





Damages liability for privacy infringements: the case law of the Court of Justice of the European Union in light of *'The Privacy Fallacy'*

Responsabilità per danni da violazioni della privacy: la giurisprudenza della Corte di giustizia dell'Unione europea alla luce di "The Privacy Fallacy"

[BÉATRICE SCHÜTTE](#) 

Postdoctoral researcher
University of Lapland

[KATRI HAVU](#) 

Associate Professor of EU Law
University of Helsinki

Abstract

This contribution reflects on Cofone's discussions in *'The Privacy Fallacy'* and the case law of the Court of Justice of the European Union on damages liability for privacy infringements. Cofone highlights the shortcomings of current legal rules and frameworks in addressing harm caused by data practices that affect large numbers of individuals. The Court of Justice of the European Union adjudicates individual cases of harm, which restricts it to a narrow perspective on privacy-related harm in the EU and its Member States. Cofone's assertion that legal rules and procedures fail to ascribe adequate value to privacy and impose insufficient sanctions on data practices that cause harm while benefiting companies and authorities appears to be well-founded.

Abstract

Questo contributo fornisce alcune riflessioni sulle analisi di Cofone in "The Privacy Fallacy" e sulla giurisprudenza della Corte di giustizia dell'Unione europea in materia di responsabilità per danni derivanti da violazioni della privacy. Cofone evidenzia le carenze delle attuali norme e modelli giuridici nel far fronte ai danni causati dalle pratiche di trattamento dei dati che incidono su un gran numero di individui. La Corte di giustizia dell'Unione europea si pronuncia su singoli casi di danno, offrendo così solo una visione parziale di come il danno alla privacy venga affrontato nel diritto dell'UE e degli Stati membri. L'argomentazione di Cofone, secondo cui le norme e le procedure giuridiche non attribuiscono un valore adeguato alla privacy e non impongono sanzioni sufficienti alle pratiche di trattamento dei dati che causano danni pur avvantaggiando imprese e autorità, appare fondata.

Keywords: Damages liability; Privacy; Court of Justice of the European Union

Summary: [1. Introduction.](#) – [2. Non-material harm before the Court of Justice.](#) – [3. Compensating harm to privacy under the GDPR and beyond.](#) – [4. Do we need to go beyond individual damages claims?](#) — [5. Conclusion.](#)

1. Introduction.

Civil proceedings based on an infringement of a person's privacy, as such, are nothing new under the sun. However, in the not-too-distant past, discourse about privacy was often linked to situations in which a person – often a celebrity – had been photographed and had their photo published. Caroline of Monaco/Hannover was behind some of the landmark cases.¹ Now that the Internet, AI and other digital technologies have become more common, we are facing a completely different dimension of (potential) privacy violations. Our main concern is no longer whether someone randomly snatches a picture of us in the street with their smartphone. Instead, our privacy is now in danger every time we use our computer or our smartphone. E-mail programmes, browsers, social media and other apps need (personal) data to function properly, just like we need air to breathe in order to stay alive. More often than not, we are presented with the privacy policy of a web page or app, and we need to tick or untick a varying number of boxes to continue. This exercise allegedly ensures that we know what data will be harvested from us and how it will be processed. But do we really know that? Are we provided with accurate information? And is it even feasible for us to supervise the use of our data?

Cofone's book *The Privacy Fallacy: Harm and Power in the Information Economy* asks how legal rules could properly reflect the real value that most contemporary humans place on privacy and personal data. Among other matters, Cofone considers the prevailing contractual approach to personal data and privacy to be inappropriate. He also questions the manner in which

¹ See e.g. *Von Hannover v Germany*, no 59320/00, 24 June 2004, ECHR 2004-VI, 1, (2005) 40 EHRR 1. The case addressed a series of incidents, where paparazzi had taken pictures of her on private outings. German national courts had dismissed all of her claims. The ECHR held that her right to private and family life as per Article 8 of the European Convention on Human Rights had been infringed.

damages-liability rules and courts deal with privacy intrusions. According to Cofone, they fail to account sufficiently for the intrinsic value of privacy, and they fail to set just compensation for non-material harm to privacy in many cases.² The question of damages liability is a very “individualistic” one, and it always concerns what has happened to a specific individual who already knows, *de facto*, that they have been harmed in some specific manner. In the information economy, non-material harm can accrue to numerous individuals simultaneously and in ways that are not always easy to discern; if legal rules and courts are to address this issue comprehensively, a new approach to traditional damages-liability rules is needed. Cofone, as well as other contemporary authors, is underscoring this point.³

In this short contribution, we will compare Cofone's arguments with the case law of the Court of Justice of the European Union (CJ). We will also present further remarks on harm to privacy and the means of addressing it through damages-liability rules. This discussion is presented from the standpoint of the laws of the EU and European countries.

2. Non-material harm before the Court of Justice.

There is a considerable amount of CJ case law on compensating non-material harm under EU law. Questions concerning damages claims for non-material harm arrive to the CJ either as inquiries about the wrongdoing of the EU or its specific bodies, or as preliminary-ruling requests from national courts in cases on the damages liability of a Member State or individuals. Historically, CJ judgments on non-material harm have mostly been issued in cases in which the defendant is the EU, that is, cases in which somebody has claimed damages from the Union. The existing cases include, for instance, staff cases and cases on EU public procurement. There are also cases about fundamental-rights infringements by the EU.⁴ More recently, preliminary-ruling requests on the General Data Protection Regulation (GDPR)⁵ have been on the rise. These cases have also resulted in CJ preliminary rulings in which the CJ clarifies the interpretation of EU law for the national courts that are tasked with resolving EU law-based damages claims.⁶

Despite non-material harm being a common issue before the CJ, some ambiguities remain in the application of conditions for liability to cases that involve non-material harm. Furthermore, how to adequately “quantify” non-

² I Cofone, *The Privacy Fallacy: Harm and Power in the Information Economy* (Cambridge University Press 2023) e.g. 78–80, 110 *et seq.*

³ I Cofone (n 2) 110 *et seq.*; K Havu, R Saleev, D Polad, D Pfau, T Heydari, and A Mäkelä, 'Regulating Liability for AI-Induced Harm: Developments in EU Law and Insights from a Research Project' (2024) Helsinki Legal Studies Research Paper, SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4861450 accessed 3 February 2025, 1–2, 9–18.

⁴ K Havu, 'Damages Liability for Non-Material Harm in EU Case Law' (2019) 44 *EL Rev* 492; K Havu, 'Litigation of Actions for Damages against EU Agencies: Challenges and Implications for Accountability' (forthcoming, 2025) in M Elantoni, H Hofmann and A Volpato (eds), *Agencies before the Court of Justice* (Edward Elgar).

⁵ 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) [2016] OJ L119/1.

⁶ E.g. Judgment of 14 December 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986; Judgment of 25 January 2024, *MediaMarktSaturn*, C-687/21, EU:C:2024:72; Havu et al. (n 3) 12–13.

material harm, which by definition is something other than economic harm,⁷ is a persistently vexing question. The matter of appropriate monetary compensation for non-material harm has also been fuzzy in the case law of the CJ, with the Court often just remarking that a specific amount of compensation is just without expounding any justifications for settling on that specific sum of money.⁸ The new wave of CJ preliminary rulings on the interpretation of the GDPR has nonetheless yielded several new developments, many of which are interesting from the standpoint of Cofone's arguments in *The Privacy Fallacy*. There is also CJ case law on harm to privacy beyond the scope of the GDPR. The following section analyses the new CJ judgments.

3. Compensating harm to privacy under the GDPR and beyond.

When it comes to privacy infringements, Article 82 GDPR has been the most important basis for claims in the European Union since the Regulation entered into force. Beyond the GDPR, harm to the privacy of individuals is expressly addressed only in national tort laws, and the approaches of the courts vary significantly across Member States. Preliminary rulings on the GDPR concern compensation for harm at the intersection of EU and national law. The GDPR establishes the principle that individuals who suffer non-material harm due to a data-protection infringement have a right to compensation, as per Article 82. Since national law supplements EU law in this area, EU law is neither comprehensive nor intended to be exhaustive. In recent years, the CJ has issued a number of preliminary rulings concerning the recoverability of (non-material) harm, offering guidance in relation to certain issues. These GDPR-based rulings from the CJ largely align with the previous case law on compensating non-material harm, and they offer clarifications rather than introducing significant jurisprudential novelties.

One long-awaited decision on the recoverability of non-material harm and the point at which harm becomes legally relevant under Article 82 GDPR was *Österreichische Post*⁹, which was handed down by the CJ in May 2023. An address broker company that was established in Austria had collected data on the political affinities of the Austrian population. The data were then sold to different organisations, enabling them to send out targeted advertisements. The claimant felt offended by the fact that an affinity for a certain political party was attributed to him and initiated legal proceedings, seeking an injunction and claiming €1000 in non-material damages for the harm that he had suffered. The court of first instance granted the injunction but rejected the damages claim.¹⁰ The court of appeal confirmed that decision, arguing that Austrian national law required a threshold of “seriousness” to be met for harm to be legally significant.¹¹

⁷ E.g. Opinion of AG Wahl of 9 October 2013, *Petillo*, C-371/12, EU:C:2013:652, paragraph 38.

⁸ *Havu* 2019 (n 4) 506–508.

⁹ Judgment of 4 May 2023, *Österreichische Post*, C-300/21, EU:C:2023:370.

¹⁰ *Österreichische Post* (n 9), paras 11-13.

¹¹ *Ibid.* para 14.

The Supreme Court of Austria submitted the case to the CJ for a preliminary ruling, asking, among other questions, whether the mere infringement of the rules of the GDPR was sufficient to trigger liability or whether additional harm was required. In addition, the Supreme Court asked whether the Austrian requirement that an infringement go beyond merely being upsetting before compensation could be awarded was compliant with EU law.¹²

The CJ clarified that the expressions “material and non-material damage” and “compensation for the damage suffered” must be interpreted as matters of autonomous EU law. Furthermore, it issued a reminder that the separate references to “infringement” and “harm” in the wording of the GDPR would be superfluous if a mere infringement would suffice as a basis for an award of damages.¹³ However, *Österreichische Post* did not provide the comprehensive clarification that could have been expected from the circumstances of the case. Despite the fact that the case provided the CJ with an opportunity to elaborate on the notion of “harm”, the Court did not provide any criteria for determining what constitutes actual harm that goes beyond a mere infringement of the GDPR.

Other GDPR preliminary ruling requests have also required the CJ to discuss the question of whether there is or whether there can be a “minimum threshold” for recoverable non-material harm. In *Ummendorf*, a national court inquired whether it is permissible to conclude that, when data subjects lose control over their data for a short period of time without experiencing a noticeable disadvantage or an objectively comprehensible impairment to their personal interests, there is no recoverable harm within the meaning of Article 82 of the GDPR. In response, the CJ explained that there is no “*de minimis limit*” that is applicable to non-material harm in the context of GDPR-based damages disputes and that EU law precludes the application of a Member State law that would lead to the rejection of a claim for compensation based on such a limit alone.¹⁴ This holding can be understood as affirming the proposition that any non-material harm to privacy is legally relevant and as an additional confirmation of the holding in *Österreichische Post*. At the same time, the requirement to substantiate harm limits compensation claims, in practice, which has both positive and negative implications. On the positive side, it ensures that purely speculative claims cannot succeed. On the negative side, the burden of proof might deter those who have legitimate claims from enforcing their rights. That having been said, it is generally difficult to define objective benchmarks for proving non-material harm, which, particularly in cases of privacy infringements, can be highly subjective. What one person perceives as a violation can still be acceptable for another.

On the whole, the GDPR preliminary rulings demonstrate that negative emotions, such as fear of one's personal data being misused or distributed, are recognised as legally significant forms of non-material harm.¹⁵ Claimants, however, bear the burden of proving harm. If harm manifests as feelings of

¹² Ibid. para 20.

¹³ Ibid. paras 30, 34.

¹⁴ Judgment of 14 December 2023, *Gemeinde Ummendorf*, C-456/22, EU:C:2023:988.

¹⁵ *Natsionalna agentsia* (n 6), paragraph 86; *MediaMarktSaturn* (n 6), paragraph 65.

fear, national courts are required to discover whether that fear is justified.¹⁶ Fear of entirely hypothetical threats does not constitute recoverable harm.¹⁷

It is worth noting that, in Germany, for example, the courts have stressed that awards of damages for non-monetary losses that arise from infringements of the GDPR need to be substantial enough to maintain the deterrent effect of the law and to respect the effectiveness principle.¹⁸ Ideas such as this one can have a notable impact on damages awards since the mere quantification of harm is difficult and valuing it requires judges to make subjective calls. Examining comparable cases is another possibility, although the case law on the GDPR is still rather limited.¹⁹

Returning to the CJ judgments, in a recent case of a different nature which concerned demands for compensation from the EU rather than claims heard by national courts, the CJ addressed a specific provision on the liability of Europol for the improper handling of personal data in situations that involve collaboration between itself and the Member States.²⁰ According to the description of the facts in the *Kočner* case, the claimant's "intimate conversations" were published by the press,²¹ which is obviously a matter of concern when the disclosure results from the manner in which the authorities have gathered and handled data for the purposes of an official investigation. In this case, the CJ confirmed that Europol was liable but, by setting compensation at €2,000, it indicated that CJ awards would tend to be modest.²² This finding accords with the prior CJ case law on non-pecuniary harm caused by the EU, in which limited or even nominal compensation is common.²³

Kočner suggests that the value which the law and the judiciary put to privacy is not necessarily the same as that which the harmed individuals attach to the confidentiality of their personal affairs.²⁴ However, in the context of the CJ and harm caused by the EU, the approach of awarding modest compensation is not limited to privacy-related harm but is also applied, for instance, in cases that revolve around a "state of uncertainty" that arises from excessively long court proceedings.²⁵ This similarity suggests that the approach of the CJ to determining suitable monetary compensation in cases of privacy-related harm is consistent with its treatment of other forms of non-material harm. In other words, there is no apparent tendency to specifically downplay harm to privacy. At this point, it seems that the CJ determines whether a data subject has

¹⁶ *Natsionalna agentsia* (n 6), paragraphs 84–85.

¹⁷ *Natsionalna agentsia* (n 6), paragraph 85; *MediaMarktSaturn* (n 6), paragraphs 68–69.

¹⁸ (OLG Dresden, ZD 2022, 159, para 12, after W Wurmnest, M Gömann, 'Comparing Private Enforcement of EU Competition Law and Data Protection Law' (2022) 13(2) JETL, 154-166)

¹⁹ (*ibid.* 173)

²⁰ Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L135/53, art 50; see also recital 57.

²¹ Judgment of 5 March 2024, *Kočner*, C-755/21 P, EU:C:2024:202.

²² *Kočner* (n 21), paragraphs 132–140, 146.

²³ Judgment of 14 June 1979, *V v Commission*, 18/78, EU:C:1979:154; Judgment of 23 January 2002, *Reynolds*, T-237/00, EU:T:2002:11; Judgment of 1 February 2017, *Kendrion*, T-479/14, EU:T:2017:48; Judgment of 13 December 2018, *Kendrion*, C-150/17 P, EU:C:2018:1014; *Havu* 2019 (n 4) 506–508.

²⁴ See also *Cofone* (n 2) e.g. 110–129.

²⁵ *Kendrion* (n 23); *K Havu and S Kurki-Suonio*, 'Damages Liability of the EU for Harm Caused by Excessive Duration of Court Proceedings' (2021) 27 EPL 305.

suffered actual harm on a case-by-case basis instead of establishing criteria of general application. The absence of such criteria will, in the short run, lead to more requests for preliminary rulings. It must be conceded that, given the rapid technological development of the recent years and the new methods of data gathering and data mining that have emerged, it would be very difficult to formulate future-proof criteria.

Some aspects of harm to privacy that occur in society remain largely undiscussed, let alone compensated.²⁶ Evidently, legal discourse often overlooks the aggregate incidence of such harm. Notably, cases such as Kočner, along with preliminary rulings on damages liability for GDPR infringements and similar compensation claims, tend to focus narrowly on the individual complainant. This approach inherently neglects critical questions about the broader ramifications of harm. For instance, the cases in point seldom consider who else may have been affected by the infringement, whether directly or indirectly. The entire extent of the harm that has been caused remains mostly unexamined. Furthermore, there is limited discussion of the measures that might be appropriate to remedy data-protection or privacy violations comprehensively. Cofone, as well as other authors, has correctly argued that what we can discern and remedy through individual-centric rules and court cases is not sufficient to address the entire problem of harm in the AI era.²⁷ Many instances of discrimination, unfavorable classification or unauthorized access to personal data likely go unnoticed by those affected.

4. Do we need to go beyond individual damages claims?

What kind of legal framework would tackle the harm that is caused in the information economy adequately? From the standpoint of EU law, Cofone seems to raise the highly salient point that the current legal rules are not sufficient to regulate harmful data practices. For instance, users have little or no control over the practice of inferring preferences and behaviours from data, and they are therefore insufficiently protected by the GDPR.²⁸ These inferences can consequently be used for profiling. The use of such analytics could lead to non-material harm for online users. Due to inference analytics, data which the GDPR does not protect in virtue of it being “special category data” (Article 9 GDPR) may suddenly fall within the scope of the Regulation when it is combined with other data. This could happen if, for instance, information on the user’s health condition is combined with detailed information on their food purchases or exercise regimen.²⁹

Harm prevention is, of course, a matter of great interest for the design of an optimal legal framework, but the same is also true of the development of

²⁶ Cofone (n 2) e.g. 110–129.

²⁷ Cofone (n 2) 110 *et seq.* See also e.g. G Nelson, ‘Risk-based Regulation and the EU AI Act’ (LSE Media Blog, 29 November 2024) <https://blogs.lse.ac.uk/medialse/2024/11/29/risk-based-regulation-and-the-eu-ai-act/> accessed 3 February 2025.

²⁸ S Wachter, B Mittelstadt, ‘A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI’ (2019) 2 *Colum. Bus. L. Rev.*, 495

²⁹ For a broader discussion on liability for data gathering see B Mäihäniemi, B Schütte, ‘Damages Liability Regimes for Unfair Data Gathering in the EU’ (2022) 29 *Concorrenza e Mercato*, 133-160

liability rules and compensation mechanisms. Some ideas have been presented, but none of them are perfect. For example, various types of no-fault compensation schemes, potentially supplemented with mandatory insurance policies for operators that engage in certain activities, can provide compensation to those who are harmed while minimizing strain on both the judicial system and the disputing parties. When instituting such systems, the main questions to consider should include the substantive scope of the compensation scheme. Furthermore, the schemes may need to be field- or activity-specific, which may make them burdensome for legislators.

One could also argue that the provision of compensation to an injured party should not always depend on them making proactive efforts, particularly when the existence of harm can be demonstrated through collective proceedings that assess broader contexts and probable impacts. In addition, an economic operator could be required to contribute a payment, similar to damages compensation, into a dedicated “compensation fund” when identifying all of the victims of a particular infringement is not feasible. This fund could serve as a financial resource to support harmed individuals, including those who are affected in cases in which the responsible parties are either insolvent or cannot be identified conclusively.³⁰

Finally, one could also consider moving away from the requirement that actual damage have occurred and consider the mere violation of GDPR data-processing rules sufficient to trigger liability. The EU legislator could resort to amending the relevant provisions of the GDPR. However, such a development would not accord with the traditional concepts and requirements of liability law, which are based on a harmful act or omission; damage; a causal link between the two; and, outside the of strict liability, the faulty behaviour of the wrongdoer.

This said, in discussions about adapting private law to the digital age, it is often stated that traditional liability rules can be ill suited to new technological developments. While this argument has often been made in relation to liability for damage caused by AI, given the difficulty of pinpointing the origin of the damage, one could equally argue that the advent of Big Data and the new dimensions of data gathering have rendered the original concept of liability, as it is embodied in the GDPR, inadequate. The deterrent effect of civil-liability rules could cause economic operators to comply more readily with the general rules of the GDPR, such as the principles that are set out in Articles 5 and 6, when they process data. Another argument in favour of abolishing the requirement of (proof of) actual harm is that, in many cases, the gathering of data can also affect third parties. Some years ago, it became known that social-media platforms such as Facebook were harvesting data from their users’ contacts even if they were not using the platform.³¹ Amending Article 82 GDPR so that separate damage is no longer required could also be seen as a potential avenue for reform that accords with the objectives of the GDPR, some of which are described in Recital 10 to the Regulation and were cited by the CJ in

³⁰ See e.g. Havu et al (n 3) 17–18.

³¹ See e.g. A Hern, ‘Facebook admits tracking users and non-users off-site’, newspaper article, The Guardian, 17 April 2018.

Österreichische Post.³² The objectives in question include ensuring a consistent and high level of protection for natural persons in the processing of personal data within the European Union.

5. Conclusion.

Judges often claim to be unable to assess harm to privacy, thus placing the burden on those who privacy laws ought to protect.³³ In its recent decisions, the CJ seems to have attempted to overcome this limitation of the judicial process. However, as mentioned above, so far, the Court has failed to establish dedicated criteria for determining whether actual harm has occurred or not. Against this background, one may also raise the question whether, given the current rate of technological development and the highly subjective nature of non-material harm, it is even feasible to establish such criteria. One core issue in privacy harm is that it is frequently unquantifiable, that is, that it is hard – if not impossible – to attach a price to it. Economic harm, such as loss of earnings, that occurs as a consequence of the same events as non-material harm is quantifiable but separate from the latter.

What is visible from the existing CJ judgments on harm to privacy is not a full framework but rather scattered individual ideas. This tendency results from the division of interpretative labour that frameworks such as the GDPR engender. However, at least some of the concerns which Cofone voices resonate with our findings from the overview of the case law. At the same time, remedying Cofone's concerns would require new approaches to information-economy harm, not just fine-tuning the outcomes of individual damages claims.

This is particularly important because, in today's information society, it is no longer appropriate to view an individual's personal data in isolation. Due to our inevitable online activities, we are connected to hundreds, sometimes thousands, of people. We need not even be active on social media to establish such connections. The web pages that we visit place cookies into our computers, enabling online service providers to gather information about the other web pages that we have been visiting and the individuals with whom we have been corresponding, supposedly all for the sake of providing us with the best possible service. Dark patterns and hyper-nudging frequently make it difficult for us to make informed decisions. Often enough, we are not even able to access certain information without consenting to cookies being installed on our devices. We are giving away not only our own personal data but also the data of the people with whom we interact, usually without being aware of this happening. Our choices, particularly online, affect us but also others, and we do not necessarily foresee their consequences. At the same time, corporations and authorities can collect a significant amount of information about us, profit from it, and sometimes even infringe our rights without being held accountable.

The linear, one-case-at-a-time approaches of the EU legislator have already been criticised in the field of technology regulation, for instance in the

³² See e.g. Österreichische Post (n 9), para 46-48.

³³ Cofone (n 2) 110.

literature on the risk-based approach of the AI Act, which is blind to interactions between different systems.³⁴ In the same way, one can criticise the purely linear, individualistic approach of the GDPR, which neglects the effect that the processing of one person's data can have on others. Furthermore, one could challenge the ideas that individuals can even discern how their data is used, determine whether their privacy has been infringed or know when they can claim compensation for it.

³⁴ See e.g. K Stuurman, E Lachaud, 'Regulating AI. A label to complete the proposed act on Artificial Intelligence, (2022) 44 Comput Law Secur Rev, 4.