GIVE YOUR DATA DEARLY – BRIEF ANALYSIS OF THE LATEST JUDGEMENT IN THE SCHREMS V. META IRELAND PLATFORMS CASE

Csík Aurél*

Abstract

The more modern technology develops, the more valuable our data becomes. Direct marketing that reaches users directly has reached unprecedented proportions. Today, most direct marketing activities on the internet are spread across social media sites, using the personal data of those who use them. The Schrems v. Meta Ireland Platforms case highlights the dangers of giving social media service providers control over our data and what we can do to prevent them from misusing the sensitive information about us.

Keywords: Social Media, European Union, data, GDPR, direct marketing

1. Introduction

The achievements of the information society are hammering nails ever deeper into the coffin of human autonomy. Social media platforms have become not just communication tools for us, but complex digital ecosystems in which expression, identity building, social interaction all take place in a single website. In this real-time, algorithmised space, the question of where the boundary lies between the self-determination of individual rights and the economic interests of platform providers is highly relevant.

The case of Max Schrems v Meta Platforms Ireland is a landmark case in this aspect. In a judgment handed down in October 2024, the Court of Justice of the European Union (CJEU) took a clear position on the EU law treatment of data processing in the context of online targeted and direct advertising practices, with particular emphasis on the treatment of sensitive personal data. The judgment has not only had implications for Meta in principle and in practice, but has also set a precedent for the interpretation of the balance of fundamental digital rights.

Max Schrems, an Austrian data protection activist and lawyer, has been in the spotlight several times over the past decade after playing a key role in the invalidation of the EU data transfer mechanisms Safe Harbour (C-362/14) and Privacy Shield (C-311/18). In the present case, he complained that Meta used his and several European users' particularly sensitive personal data, including information on sexual orientation, political affiliation or ethnicity, to distribute direct advertising without his consent.

The aim of this paper is to provide a brief legal analysis of the judgment, with a particular focus on how it strengthens the regulatory logic of the GDPR. The paper pays particular attention to how the judgment interprets the notion of „sensitive data" in the digital context and how it can be used to draw general conclusions about the limits to freedom of expression online - especially when data reflect not only opinions but also personality profiles.

* Aurél Csík, PhD student, fourth year, University of Miskolc Deák Ferenc Doctoral School in Law and Political Sciences, Department of Constitutional Law, 3515 Miskolc-Egyetemváros, acsik96@gmail.com

2. Max Schrems v. Meta Platforms Ireland

In the following, I will analyze the judgment of the Court of Justice of the European Union in preliminary ruling proceedings C-446/21, delivered on October 4, 2024[1]. However, first of all, I would like to introduce the parties involved.

2.1. The parties of the case

The case, which was closed last October, has its roots in 2013, when Edward Snowden disclosed documents from the National Security Agency (NSA) showing that US intelligence agencies were monitoring people's mobile phone use and internet activity around the world. The documents, which were leaked by Snowden have fundamentally shaken trust in the state to handle sensitive data. This fear is not unfounded, as the United States (which remains the most powerful country in the Western world) is also home to most of today's most influential tech giants (Alphabet, Meta, Amazon, etc.), which have access to immense amounts of data every day.

Austrian activist Max Schrems - following in the footsteps of Edward Snowden - saw the potential dangers and used the tools provided by law to address them. Schrems submitted a request[2] to Ireland's Data Protection Commissioner[3] in 2013, asking the country to block Facebook's data transfers to the US. In his application, Schrems argued that the protection of his data was, in his view, insufficient to prevent abuse. The application was triggered by a judgment of the Court of Justice of the European Union (CJEU) (Schrems I, 2015), which annulled an earlier (2000) decision of the European Commission in favour of the United States on the subject matter. A year later, the EU issued a new decision (Privacy Shield) which, in Schrems' view, failed to remedy the problems outlined in the earlier proceedings, leading to a new judgment of the CJEU (Schrems II, 2020) which terminated the existing Privacy Shield between the EU and the US. The CJEU applied a similar logic in this judgment as in Schrems I: the US does not follow EU data protection rules and does not provide EU citizens with sufficient protection against US authorities to safeguard their data.

The other party in the case was Meta Platforms Ireland Limited, which is the controller of personal data of users of Facebook and other related platforms (Instagram, WhatsApp) in the EU. On 6 November 2023, Meta introduced a new subscription model on the social media platforms it owns. As of that date, the services provided by Meta remained free of charge only to users who consented to the use of their personal data by Meta for direct marketing purposes. If someone wanted to keep their data safe or wanted Meta's former customer service to remain available, they had to pay for it. It is important to point out that the social media platforms under Meta (Facebook being the most prominent among them) are heavily dependent on advertising systems personalised to users, which operate on the basis of profiling. Under the terms and conditions, this data includes information on users' activities inside and outside the social network, which is linked to the Facebook accounts of the users concerned. Meta collects this data through cookies and various social plugins, the most well-known (and, according to Facebook's algorithm, the most important) of which is the „like" button. Based on these, the algorithm displays content on Facebook in the timeline tailored to the user.

[1] C-446/21 Maximilian Schrems v Meta Platforms Ireland Limited ECLI:EU:C:2024:834 (CJEU)
[2] Natasza, GADOWSKA: Schrems Saga: Weighing Collective Security Against Individual Privacy, https://jolt.law.harvard.edu/digest/schrems-saga-weighing-collective-security-against-individual-privacy (2025. 07. 19.)
[3] Most tech giants have established branches in Ireland within the European Union, so Facebook (now known as Meta) also has its local jurisdiction in Ireland.

2.2. The main proceedings

One of the main problems of Schrems with this system was that these „plug-ins" could be found on sites that would allow for far-reaching conclusions to be drawn about Schrems' political and sexual orientation in the event of profiling. Schrems did not, for this reason, consent to Meta Platforms Ireland collecting data about his internet activities outside of Facebook for the purpose of serving personalised advertisements, but it did collect data through the use of cookies and plug-ins embedded in third-party sites, which it used to serve ads tailored to Schrems on his timeline. It is also clear from the proceedings that Schrems is aparticularly aware Facebook user: his activities are only visible to his friends, and his list of friends is not public. The proceedings also show that Schrems openly admits his homosexuality but does not disclose it in any form on his Facebook profile. It is therefore clear from the background to the case that Schrems' main concern about the data processing of Meta Ireland Platforms is that, regardless of the user's consent, the site also accesses data that, on the one hand, is not generated on one of the platforms covered (Facebook, Instagram, WhatsApp) and, on the other hand, may contain particularly sensitive personal data (including political and sexual identity).

The main case was brought before the Landesgericht für Zivilrechtssachen Wien (Regional Court for Civil Matters in Vienna). In the proceedings, Schrems alleged that Meta Platforms Ireland had breached several provisions of Regulation 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (General Data Protection Regulation, also known as the GDPR), namely Articles 6(1), 7 and 9. These articles primarily address the fact that the processing by Meta Platforms Ireland is subject to a consent which it has not obtained from Schrems in advance, and thus Meta Platforms Ireland has consistently breached or is in breach of the cited provisions of the GDPR. Meta Platforms Ireland, on the other hand, defended that Schrems' data was processed in accordance with the terms of use of the community site, which were drafted in accordance with the GDPR and therefore did not breach its rules.

The Oberster Gerichtshof, to which Schrems has applied for review, points out that Meta Ireland Platforms' services are centred on an advertising system based on the preferences and interests of the users, and that Meta therefore derives the majority of its revenue from the processing of users' personal data. And since this processing allows Meta to offer free services to users, it can be considered necessary for the performance of the contract with those users within the meaning of Article 6 (1) b) of the GDPR. However, according to the Oberster Gerichtshof, that provision, which must be interpreted restrictively, does not allow such processing without the consent of the user concerned. The Oberster Gerichtshof further notes that Meta Platforms Ireland processes personal data that can be qualified as 'sensitive' under Article 9 (1) of the GDPR. The Oberster Gerichtshof referred four questions to the Court of Justice of the European Union. The first question concerned the interpretation of the provisions of Article 6 (1) a) and b) of the GDPR, in particular whether contractual provisions in the general terms and conditions of use for online platforms in relation to similar contracts at issue in the main proceedings (in particular contractual provisions such as: „*Instead of paying (...), by using Facebook products covered by these Terms, you agree that we may display ads to you (...) Your personal data (...) will be used to display ads to you that are more relevant to your interests.*„), which involve the processing of personal data for the purposes of aggregating and analysing data for the purposes of personalised advertising, must be assessed on the basis of the requirements of Article 6 (1) a) of the GDPR read in conjunction with Article 7 of the GDPR, which cannot be replaced by reference to Article 6 (1) b) of the GDPR. The second question

concerned the interpretation of Article 5 (1) c) of the GDPR (data minimisation) as to whether all personal data held by a platform such as the one at issue in the main proceedings (in particular through the data subject or through third-parties using the platform and outside the platform) can be aggregated, analysed and processed for the purposes of personalised advertising without any limitation in time or type of data. The third question was asked in relation to Article 9 (1) of the GDPR, which focused on whether this provision should apply to processing that allows for the filtering of special categories of personal data, such as political opinion or sexual orientation, for specific purposes (e.g. for advertising), even if the controller does not distinguish between these data. The last and fourth question was asked in the context of Article 9 (2) e) of the GDPR, whether Article 5 (1) b) of the Regulation should be interpreted as meaning that a statement made for the purpose of a panel discussion about one's own sexual orientation allows other data relating to sexual orientation to be processed for the purpose of aggregating and analysing data for the purpose of personalised advertising.

Following the judgment of the Court of Justice of the European Union of 7 April 2023, the Oberster Gerichtshof withdrew two questions - the first and the third - so that the Court of Justice only had to answer the second and the fourth question on the substance.

2.3. The answers to the questions

As regards the second question, the Court examined whether the principle of „data minimisation" provided for in the GDPR precludes the operator of a social media platform, as data controller, from aggregating, analysing or processing personal data obtained from the data subject or from third-parties for advertising purposes.

The defendant in the main proceedings objected to the question because, in its view, the referring court had not sufficiently demonstrated why it would be useful to answer the question for the purpose of resolving the dispute. The defendant also pointed out that the referring court had wrongly concluded that it was using all personal data for advertising purposes without any limitation as to time or the nature of the data. The Court disagreed with the defendant's reasoning, first, because the application clearly showed the relevance of the issue to the resolution of the case and, second, because the referring court must examine the merits - and necessity - of the issue in the main proceedings, and it is therefore not within the jurisdiction of the Court of Justice of the European Union to consider it. The Court of Justice of the European Union has therefore concluded that the second question is answerable.

In the context of the second question, the Court underlines that, in the light of Article 23 of the GDPR, the data controller must comply with three criteria for the processing of personal data: it must comply with the principles – which must be interpreted together – set out in Article 5 of the GDPR, it must fulfil the conditions set out in Article 6 and it must respect the rights of the data subject under Articles 12 to 22. Of these, the Court examined in particular the principles set out in Article 5. The first principle is that personal data must be processed fairly and lawfully and in a way which is transparent to the data subject, and that data must be collected for specified, explicit and legitimate purposes. The next principle is the „principle of data minimisation", which implies that processing must be adequate, relevant and limited to what is necessary for its purposes. The Court has underlined in this principle that the controller must process the data subject's data for as short a period as possible, since the longer the processing, the greater the impact of the processing on the interests and privacy of the data subject. The principle of data minimisation is also linked to the fact that data processing should not be of a general nature and should refrain from collecting data that are not strictly necessary. The third principle addressed by the Court is the principle of accountability, which means that the controller must, on the one hand, demonstrate that the data from the data subject are processed

in accordance with the principles mentioned above, but also provide information on the purposes for which the data are intended to be processed and the legal basis for the processing. In response to the second question, the Court of Justice has ruled that the principle of „data minimisation" is countered by the use of data collected from the data subject or from third-parties for advertising purposes without time limits. In support of this, the Court of Justice has used several previous judgments.

The fourth question was based on an interesting analogy. The question asked whether a data subject who openly discussed his sexual orientation in a panel discussion independent of the controller, could authorise the controller to collect data on the data subject's sexual orientation. The Court underlined that Article 9(1) of the GDPR enshrines the principle of the prohibition of processing of the special categories of personal data referred to therein. These include personal data revealing racial or ethnic origin, political opinions, religious beliefs, health data and – in respect of this case – personal data concerning the sex life or sexual orientation of persons, but, in relation to the derogation provided for in Article 9(2) e), it should be recalled that, under that provision, the prohibition on processing special categories of personal data laid down in that Article 9 (1) does not apply where the processing relates to personal data „which have been explicitly made public by the data subject". In the light of the above mentioned, the answer to the fourth question is that GDPR 9. Article 9(2) e) must be interpreted as that a person has spoken about their sexual orientation in a public panel discussion does not entitle the operator of an online social networking platform to process data relating to that person's sexual orientation, which it may obtain from third-party partner applications and websites outside that platform for the purposes of aggregating and analysing that data in order to offer him or her personalised advertising.

3. Summary

In its judgment, the Court of Justice of the European Union confirmed that Article 9 of the General Data Protection Regulation (GDPR) clearly prohibits this type of processing unless the data subject gives his or her explicit consent. The Court stated that mere registration of users or use of the platform cannot be interpreted as „unambiguous consent" to the use of sensitive data for profiling purposes. This finding could have far-reaching consequences not only for Meta, but for any digital service provider that builds targeted advertising on personal profiles.

The significance of the decision beyond this lies in its redefinition of the relationship between expression and privacy in the digital space. Social media platforms have become a major arena for social discourse, where individuals not only consume information, but also shape identities, form political opinions and, last but not least, try to maintain the boundaries of their own privacy. The Court's judgment serves to reinforce these boundaries by making it clear that the exercise of fundamental rights in the digital space cannot be a purely technical or commercial matter.