Pregledni rad
UDK 316.77:004.738.5
DOI 10.7251/BLCZR0623019C

PERSONAL DATA PROCESSING BY SOCIAL MEDIA - NEW PERSPECTIVE IN META PLATFORMS CASE

Jasna Čošabić[1]

SUMMARY

Digital era has brought enormous changes not only to IT sphere, but also to media, especially social media, who strive to make their economic growth by collecting data of its users. How or if these users willingly give their personal data is questionable and subject to strict requirements of the new data protection legislation, which made its way in the EU especially since the GDPR has entered into force. The consent for processing of personal data of private subjects is multilayered and depends upon various features such as type of data, its sensitivity, but also upon the mode of giving such a consent. Whether direct or indirect, consent must contain certain prerequisites, so that the processing of that data would be considered as lawful. The more pronounced the value of personal data for a subject processing and using that data, the more thorough the legal requirements should be, especially when it comes to new forms of predictable behaviour, used for behavioural advertising, for example. The new judgment in the case of Meta Platforms[2] *gives a new light to data protection law, especially in social media sphere, widening its concept to competition law, dominant position of social media networks and antitrust policies.*

KEYWORDS: *privacy, lawfulness, legal informatics, data protection law, consumers´ personal data, social media*

PERSONAL DATA, CONSUMERS´ PERSONAL DATA AND SOCIAL MEDIA PLATFORMS

Personal data, according to Article 4 of the General Data Protection Regulation ('GDPR'), means any information related to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The European Court of Human Rights (´ECtHR´) has already emphasised the importance of extensive interpretation of personal data as any information relating to an iden-

1 Dr. iuris Jasna Čošabić, CIPP/E, Prodinger & Partner Wirtschaftstreuhand-Steuerberatungs GmbH & Co KG, www.linkedin.com/in/jasna-cosabic

2 The Court of Justice of the European Union, Judgment of the Court (Grand Chamber) of 04 July 2023 (request for a preliminary ruling from the Oberlandesgericht Düsseldorf-Germany) – Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd, Facebook Deutschland GmbH v Bundeskartellamt, Case C-252-21, Meta Platforms and Others (General terms of use of a social network)

tified or identifiable individual, in Amann v. Switzerland and Rotaru v. Romania cases. (Amann v. Switzerland, 2000.)

The Court of Justice of the European Union (´CJEU´) has took the important standing in extending the notion of personal data, considering that a dynamic IP address registered by an online media services provider, when a person accesses a website that the provider makes accessible to the public, constitutes personal data, in relation to that provider, ´where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person'.[3]

Consumers' personal data that is willingly or unwillingy stored at the social media platforms, enables these platforms to use such data, inter alia, for targeted advertising.

Targeted advertising is closely connected to profiling which is aimed in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements'[4]. Individuals have the right not to be subjected to automated processing of personal data, including profiling, especially when such a profiling would have legal effects to those individuals. (Leenes R., Van Brakel R., Gutwirth S., De Hert P., 2017). Automated processing with the aim of profiling and targeted advertising may collect data from individuals on be basis of visiting certain web sites such as online shopping sites or social media, that would, based on consumers´ search for products, create offers that would reach those consumers in a form of popup messages or a variety of other means.

Behavioural advertising is defined as the practice of tracking an individual's online activities to deliver advertising tailored to the individual's interests[5]. But tracking of individual online activities can have a far-reaching impact not only the creation of targeted advertising towards those individuals. Free psychological tests, offered often on social media, give more complex data results then what individuals participating in those tests may envisage. They may have impact on political debate and public society (See Chen Jiahong) and the consumer behaviour may give a clue to economic tendencies more then consumers may be aware of.

PROCESSING OF PERSONAL DATA

Processing, according to Article 4 of the GDPR means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing has to be in accordance with the principles of lawfulness which presupposes not only formal lawfulness but a substantive as well. Pure mathematical equation with law is not enough, but the law must have certain qualities such as adequately accessible, formulated with sufficient precision to enables citizens to regulate their conduct to be able – if

3 Judgment of the Court (Second Chamber) 19 October 2016 (*) In Case C 582/14, interpretation of 'article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

4 According to Recital 71 of the GDPR

5 FTC Staff, Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf, p. i

need be, with appropriate advice – to foresee, the consequences which a given action may entail. This concept was established also by the case-law of the ECtHR in the case of Sunday Times v. the United Kingdom.[6] Foreseeability of the consequences is also inherent to first of six preconditions of lawfulness provided for by GDPR (Article 6), which is consent for processing. Legal certainty is a general principle of the EU legislation, contending that the law must be clear and precise with its legal implications foreseeable.

We could interpret this concept so that the citizens, by consenting to giving their personal data, also as consumers at social media platforms, must be able to apprehend what is happening with their data, how their data shall be used by such platforms and also by other web entities that are connected to platforms, and to be able to control the use of their data. Given the flow of personal data on social media platforms and the economic value of personal data to those web entities, it is understandable that the scrutiny or control of the use of such data should be extensive.

MAIN FEATURES OF ´´CONSENT´´

The consent of a person for the use or processing of his or her data must be freely given, specific, informed and unambiguous indication of the data subject's wishes. [7]

Lack of the attributes of the consent, such as freely given, specific, informed and unambiguous, may lead to violation of the lawfulness principle of the GDPR.

The consent was already a subject of ruling of the ECtHR in the case of Barbulescu v. Romania[8], where Mr. Barbulescu did not receive any warning, by his employer, of the possibility that his communications might be monitored or read, nor had he given any consent in that regard. In this case, the employer has monitored the applicant's private e-mail and SMS account and has dismissed him as a consequence of using the computer for his private purposes during the working hours. European Trade Union Confederation, took the view in this case that the 'consent or at least prior notification, of employees was required, and that staff representatives had to be informed, before the employer could process employees' personal data.'

Moreover, only prior information might not be enough, when speaking of the consent. In the case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland of June 2017[9], the ECtHR took the view that the fact that data subjects had been informed that their data might be made public was not sufficient to establish that they had given their consent to its publication.

Freely given consent is a prerequisite that requires the free and undisturbed will of the data subject. In order for the consent to be free, data subject must not feel pressured, or urged to consent, or subjected to non-negotiable terms, making him unable to refuse giving the consent without detrimental effect to him, according to WP29 Guidelines on consent[10]. He must not be deceived, or conditioned by obtaining goods or services, upon placement a consent.

6 See the European Court of Human Rights, Judgment in the case of Sunday Times v. The United Kingdom of 24 October 1991

7 Article 4 (11) of the GDPR

8 European Court of Human Rights, Judgment in the Case of Barbulescu v. Romania of 5 September 2017

9 European Court of Human Rights, Judgment in the Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland of 27 June 2017

10 Article 29 Data Protection Working Party, adopted on 28 November 2017

Not freely given consent appears when there is an imbalance of powers between the data subject and controller and stems out from inequality of parties in a contract. If one party is a public authority it is unlikely that the consent was freely given, according to Rec (43). So, when the public authority is a controller, the consent might not be the best option. Other grounds for lawful processing such as contract, or legal obligation may be adhered to.

Withdrawing consent should be easy and freely just like giving consent. According to Article 7, para 3 of the GDPR, the data subject has the right to withdraw consent at any time. The effect of withdrawal is ex Nunc, or forward from the date of withdrawal, not affecting the processing which occurred prior to withdrawal. In that regard, the withdrawal is not going to affect the lawfulness of processing based on consent before the withdrawal. Data subject must be informed of possibility of withdrawal of consent, before giving it.

In order that processing is considered lawful, consent must be specific. The wording of consent must not be vague, abstract, or extensive. It must be related to certain processing and must be specific in that sense, not leaving room for wider interpretation of consent[11]. Consenting to the use of cookies should not mean consenting to using a geolocation for example. If a person has consented to the use of cookies, by opening a web site connected to a social media platform, he should not expect other similar websites to contact him and to have his data. In the wide spread net of the web entities connected to a social media platforms, this could open many possibilities to unlawful use of one´s data.

In that sense, in order to avoid any form of deception, mislead or misconception, a person giving consent or a data subject must be informed about what consent implies its scope and consequences. Data subject has to be informed about who is controller, what kind of data processing shall follow upon consent, for how long, etc.

Consent has to further be unambiguous, or given beyond any doubt, and this feature comes as an upgrade to all features mentioned above. The will of the data subject has to come in a clear statement or affirmative action by which he or she allows the processing of personal data.

Affirmative action has to be clear enough, while the mere visiting a website does should not suppose the consent to use personal data. This has also to do at a greater extent with technical prerequisites, which may, according to Recital 32 of the GDPR, include ticking a box when visiting an internet website, choosing technical settings, and may be a part of privacy of design concept in providing compliance with the consent requirements in the GDPR. In the world of fast-moving digital technologies, when various internet actions occur in every millisecond, it is normal that, due to a number of providing consents, we shall face a great majority of consents that are technically prepared, according to a certain format, respecting all the above requirements for the consent to be lawful, and in a plain and simple language..

CONTRACT AND SOCIAL MEDIA

Another aspect of lawfulness is processing stemming out from a contract to which data subject is a party.

Processing is lawful if it is 'necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering

11 Recital 32 of the GDPR

into a contract', according to Article 6, 1 (b) of the GDPR. Being a party to the contract, is still one form of consent. Free will when entering contracts is one of the prerequisites for the legality of contracts, and in the absence of free will the validity of the contract may be questioned, and sometimes denied at the outset. Just like the consent has to be undisturbed, free, in which the choice of the party is undisputable, so is the case with the contract. As to the formulation 'necessary for the performance of a contract' WP29 has again stressed that that term is to be interpreted strictly, as well as that there must be a 'direct and objective link' that connects the processing of data and exercise of the contract. But consent and contract cannot be tied together. The contract cannot present a legal ground for processing a sensitive data, for which an explicit consent is required.

Contract is another way of demonstrating free will of the data subject. While in the consent case, the data subject's consent is visible and unambiguous, and controller's consent for processing is presupposed, in case of a contract, both parties express their will by entering into contract. Accordingly, contract may be a lawful ground for processing personal data, in so far as it is needed for the fulfilment of the contract itself. Therefore, the consent and contract are both forms of providing a wish for processing of data, by data subject, according to the GDPR, but are still two separate grounds for processing. The form of contract is in writing including in electronic form. The contract can also be a ground for transfer of data to a third country or international organization, pursuant to Article 49, 1 (b).

Contract is one of the grounds for processing personal data when it comes to social media networks.

According to Facebook Data Processing Addendum, users authorise 'Meta' to subcontract its data processing obligations. 'Meta shall do so only by way of a written agreement with such sub-Processor which imposes the same data protection obligations on the sub-Processor'[12].

The wide spread of social media networks has led to changes in both technology, including law regulating technology and market. The fast growth of social media has crystallized some of them holding a dominant position in market. The recent judgment in the Meta Platforms connects the rules governing dominant position in market with data protection rules. It makes the new ground for correlation of the two important segments of society, information technology law and antitrust and competition law in order to strengthen the protection of personal data.

According to the said judgment, the competition authority of a Member State can find, in the context of the examination of an abuse of a dominant position, that the terms of use relating to the processing of personal data are not consistent with the data protection requirements. It should be applied when such finding of inconsistency with the personal data protection requirements, is necessary for finding the abuse of dominant position.

Special personal data, such as health data, data connected to expression of religion or belief, should be dealt with special attention. According to the Meta Platforms judgment when a user enters information in such websites or apps or where he or she clicks or taps on buttons integrated into those sites and apps, such as the 'Like' or 'Share' buttons and thus makes this information public[13], which is related to special personal data, an 'explicit

12 Data Processing Addendum, point 2. c, https://www.facebook.com/legal/Workplace_GDPR_Addendum
13 Meta Platforms Judgment, see supra 2.

choice' beforehand must be enabled. On this way the CJEU has underlined the explicit consent necessity for the processing the special categories of personal data.

Most importantly, the judgment stresses the importance of enabling a free consent for processing the personal data of the users of social media networks regardless of the fact that such a network holds a dominant position on the market. It contends that the 'fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent to the processing of their personal data by that operator'[14]. A consent, being a free will, is in theory often regarded as possibly questionable when given to a party which has a more strong position in this relationship. Example for this is the labour relation, where the employee's consent to his employer is not considered as freely given, as the two parties in that relationship do not hold equal positions. (Cosabic J., 2021.) One being economically dominant, the employer, and another being economically dependant, the employee. With analogy to that, the dominant position of social media networks must require a very strict scrutiny of data processing of their users and consumers. It must not in any way prevent or not enable its users to freely express their will, and to decide for themselves whether to entrust such a social network with his or her personal data or not.

CONCLUSION

Personal data have a special value in a digital society, especially when it comes to social networks. GDPR has made an important foundation for efficient protection of such data and a supervisory mechanism. The recent judgment of the European Court of Justice has introduced the antitrust authorities in the system of supervising the data protection in digital surroundings, when a dominant position of a social network is at play. This strengthens the system of protection of personal data and creates a new connection between economy, social media and its users.

BIBLIOGRAPHY

1. The Court of Justice of the European Union, Judgment of the Court (Grand Chamber) of 04 July 2023 (request for a preliminary ruling from the Oberlandesgericht Düsseldorf-Germany) – Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd, Facebook Deutschland GmbH v Bundeskartellamt, Case C-252-21, Meta Platforms and Others (General terms of use of a social network)
2. Amann v. Switzerland [GC], no. 27798/95, § 65, ECHR 2000-II). Para 43, Rotaru v. Romania Strasbourg, 4 May 2000
3. Judgment of the Court (Second Chamber) 19 October 2016 (*) In Case C 582/14, interpretation of 'article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
4. General Data Protection Regulation, entered into force on 24 May 2016, applicable since 25 May 2018
5. Leenes Ronald, Van Brakel Rosamunde, Gutwirth Serge, De Hert Paul, Data Protection and Privacy, The Age of Intelligent Machines, Hart Publishing, Oxford and Portland, Oregon, 2017,

14 Meta Platforms Judgment, point 8

6. FTC Staff, Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf,
7. Chen Jiahong, Regulating Online Behavioural Advertising through Data Protection Law, especially regarding Cambridge analitica and Facebook, University of Nottingham, UK, Edward Elgar Publishing, Cheltenham, UK, Northampton, MA USA
8. The European Court of Human Rights, Judgment in the case of Sunday Times v. The United Kingdom of 24 October 1991
9. The European Court of Human Rights, Judgment in the Case of Barbulescu v. Romania of 5 September 2017
10. The European Court of Human Rights, Judgment in the Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland of 27 June 2017
11. Article 29 Data Protection Working Party, Guidelines on Consent, adopted on 28 November 2017
12. Data Processing Addendum, https://www.facebook.com/legal/Workplace_GDPR_Addendum
13. Cosabic, J. , Data Protection of Employees-Certain Aspects of ECHR and GDPR Protection, IRIS21 (Internationales Rechtsinformatik Sympsion IRIS 2021), Salzburg, 2021