The CJEU's Russmedia Judgment: Joint Controllership and Platform Responsibility for User-Generated Content

By Päivi Korpisaari

The Grand Chamber of the Court of Justice of the European Union (CJEU) delivered a significant judgment on 2 December 2025 in *X v Russmedia Digital SRL and Inform Media Press SRL*, (C-492/23; ECLI (EU:C:2025:935), later Russmedia), clarifying the responsibilities of online platforms publishing user-generated content containing personal data. The Court held that the operator of an online marketplace may qualify as a joint controller together with the user posting unlawful content and that the liability exemptions of the eCommerce Directive (2000/31/EC) cannot limit obligations arising under the GDPR. The ruling is likely to have important implications for online marketplaces and other platforms relying on user-generated content.

Facts

Russmedia operated the Romanian website publi24.ro, an online marketplace where users could publish advertisements either free of charge or for a fee. An unidentified third party published a false advertisement presenting the applicant as offering sexual services. The advertisement included photographs of her and her telephone number, published without her consent.

Although Russmedia removed the advertisement within approximately one hour of being contacted by the applicant, the content had already spread to other websites reproducing the advertisement. The applicant subsequently brought proceedings against Russmedia, arguing that the publication infringed her right of personal portrayal, privacy, and reputation, and her data protection rights.

Russmedia argued that it merely acted as a hosting provider benefiting from the liability exemption under the eCommerce Directive. The Romanian appellate court accepted that argument. The applicant then appealed further, contending that the GDPR applied independently of the eCommerce Directive and that Russmedia had played an active role in managing and disseminating content published on its platform.

The referring Romanian court asked the CJEU to clarify the relationship between the GDPR and the eCommerce Directive, particularly in situations involving manifestly unlawful and harmful content containing personal data.

The CJEU Confirmed the GDPR Obligations for Online Marketplaces

The Court first noted that the advertisement contained personal data because it included information identifying the applicant, such as photographs of her and her telephone number. It further held that the data belonged to the special categories of personal data under Article 9 GDPR, since the advertisement concerned the applicant's alleged sex life. The Court emphasised that even false allegations relating to a person's sexual life remain sensitive personal data deserving enhanced protection.[1] The CJEU further clarified that uploading and publishing the adver-

Päivi Korpisaari

1 See Grand Chamber judgment *Commission v. Poland* (independence and private life of judges and publishing the data on the internet), C-204/21, ECLI: EU:C:2023:442 and *ZQ v. Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts* ('an employee's health data'), C667/21, EU:C:2023:1022.

tisement constituted processing of personal data under the GDPR.[2]

The Court then proposed a broad interpretation of the concepts of 'controller' and 'joint controllers', in line with its earlier case law.[3] Although the unlawful advertisement had been created by an anonymous user, Russmedia also qualified as a controller because it influenced the purposes and means of processing.[4] In particular, the platform published advertisements for its own commercial purposes, retained extensive rights over user content in its terms and conditions, and determined important aspects of dissemination, such as presentation, visibility, and distribution. Accordingly, the Court considered Russmedia and the anonymous advertiser to be joint controllers, even though Russmedia had neither created the harmful content nor shared the advertiser's unlawful intentions.

The judgment follows the Court's earlier case law, according to which each entity regarded as a joint controller must independently satisfy the requirements of controllership by significantly influencing the purposes and means of processing in pursuit of its own interests. At the same time, the Court has repeatedly emphasised that joint controllership does not require equal responsibility or participation in every stage of processing. Joint controllers need not exercise equal influence, participate in all stages of processing, or even have access to the personal data concerned. What is decisive is the actual influence exercised over the purposes and means of the processing of personal data. It may therefore be argued that the Court has interpreted the concept of joint controllership broadly and functionally.[5]

The Court further emphasised that, under Article 5 GDPR, personal data must be processed lawfully, fairly, transparently, accurately, and securely, and that controllers must take reasonable steps to rectify or erase inaccurate personal data without delay.

Online marketplace operators are therefore subject to the GDPR's accountability obligations if they are controllers of personal data. Therefore, they must implement appropriate technical and organisational measures before publishing advertisements containing personal data, particularly special categories of personal data under Article 9 of the GDPR. The Court's reasoning strongly reflects the logic of Articles 5(2), 24, 25, and 32 of the GDPR, effectively extending 'privacy by design' obligations to the architecture and operation of online platforms themselves.

The Court has already previously emphasised the particularly sensitive nature of special categories of personal data and the need for strict safeguards concerning their processing.[6] In this case, the Court stated that where advertisements may contain sensitive personal data, platforms must identify such advertisements in advance, verify the identity of the advertiser, and determine whether the advertiser is the data subject or has obtained the data subject's explicit consent. If identity verification is not possible, or if explicit consent cannot be demonstrated, the platform must refuse publication of the advertisement.

The Court also held that platforms must implement technical and organisational security measures to reduce the risk that sensitive personal data published online will be copied and unlawfully republished on other websites. The Court nevertheless clarified that platforms are not strictly liable for every subsequent unlawful dissemination of personal data online and must be allowed to demonstrate that their security measures were appropriate.

Furthermore, the Court observed that Article 26 of the GDPR requires joint controllers to define transparently their respective responsibilities under the Regulation.

Finally, the Court held that online marketplace operators cannot rely on the liability exemptions stated in Articles 12 to 15 of the eCommerce Directive in order to avoid responsibility for infringements of GDPR obligations. According to the Court, liability exemptions under the eCommerce

2 Regarding the concept of processing personal data, see, for example, Grand Chamber judgment *OT v. Vyriausioji tarnybinės etikos komisija* ('the operation of loading personal data on an internet page constitutes processing'), C184/20, EU:C:2022:601.

3 According to GDPR Article 4 subsection (7), "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law" and according to the first sentence of GDPR Article 16(1) 'Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers'.

4 For example, in *Google Spain, S.L. y Google Inc. v. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* (C131/12), the CJEU interpreted Google as being a controller, even though a search engine such as Google does not control what is published on websites maintained by third parties.

5 See, for example, Grand Chamber judgmnet *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos v. Valstybinė duomenų apsaugos inspekcija,* C683/21, EU:C:2023:949 and Fashion ID, C40/17, EU:C:2019:629 and *Wirtschaftsakademie Schleswig-Holstein GmbH v Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, C-210/16, EU:C:2018:388.

6 For example, Grand Chamber judgment *OT v. Vyriausioji tarnybinės etikos komisija*, C184/20, EU:C:2022:601. See also note 1.

Directive cannot override or limit obligations arising under the GDPR. Even if a platform qualifies as an intermediary service provider, it must still comply with its own data protection obligations as a controller or joint controller.

The Court did not explicitly determine whether Russmedia qualified for the hosting liability exemption under the eCommerce Directive. Instead, it focused on the independent applicability of GDPR obligations, holding that intermediary liability exemptions cannot limit responsibilities arising under the GDPR.

Implications of the Judgment

Although the case formally concerned the eCommerce Directive, the reasoning is likely to have broader relevance under the Digital Services Act ('DSA'), which retained the core intermediary liability framework of the earlier directive. The judgment suggests that intermediary liability exemptions available to platform operators cannot limit obligations arising under the GDPR. Moreover, Article 2(4)(g) of the DSA expressly provides that the Regulation is without prejudice to Union law on the protection of personal data, in particular the GDPR and the ePrivacy Directive (Directive 2002/58/EC). This further supports the view that intermediary liability exemptions under the DSA cannot displace or limit obligations arising under EU data protection law.

More broadly, the judgment reflects an ongoing shift in EU digital law away from purely reactive notice-and-take-down systems, which are used, for example, to address copyright infringements, toward a more active model of platform responsibility. GDPR compliance obligations may already arise at the service-design stage, meaning that the architecture of digital platforms itself may be relevant when determining the legal status of the parties involved and the corresponding obligations under the GDPR.

The judgment therefore appears to move platform compliance from a primarily reactive model towards ex ante risk prevention and "preventive vigilance". Platforms enabling user-generated content may increasingly be expected to bear responsibility for the fundamental-rights risks inherent in the structure and functionalities of their services.

At the same time, the judgment should not be interpreted as establishing a general obligation to monitor all user-generated content. The decisive factors in the Court's reasoning were the presence of manifestly sensitive personal data under Article 9 of the GDPR, the obvious harmfulness of the content, the anonymous nature of the publication – which made it difficult, in practice, to hold the original author accountable – and the platform's structural role in enabling the dissemination and reuse of that content for its own commercial purposes.

Nevertheless, the obligations imposed by the Court create a certain tension with the prohibition on general monitoring obligations under EU intermediary law. In practice, ex ante identification of sensitive personal data may require automated screening systems or extensive moderation mechanisms capable of reviewing content before publication. At the same time, it would likely be impossible, in practice, to design an online platform or marketplace in a manner that entirely prevents the further dissemination or republication of content by third parties once published online, particularly given the ease with which digital content may be copied, captured, reproduced, and redistributed by users.

The case thus encourages platforms to adopt stricter identity verification systems and to limit anonymous publication. This creates a notable paradox: stronger protection of privacy and personal data may simultaneously incentivise platforms to collect more user identity data in order to reduce legal risk.

The judgment therefore raises important questions about the balance between freedom of expression, the right to private life, and the protection of personal data. This is particularly significant given that anonymous expression may itself constitute an important dimension of both freedom of expression and private life. Anonymity may enable individuals, for example, to seek peer support or information relating to illnesses, personal relationships, or sexual orientation without fear of stigma or exposure. More broadly, the ruling raises significant questions about the underlying logic and principles governing the regulation of digital platforms and online interaction in EU law.

The judgment may further contribute to a two-tier model of platform responsibility. Traditional notice-and-action procedures may remain sufficient for many forms of 'ordinary unlawful content', whereas content involving special categories of personal data may trigger significantly stricter ex ante obligations under the GDPR.

The significance of Russmedia's terms and conditions also remains noteworthy. The Court repeatedly referred to the platform's extensive contractual rights to use, distribute, reproduce, and commercially exploit user content. It therefore remains uncertain to what extent the finding of joint controllership depended on those particularly broad rights clauses. Platforms exercising more limited rights over user content might not necessarily qualify as joint controllers in the same way.

One notable aspect of the judgment is that the Court did not expressly rule on whether Russmedia fell within the scope of the hosting liability exemption under the eCommerce Directive. One particularly significant observation is that it may

reasonably be argued that the case did not concern a purely neutral hosting service. Russmedia did not merely passively store third-party content; rather, its core business activity consisted of publishing and disseminating third-party advertisements for commercial purposes. Moreover, the platform's terms and conditions appear to have granted Russmedia extensive powers over the publication, removal, distribution, and commercial exploitation of user-generated content, further distancing its role from that of a purely neutral intermediary.

It is also noteworthy that the GDPR's journalistic exemption under Article 85 does not appear to have been invoked in the proceedings. The implementation and scope of that exemption also vary considerably between Member States.[7] In any event, reliance on the journalistic exemption would have been fundamentally incompatible with Russmedia's own argumentation that it merely acted as a neutral hosting service provider within the meaning of the eCommerce Directive. Consequently, the judgment does not provide a comprehensive answer applicable to all forms of online publication, particularly journalistic and editorial contexts involving freedom of expression considerations.

In this respect, it is important to understand that digital platforms are often neither purely passive hosting services nor traditional publishers or editorial actors. Rather, they occupy an intermediate position and exercise significant structural power through, for example, algorithms, visibility management, moderation practices, and terms of service. From this perspective, platform responsibility may no longer be meaningfully assessed through a dichotomous model in which an actor is regarded either as a hosting provider benefitting from liability exemptions or as a publisher bearing full editorial responsibility for content.

Colourbox

The judgment additionally leaves several practical and doctrinal questions unresolved. The Court did not clarify the precise scope of liability for subsequent republication of unlawful content by third parties, nor did it explain when downstream dissemination may break the chain of causation for damages purposes. The Court nevertheless observed that the loss of control over personal data originated from the initial unlawful publication of the harmful advertisement in breach of the GDPR. The ruling therefore leaves substantial uncertainty regarding compensation claims under Article 82 GDPR in situations where information rapidly spreads across multiple online services.

Moreover, the Court imposed demanding compliance obligations without fully clarifying what level of identity verification, screening, or anti-copying measures should be regarded as sufficient or proportionate in practice. Considerable uncertainty therefore remains regarding how platforms can operationalise these obligations in technically and economically realistic ways. The broad and functional interpretation of joint controllership adopted by the CJEU may also create uncertainty concerning the allocation and limits of responsibility in complex digital platform environments involving multiple interconnected actors.[8]

The judgment may also incentivise platforms to remove or block

7 See Päivi Korpisaari, 'The journalistic exemption in personal data processing'in Taina Pihlajarinne & Anette Alén-Savikko (eds) *Artificial Intelligence and the Media: Reconsidering Rights and Responsibilities* (2022) 61–91.

8 Regarding the latter, see Benjamin Wong, 'Problems with controller-based responsibility in EU data protection law' (2021) *International Data Privacy Law, Volume 11, Issue 4,* 375–387.

lawful but potentially sensitive content more aggressively in order to minimise regulatory exposure. Consequently, the ruling may indirectly affect freedom of expression, anonymous speech, whistleblowing, and access to information online.

The judgment appears consistent with broader academic discussions according to which responsibility in platform environments increasingly stems from the functional role actors play in shaping dissemination, visibility, and interaction rather than merely from formally defined intermediary categories.[9]

Finally, Russmedia reinforces a broader trend in European law: responsibility increasingly follows platforms' actual influence over the conditions under which digital content is created, organised, moderated, and interacted with online, as well as over the dissemination architecture, visibility, and amplification of such content. In this respect, the judgment resembles the broader approach adopted by the European Court of Human Rights in the Grand Chamber judgments Delfi AS v. Estonia (Application no. 64569/09), concerning civil liability for unlawful user comments, and Sanchez v. France (Application no. 45581/15), concerning criminal liability relating to user-generated content.[10] Russmedia may therefore prove to be an important step in the development of EU digital law towards a model in which platforms that actively structure, disseminate, and commercially exploit user-generated content may bear increasing responsibility for the fundamental-rights risks connected to such activities. The judgment also reflects a broader understanding according to which digital infrastructures and technical architectures are not neutral, but actively shape the dissemination of information and the allocation of risks and responsibilities online.[11]

> Russmedia may therefore prove to be an important step in the development of EU digital law towards a model in which platforms that actively structure, disseminate, and commercially exploit user-generated content may bear increasing responsibility for the fundamental-rights risks connected to such activities.

Päivi Korpisaari is Professor of Communication Law at the University of Helsinki. Her research focuses on media and information law, data protection, constitutional and human rights law, tort law, and legal questions relating to new technologies and artificial intelligence. She has led several research projects and serves in multiple national and international expert positions, including the Council of Europe's Access Info Group.

9 See, for example, Natali Helberger, Jo Pierson & Thomas Poell, 'Governing online platforms: From contested to cooperative responsibility' (2017)*The Information Society*, 34, 91–14 and (very critical) Tobias Mast, 'Responsibility in the Platform Quadrangle: Balancing Rights between Content-Creating Users, Internet Service Providers, Affected Parties and Recipients; Also a Case Note on CJEU Russmedia, Case-492/23, [2025] ECLI:EU:C:2025:93' (2025) working paper, https://doi.org/10.21241/ssoar.108734

10 For further discussion, see Päivi Korpisaari 'From *Delfi to Sanchez* – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the Digital Services Act' (2022) *Journal of Media Law, 14*(2), 352–377 and Päivi Korpisaari 'Sanchez v France: ECtHR judgment raises questions about a politician's liability to moderate his own Facebook "wall"' (2023) *Journal of Media Law,* 15(2), 140–151.

11 See Thomas Poell, David Nieborg, and José van Dijck,'Platformisation' (2019) *Internet Policy Review,* 8(4).