the mandatory rules more flexible and gain room for the evaluation of the concrete circumstances. In this sense, they can also be valuable on the ex-post side of conduct assessment, ensuring a smoother interchange between the apparatus of preventive obligations and

[2] For a detailed account, see I Cofone, *The Privacy Fallacy. Harm and Power in the Information Economy* (Cambridge University Press 2024) 46 ff.

[3] For an outspoken critique of the model based on individual rights in the face of the social damage caused by the economy that extracts value from data cfr. AE Waldman, 'Privacy's Rights Trap' (2022) 117 Northwestern University L Rev, 88 ff.; O Ben-Shahar, 'Data Pollution' (2019) 11 Journal of Legal Analysis, 104 ff.

[4] A Häuselmann, B Custers, 'Substantive Fairness in the GDPR: Fairness Elements for Article 5.1a GDPR', (2024) 52 Computer Law and Security Review.

the criteria for attributing responsibility, avoiding automatic correspondences between formal compliance and exemption from liability.

The Artificial Intelligence Act is characterised by a similar approach in setting out safety rules aimed at permitting, and even encouraging, the development of artificial intelligence systems while minimising the risks associated with them. The prohibition of practices deemed to pose unacceptable risks to the fundamental rights of individuals, together with a detailed regulation of high-risk systems, including essential product conformity requirements to be contemplated within an articulated risk management process, form the basis for the lawfulness of the production, marketing and use of artificial intelligence.

In contrast to the data protection system, this apparatus is more rigidly structured, since it does not contain any general clauses or flexible devices that could help to underpin the array of procedural and substantive safeguards, and limits to a minimum the scope for the exercise of individual rights and remedies.[5]

2. Overlaps, interactions, clashes.

These legal frameworks can certainly work in sinergy, as practical experience also shows. It is worth noting that some applications of artificial intelligence had already been analysed from a data protection perspective before they were directly regulated by the AI Act. This is the case of the platform that offered a reputational profiling service;[6] of municipal research projects used for predictive policing and urban surveillance purposes;[7] of facial recognition systems trained through the indiscriminate collection of images posted on freely accessible social sites and accounts;[8] and of a chatbot that, by generating a virtual friend, enabled interactions, including with minors and vulnerable people, that were considered ambiguous and potentially dangerous.[9]

The rule on automated decisions, Article 22 of the GDPR, is also a cornerstone among the set of instruments that can be used to frame and regulate the deployment of artificial intelligence. Indeed, it was the first tool available to counter the phenomenon of algorithmic discrimination.[10] The

[5] Cfr. G De Gregorio, P Dunn, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59 Common Market L Rev, 473 ff.

[6] Italian Data Protection Authority, decision n. 488, 24.11.2016; Trib. Roma, 4.4.2018, n. 5715; Cass., 25.5.2021, n. 14381, *Dir. inf. inform.*, 2021, 1001 ff.; Cass. 10.10.2023, n. 28358, *Nuova giur. civ. comm.*, 2024, I, 408 ff.

[7] Italian Data Protection Authority, decision n. 5, 11.1.2024, concerning the use by the Municipality of Trento of AI systems, developed within the framework of some European projects, which involved the collection of data through microphones and surveillance cameras and their subsequent processing in order to detect situations of danger to public safety.

[8] The Italian Data Protection Authority, as well as other European authorities, launched an investigation on the application developed by the company Clearview, that ended with the decision n. 50, 10.2.2022. Art. 5, lett. e), of the AI Act now forbids AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage. Cfr. also the decision of the French CNIL, 19.10.2022.

[9] Italian Data Protection Authority, decision n. 39, 2.2.2023.

[10] Amsterdam Court of Appeal, 4.4.2023, concerning the algorithms used by Uber and Ola Cabs to assess the drivers' behaviour and deactivate their accounts in case suspicious activities were detected.

European Court of Justice has recently endorsed a broad interpretation of the notion of decision, [11] and acknowledged the wide scope of the set of information on the logic used in the automated processes that must be provided to the data subject, thus allowing the construction of a genuine right to an explanation.[12]

However, not all potential risks inherent in algorithmic practices can be covered by privacy protection. For example, Regulation 679/2016 lays down the principle of accuracy and requires personal data to be up to date; these aspects are undoubtedly relevant to the data quality requirement, which is also central in the AI Act, but they do not exhaust it. In fact, data quality also includes the aspects of relevance, representativeness and completeness (Art. 10(3) of the AI Act), which allow the algorithm to be inclusive, thus capable of expressing the variability present in the population that will be the recipient of the process outputs, and as free as possible from discriminatory results.

In addition, many exploitative practices do not originate from a violation of privacy (data is not necessarily illegally shared or disseminated), nor do they cause any harm to privacy. Exposure of minors to harmful content that may lead to dangerous behaviour, manipulation of consumer autonomy that may encourage compulsive consumption, price discrimination that causes economic loss and other similar techniques can only be addressed by a combination of instruments, including data protection law in case of unlawful collection and processing of data;[13] and the legislation on AI, drawing especially on the rules on prohibited practices [14] and the transparency obligation imposed on providers and deployers.

The legislation on unfair commercial practices can also make a useful contribution, given the broad definition of commercial practice and transactional decision, which allows all activities surrounding a contract to be assessed. This was the case with the customisation function of the TikTok platform's feed, which, under the guise of a challenge, suggested videos that showed self-harming behaviour, targeting precisely those users, presumably vulnerable, who were more engaged by the viewing. The recurrent presentation of this content by means of a recommendation system based on profiling was found to be capable of appreciably distorting consumer behaviour, which may in fact consists of scrolling through the feed and increased time spent on the social network, 'as well as indirectly threatening the safety of children and adolescents'.[15]

In several EU countries, market surveillance authorities have approached data collection from the perspective of unfair commercial practices, checking whether the conditions for valid consent were met, information was sufficient and provided in a clear manner, and whether the design of the interface was misleading or encouraged anti-privacy choices.

---

[11] ECJ, 7.12.2023, case C-634/21.
[12] ECJ, 27.2.2025, case C-203/22.
[13] Cfr. SMO v TikTok Inc and others [2020] EWHC 3589 (OB).
[14] A number of class actions have been brought against the TikTok platform under, inter alia, Section 5 of the newly enacted AI Act: <https://www.medialaws.eu/tiktok-and-x-faces-class-action-suit-for-violations-of-dsa-gdpr-and-ai-act/>.
[15] AGCM, decision n. 31124 – TikTok French scar, 5.3.2024, in *Bollettino* n. 11, 18.3.2024, 67 ff.

A further advantage of this regulation is its substantive quality: it does not consist of procedural rules, but rather of general clauses that make it possible to assess a given practice on a substantive level, leaving no room for mere formal compliance. A disadvantage may be that, in order to be unfair, the practice must be capable of influencing the behaviour of the average consumer, who is deemed to be the reasonably well informed and circumspect consumer. This standard does not take into account the asymmetry of power and information between businesses and consumers in the digital environment.

However, the notion of vulnerable consumer could prove useful: some scholars point to the need to revise it, taking into account the findings of behavioural economics and the particular vulnerability of consumers in the face of platforms and large digital operators with detailed knowledge of their users.

Another piece of legislation relevant to our purposes is the regulation of platforms: the use of dark patterns is now prohibited by Article 25(1) of the Digital Services Act; and information obligations have been introduced by the Directive on the Modernisation of Consumer Law to counter some practices that may tend to manipulate users in digital marketplaces, such as the use of recommendation systems, the ranking of commercial offers in response to an online search, and the system for managing customer reviews.

As we have seen, the possible interactions between the disciplines of data circulation, on the one hand, and the development and deployment of artificial intelligence systems, on the other hand, are manifold. However, the doctrine has also explored the conflicting dynamics between these bodies of law. They focus in particular on the functioning method of machine learning algorithms, which require the processing of huge amounts of data, often in search of correlations according to purposes and logics that have not been defined in advance. This mode of operation may run counter to the principles of minimisation and purpose limitation that govern the processing of personal data and determine its lawfulness.

Leaving aside the analyses that see an irreducible contrast between the two disciplines, [16] recent opinions point to evolutionary interpretation as a means of reconciling the divergent approaches and smoothing out the main conceptual and operational problems. [17] For example, the principle of data minimisation can be understood as a relative rather than an absolute criterion, which links the amount of data necessary for the processing to the objectives that the controller seeks to achieve, and can also purport on the notion of compatible purpose. By properly framing the purpose of the processing, it is possible to legitimise big data practices that can have positive effects for those affected, such as algorithmic credit scoring that is calculated on the basis of multiple variables rather than the most conventional ones, which can end up penalising those who do not have a credit history.

[16] T Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 Seton Hall L. Rev. 1009 ff.

[17] I Spiecker, G Döhmann, 'AI and Data Protection', in DiMatteo, Poncibò, Cannarsa (eds), The *Cambridge Handbook of Artificial Intelligence. Global Perspectives on Law and Ethics* (Cambridge University Press 2022), 132 ff.; M Winau, 'Areas of Tension in the Application of AI and Data Protection Law' (2023) European Data Protection Law Rev., 123 ff.

3. Privacy harms and AI harms.

One of the most promising interactions between the GDPR and the AI Act concerns the remedial side. The AI Act is characterised as a preventive security regulation that leaves little room for individual remedies, with the exception of the right to lodge a complaint (Art. 85) and the right to an explanation of the logic used in automated decision-making (Art. 86), the latter complementing the protection already provided by Art. 22 GDPR.

The absence of a specific provision on compensatory remedies in the AI Act, the objective similarities between privacy harms and AI harms, and the broad scope of Art. 82 GDPR suggest that it should be relied upon more extensively.

The closeness of the two figures can be observed first of all from a phenomenological point of view. The offence may originate from a common root, such as an unauthorised intrusion into the private sphere, the collection of data outside any requirement of minimisation and containment, the dissemination and transfer of sensitive data information to third parties.

Processing activities carried out in violation of the general rules of lawfulness, or undertaken without obtaining valid consent (for example, because consent is given on the basis of inadequate information about the purposes for which the data will be used, or is obtained through pre-selected options), could make the subsequent practices of profiling and communication of data to third parties unlawful. Consent, on the other hand, cannot legitimise discriminatory or predatory algorithmic practices aimed at exploiting the vulnerabilities of data subjects, and its invalidity constitutes both an unlawful processing of personal data and, hypothetically, a practice prohibited by the AI Act. Moreover, it is the text of the Data Protection Regulation itself that identifies the evaluation of personal aspects relating to employment and economic status, behaviour, health or personal interests for profiling purposes as one of the main risks to rights and freedoms (recital 75), which may then result in actual harm (recital 85).

The profiling of individuals through the processing of massive amounts of data collected on the web can lead to arbitrary constructions of personality, which in themselves are detrimental to one's image, but is fraught with further consequences, such as stigmatising individuals, excluding them from opportunities of various kinds, and segregating or marginalising entire social groups.[18] If a digital profile erects a bubble around the person, they may be excluded from job opportunities, because the algorithms used in screening applications do not recognise the value of their application, perhaps on the basis of elements of little significance or decontextualised information. Prior to this, the individual may not even be aware of the availability of a job position, as he or she is not one of the recipients of the relevant communication due to algorithmic management of the relevant advertising.

In a cycle of hyper-personalisation, the same stereotypes can be reinforced and spread to other spheres of private life, leading to outright discrimination

[18] Cfr. S Barocas, A Selbst, 'Big Data's Disparate Impact' (2016) 104 California L. Rev., 671 ff.; C O'Neil, *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy* (Crown Publishing 2016).

or at least making it more difficult to access private services (in the credit and insurance markets, as well as the labour market) or public services (such as education, health, welfare), when they are managed on the basis of automated decisions.

It is well known that a typical form of algorithmic bias concerns the female gender, due to the fact that women are generally underrepresented in the datasets on which the software is trained: they are less present on the web, less often mentioned as the subject of news items or as a source of opinion, and scarcely described in the case histories expressed by health databases. The erroneous result this produces may only affect the level of representation and simply return a distorted image of reality. But the same flaw in the design of the model can have a major impact on the person if it is used to make a decision about him or her. The employment situation remains paradigmatic, with the increasing use of algorithms to support the selection process and the evaluation of CVs. If the male gender was predominant in previous recruitment experiences, the system will recognise this factor as an index of success and will tend to consider it as a preferential criterion for recruitment.

In the context of consumer relations in the digital environment, profiling activities may interfere with the proper exercise of private autonomy. [19] Personalised and aggressive marketing that exploits group or individual vulnerabilities, even incidental or occasional ones, or relies on emotional AI techniques, [20] can manipulate intent and induce contractual behaviour detrimental to economic interests, such as compulsive buying. The practice of price discrimination, which is based on the prediction of income capacity or urgent need for a particular good, prevents access to goods or services that may be essential, for instance in the transport sector, and generates unjustified rents. Algorithms embedded in everyday objects, such as personal digital assistants or smart home devices,[21] could be used to promote specific products or services, possibly from the same supply chain as the trader, with the effect of steering market movements and trends.

The addiction created by the so-called attention economy[22] through social networks can cause psychological damage at an individual level; at a societal level, it can distort information, polarise public discourse and cause a decline in the principle of pluralism and the open nature of the democratic circuit.

Algorithmic practices such as fake news or hate speech cause discomfort and suffering to those directly affected by them; online misinformation can lead to psychological harm or even physical injury if it relates to health or food issues.

---

[19] Norwegian Consumer Council, *Out of control. How consumers are exploited by the online advertising industry*, 14.1.2020; E Mik, 'The erosion of autonomy in online consumer transactions' (2016) 8(1) Law, Innovation and Technology, 1 ff.; BEUC, *Regulating AI to protect the consumer*, 7.10.2021; N Helberger et others, *EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets*, March 2021.

[20] P Hacker, 'Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law' (2023) 29 European Law Journal, 142 ss.; R Montinaro, 'Emotion Recognition and Personalized Advertising' (2024) 32 European Review of Private Law, 1003 ff.; P Valcke, D Clifford, VK Dessers, 'Constitutional Challenges in the Emotional AI Era', in HW Micklitz and others (eds), *Constitutional Challenges in the Algorithmic Society* (2022 Cambridge University Press), 57 ff.

[21] JM Paterson, Y Maker, 'AI in the Home: Artificial Intelligence and Consumer Protection Law', in E Lim, P. Morgan (eds), *The Cambridge Handbook of Private Law and Artificial Intelligence* (2024 Cambridge University Press), 113 ff.

[22] Cfr. European Parliament resolution of 12 December 2023 on addictive design of online services and consumer protection in the EU single market (2023/2043(INI)).

And above all, they can have wider social impact, with the spread of anti-scientific or historically uncorrect views and the incitement of the most radical positions.

The tendency to produce content that is illegal or offensive towards individuals or entire classes of people, to reinforce prejudice and discrimination and, as a consequence, to marginalise disadvantaged communities seems to be particularly peculiar to AI generative models.[23]

A pervasive use of surveillance and biometric recognition systems in public places may have a chilling effect on the exercise of freedoms such as the freedom of association and of movement. But this inhibiting effect can also be felt in relation to information on the Internet, when people refrain from carrying out searches, particularly on sensitive topics (health, sexual orientation, political leanings, etc.), for fear of not being able to do so anonymously and of revealing attitudes, behaviours and other things they wish to keep private. [24]

These briefly outlined cases share a number of common features, which make them difficult to address trough individual remedies.[25] They relate to the often minimal or modest incidence of the conduct evoked on the individual sphere, while the harmful consequences result mainly from accumulation and repetition over time, or can only be appreciated on a larger scale. Moreover, the individual victim may not even be aware of being discriminated against or otherwise harmed: if the algorithm systematically discards someone from the targeted audience for a job advertisement, whether because of incorrect profiling or discriminatory construction, it is impossible to detect that one has been arbitrarily excluded. The same effect could occur at a later stage in the recruitment process due to programmes that filter the applications received. Or a consumer may receive online commercial offers with higher prices based on a prediction (no matter whether correct or not) of wealth and good purchasing power; but if price differentiation is a widespread practice, the ability to compare the offers and thus perceive the unfair treatment is limited, because one will be subject to the same or a very similar calculation in each marketplace.

The lack of transparency therefore conceals the infringing practice and prevents any reaction; the low level of damage in turn discourages action, since the costs of litigation could be disproportionate to the benefit of a successful claim.[26]

Faced with these difficulties, the liability regime of Article 82 of Regulation 679/2016 may be a suitable container for the wrongs described and represent the pole of attraction for many algorithmic practices that feed on information for profiling purposes, decision making, or producing other types of content

---

[23] R Bommasani and others, *On the Opportunities and Risks of Foundation Models*, Center for Research on Foundation Models (CRFM) at the Stanford Institute for Human-Centered Artificial Intelligence, 12 July 2022, 129 ss., <https://arxiv.org/abs/2108.07258>.

[24] Federal Trade Commission, *Online Profiling: A Report to Congress*, 2000, 13.

[25] Cofone, *The Privacy Fallacy* (n 2); DK Citron, DJ Solove, 'Privacy Harms' (2022) 102 Boston University Law Rev., 793 ff.; R Calo, 'Privacy harm exceptionalism', (2014) 12(2) Colorado Technology Law J., 361 ff.

[26] N Smuha, 'Beyond the individual: governing AI's societal harm', (2021) 10(3) *Internet Policy Review*, 9, refers respectively to the "*knowledge gap problem*" and the "*threshold problem*". These hindrances are also recognized in the context of privacy infringements: F Lancieri, 'Narrowing Data Protection's Enforcement Gap' (2022) 74 *Maine Law Review*, 15 ff.

towards a specific recipient. Discrimination, deprivation of emotional and psychological well-being, disruption of personal and professional relationships and economic losses would seem to be particularly amenable to this provision.

Art. 82 is applicable whenever damage results from the processing of personal data carried out in violation of its rules. The very broad notions of personal data, on the one hand, and of processing, on the other hand, facilitate its involvement.[27] The advantageous criterion for attributing liability, which allows the data controller to be exempted only by proving that he is in no way responsible for the event that caused the damage, makes it preferable to other regimes. Moreover, the types of damages that can be compensated include both material and immaterial damages.

In addition to belonging to similar typologies, privacy and AI harms share other features, such as the sometimes elusive nature of the damages involved and the difficulty of quantifying them. Breaches of privacy can create a sense of mistrust due to the betrayal of the expectation of confidentiality or the belief that the data would be processed for certain purposes and not for others; they can induce a feeling of frustration because the intention not to disclose it to third parties was not fulfilled; the violations, in turn, can cause fears of future abuse, in the form of a flood of unwanted commercial offers or fraudulent uses of the information by those who have come into possession of it.

These prejudices have a consistency that is sometimes barely perceptible; they may foreshadow further consequences, but only uncertain and potential ones; the flow of information captured may propagate in unexpected directions, but along routes that are not immediately foreseeable. Protecting information about one's own life and preferences can then serve to safeguard economic interests, such as avoiding being offered higher prices on the basis of a prediction of a high spending capacity; or instead to shield a simple desire for privacy, a psychological aversion to being observed; or even to defend reasons of identity. Consider the case that led to a class action lawsuit in the United States, where images collected by a dating app were then sold to another company, which used them to train a facial recognition system intended to be integrated into autonomous weapons.[28]

The consonance between the two types of harm is confirmed by the case that gave rise to the first important judgment of the Court of Justice of the European Union on Article 82 of the GDPR.[29] An Austrian citizen complained that a firm collected social and demographic information about its customers and, based on statistical projections, grouped them according to political affinity in order to sell the results to third parties interested in targeted electoral advertising. The algorithmic model employed had detected the plaintiff's affinity with an extreme right-wing party, causing him a feeling of discomfort, loss of confidence and humiliation.

[27] N Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10(1) Law, Innovation and Technology, 75, purportedly highlights the risk of overloading the system "in the circumstances where everything is personal data and everything triggers data protection".
[28] Cofone (n 2) 46.
[29] ECJ, 4.5.2023, case C-300/21. Cfr. F Episcopo, 'UI v. Österreichische Post – A First Brick in the Wall for a European Interpretation of Art. 82 GDPR' (2024) Journal of European Consumer and Market Law, 87 ff.

The ECJ decision affirms that the concept of damage in Art. 82 is an autonomous concept of Union law, which must be interpreted uniformly in all member states, and in accordance with recital 14, which states that "the concept of harm should be interpreted broadly ... in such a way as to fully reflect the objectives of this Regulation". Damage must be proven, and a mere violation of the Regulation would not be sufficient to award compensation; however, it is not required that the damage suffered exceed a minimum threshold of severity. Thus, temporary afflictions and emotional distress are, at least in theory, compensable.

Even the mere theft of data, which does not lead to immediate harmful consequences, such as identity theft, may nevertheless constitute immaterial damage, in the form of the fear that the data will be used fraudulently in the future.[30] This fear must be well-founded, whereas there can be no harm if the risk of misuse is purely hypothetical and, in the circumstances of the case, completely insubstantial. [31] Finally, it has been confirmed that the non-pecuniary damage suffered by a German citizen as a result of the transmission of his data, and in particular his IP address, to the Meta platform located in the United States is compensable. It is in fact considered a 'real' damage resulting from being 'placed in a situation of uncertainty' with regard to the control over his personal information.[32]

Private enforcement of the GDPR can also be strengthened in response to AI harms through the collective remedy provided by Article 80, which Member States can extend to compensation actions. In particular, this aggregation tool could overcome the problem of the lack of incentives to sue for small damages. And in an overall strategy, it could be valuable in addressing those systemic risks that materialise in societal damage, of which it would be able to capture the relevant portion at the individual level.

In conclusion, pending the development of a European tort law for AI, the GDPR lends itself to collecting the wrongs arising from algorithmic processing of personal data implemented in breach of its requirements. Although there is only a partial overlap between the hypotheses of damage that may arise from the use of algorithmic models and those resulting from a direct violation of the GDPR, the compensatory remedy provided by the latter may help to structure a more robust framework of guarantees against AI risks.

[30] ECJ, 20.6.2024, case C-182/22 and C-189/22; ECJ, 14.12.2023, case 340/21.
[31] ECJ, 25.1.2024, case C-687/21.
[32] General Court, 8.1.2025, case T-354/22. To be applied in this case is Article 65 of Regulation 2018/1725 since the European Commission is responsible for the offence, but Article 82 of the GDPR and the case law relating thereto contribute to determining its interpretation by analogy (cfr. § 196).