MONIKA SZARANIEC
https://doi.org/10.33995/wu2023.1.2
data wpływu (date of receipt): 14.04.2023
data akceptacji (date of acceptance): 20.05.2023

Profiling and automated decisions concerning consumers in the insurance market and threats to their right to privacy and the right of disposal over their personal data

The innovation of insurance companies' access to Big Data to collect additional information about the customer or verify the data provided by the customer can bring benefits to both parties, but also generate risks for the consumer. In the article, the author points out that in the business insurance market, profiling and automated decision-making should be distinguished depending on how personal data is used. This is relevant to decision-making by insurance companies in individual cases with regard to consumers without their consent based solely on automated processing, including profiling of their personal data. Within the scope of the analyzed issue, the obligation to provide information to the consumer about the fact of subjecting him to personalization treatments using automated data analysis tools was also presented. The consumer's privacy mechanisms based on providing information to the consumer and obtaining the consumer's consent are of debatable effectiveness. It seems that the protection of personal data in the current consumer trade should be regulated by public law instruments applied by regulatory bodies at the EU and member state levels.

Keywords: Profiling, automated decisions, personal data processing, Big Data, right to privacy, consumer information autonomy.

Introduction

The purpose of the article is to draw attention to insufficient legislative regime and the threat posed to the consumer by gathering and processing of personal data, based on which an entrepreneur profiles the consumer or makes automated decisions. Big Data, as an instrument for insurance undertakings serving to search for adequate information about the risk profile or to select individualized consumer-oriented products, is correlated to the protection of personal data and the right to privacy. Growing amounts of new data gathered about consumers can generate certain threats to the latter, i.e, invasion of privacy, violation of anti-discrimination laws, problems with party autonomy in the conclusion of contracts, or an exclusion aspect. The legal solutions emerging at the interface of security issues and personal data protection as well as consumer protection are insufficient not only in terms of the instruments of protecting the weaker party to the insurance contract but also in terms of their general purpose.[1]

1. Profiling and automated decision-making in the context of legality principles

In literature, it is pointed out that by profiling one should understand activities aimed at the evaluation of a specific person, prediction of their behaviour, etc. The process of profiling natural persons (one can also profile groups of persons, objects, phenomena) has much in common with categorization or "pigeonholing" of individuals.[2]

The mere act of profiling and automated decision-making was specified in the 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).[3] This subject area, however, had already been in the sphere of interest of the European legislator.

Protection of privacy and personal data had become an interest area of the Council of Europe before pieces of legislation governing that subject were introduced in the UE law.

---

1. The publication was co-financed/financed from the subsidy granted to the Cracow University of Economics – Project nr 088/EPG/2022/POT

2. A. Mednis, *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Wrocław 2019, p. 26 and 27. According to that author, when approaching human profiling as a process, one can distinguish its following stages: collection of data, preparation of a profile (model), application of the profile (model) to a specific person in the form of an analysis, evaluation or prediction of the person's features or behaviour. For more on that, see: M. Ciechomska, *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych,* EPS 2017, Nr 5; X. Konarski, *Profilowanie danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych osobowych – dotychczasowy i przyszły stan prawny w UE oraz w Polsce*, in: Aktualne problemy prawnej ochrony danych osobowych 2016, ed. G. Sibiga, MoP 2016, Nr 20; W. Wiewiórowski*, Profilowanie osób na podstawie ogólnodostępnych danych,* in*: Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym,* ed. A. Mednis, Warszawa 2013.

3. Hereinafter referred to as: GDPR.

In its original version, Convention 108 did not relate specifically to profiling or to automated decision-making. In 2018, the Committee of Ministers of the Council of Europe adopted a protocol amending Convention 108.[4] In Art. 9(1) letter (a), the right of an individual was specified not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration. If a given resolution is an automated decision in the above understanding, then the prohibition of its making does not apply only when the decision is authorised by a law to which the data controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests (Art. 9(2) of Convention 108).[5] It follows from the above that if the decision-making process involves a so called human factor or opinion of a person is taken into account, then we do not have to do with an automated decision. In addition, a person that may be subject to an automated decision has the right to question that process, however, this does not relate to the decision itself but to the mere evaluation made by the algorithm. In the text of the Convention, the term profiling does not appear, and it has not been defined as a type of data processing. In the opinion of certain commentators, a reference to profiling can be found in Art. 9(1) letter (c), under which every individual has the right to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her.[6]

One should note the absence of a specific profiling regime in 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, however, the cited Directive provided for the question of automated decision-making.[7] In Recital 41 of Directive 95/46, it was stipulated that any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing. Art. 15(1) of Directive 95/46 made specific the requirement to grant to every person the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.[8] A guarantee of transparency was the right of access to one's own data under Art. 12 of the discussed Directive, involving the assurance to every data subject of the right to obtain from the controller, without any constraint, at reasonable intervals and without excessive delay or expense, knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1) of the discussed Directive. As a result, the Directive addressed the questions of making automated decisions which produce legal

4. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e (accessed: 12.01.2023).
5. For a commentary to the contents of those rights, see C. de Terwangne, *The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data*, International Review of Law, Computers & Technology, 2014, t. 28, nr 2, p. 125–126.
6. A. Mednis, *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Wrocław 2019, p. 160–162. The author underlines that the revised Convention108, as far as it relates to profiling and automated decision-making, may give rise to interpretative doubts. He is of the opinion that the Convention's authors identify the outcome of profiling (evaluation) with automated decision-making and that Convention 108 regulates the matter of automated decisions differently from GDPR, which may give rise to problems with the Convention's interpretation in that regard.
7. OJ L 281, 23.11.1995, p. 31–50. See: Art. 12 and Art. 15 of the Directive and its Recital 41.
8. Art. 15(2) provided for exceptions to the prohibition to make automated decisions.

consequences for a given person or which significantly affect that person. Then, the Act of 29 August *1997* on personal data protection[9] implemented Art. 15 of Directive 95/46. The implementing provision (Art. 26a uodo)[10] referred to all types of automated decisions and did not mention the aspects of personal evaluation, which would imply coverage by the prohibition of any decisions that do not involve personal evaluation. Art. 26a uodo was formulated as prohibition to make, in relation to a person, any individual resolutions inasmuch as the content of such resolutions is exclusively an effect of operations on personal data conducted in a computerized system. The prohibition did not apply if: the resolution was made when concluding or performing a contract and took into account the data subject's request or when this was authorized by legal provisions which also provided for measures of protecting legitimate interests of the data subject. It must be emphasized at this point that it was sufficient to include in the decision-making process a so called human factor for the decision not to be subject to the prohibition. In summary, the 1997 Act on Personal data protection did not contain a legal definition of profiling. Within the framework of that Act, profiling was not the aim of processing but its type, one of the activities covered by the broad definition of data processing under Art. 7(2) uodo. Although profiling was not expressly mentioned in that provision, the list of activities included in the Article was only demonstrative and profiling undoubtedly belonged to such catalogue.[11]

The concept of profiling is only included in GDPR, which defines it as *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"* (Art. 4(4) GDPR). However, the Regulation does not provide for clearly defined conditions of the admissibility of profiling.

The definition clearly highlighted two structural elements of profiling – the method of data processing (automated processing) and the purpose of data processing (to evaluate the aspects of a natural person).[25] As opposed to the classical methods of data protection, profiling is entirely automated, uses algorithms or other techniques enabling analysis and conclusion making based on large datasets, with efficiency and accuracy unattainable in the processing of data through manual methods. As a result, profiling constitutes a fully automated form of personal data processing.[12]

On the other hand, automated decision-making (Art. 22 GDPR) literally means making a decision based "solely on automated processing, including profiling."[13] In literature, it is emphasized that only real involvement of a human factor in the decision-making process is sufficient to conclude that a given decision has not been made automatically.[14] In the same way, profiling, in the understanding of Art. 4(4) GDPR, which is not covered by the provisions of Art. 22 GDPR, must involve a certain form of automated processing but this does not preclude involvement of a human factor in the

9. Dz.U. 2016 r. poz.922, as amended. Hereinafter referred to as: uodo.
10. This happened only along with the entry into force of the Act of 25 August 2001 amending the Act on personal data protection – Dz. U. 2001, nr 100 poz. 1087.
11. So: A. Mednis, *Prawo ochrony danych* …, p. 164–165.
12. X. Konarski, *Profilowanie danych*, p. 49.
13. M. Mostowik, *Ochrona danych osobowych w Internecie rzeczy w prawie UE*, Warszawa 2022, https://sip.legalis.pl/document-view.seam?documentId=mjxw62zogi3damzzguytgmq&tocid=mjxw62zogi3damzzguytgmq&rowIndex=-1
14. W. Chomiczewski, *Profilowanie w ogólnym rozporządzeniu o ochronie danych,* in*: Polska i europejska reforma ochrony danych osobowych,* eds. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016, p. 131.

process.[15] Profiling and automated decisions were subject to the works of the Working Group Art. 29[16] transformed on 25 May 2018 into the European Data Protection Board.[17] Although guidelines of the Working Group Art. 29 do not have a legally binding force, they make an important guideline for the interpretation of the terms included in GDPR. According to the Guidelines of the Working Group Art. 29, for a data processing not to be considered fully automated it is necessary that human intervention should allow to exercise essential supervision over the decision-making. Moreover, actions must be taken by a person authorised and competent to change the decision, and must take into account all data essential for the given decision-making situation. Ostensible involvement of a human factor in the decision-making process, consisting, for example, only in confirming decisions generated by an algorithm, will not therefore be a prerequisite for exempting a given decision-making process from the scope of application of the prohibition under Art. 22 GDPR. The Working Group Art. 29 summarised the question of the relationship between automated decision-making and profiling: *"Automated decision-making has a different scope and may partially overlap with or result from profiling. (...) Automated decisions can be made with or without profiling; profiling can take place without making automated decisions. However, profiling and automated decision-making are not necessarily separate activities. Something that starts off as a simple automated decision-making process could become one based on profiling, depending upon how the data is used."*[18]

As emphasized above, GDPR does not include clearly specified permissibility conditions for profiling, and the focus is shifted to the specification of the principles of decision-making based solely on automatic processing and producing legal effects for the data subject or, in a similar way, significantly affecting the data subject, and to the data subject's right not to be bound by such decision (Art. 22(1) GDPR).[19] The right not to be subject to decisions based solely on automated processing, as a right of prohibitive nature, under Art. 22 GDPR, grants to every data subject a right not to be subject to decisions that are based solely on automated processing, including on profiling, and produce legal effects for the data subject or otherwise significantly affect the data subject. However, this right is not absolute since Art. 22(2) GDPR provides that it is permissible to make decisions in relation to a data subject based on automated processing, including based on profiling, when such decision: 1) is necessary for entering into, or performance of, a contract between the data subject and a data controller; 2) is authorised by Union or Member State law; 3) is based on the data subject's explicit consent. The legislator indicates that the effect conditioning the recognition that a given decision is automated is a consequence in the legal sphere of a natural person or similar significant effect. Such legal consequence may be refusal to grant insurance protection. In literature, it is pointed out that another significant effect is a situation in which a resolution leads to

15. D. Lubasz, *Big brother is watching you. Profilowanie i zautomatyzowane podejmowanie decyzji w kontekście zasad legalności i przejrzystości* (in:) Rok GDPR, eds. W.R. Wiewiórowski, H. Wolska, Warszawa 2019, https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3damzzguytgmrohaxdglrr&refSource=search
16. The Working Group was established under Art. 29 of Directive 95/46/EC. It forms an independent European advisory authority in the area of data and privacy protection. The Group's objectives were specified in the provisions of Art. 30 of Directive 95/46/EC and Art. 15 of Directive 2002/58/EC.
17. The Working Group Art. 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017, recently revised and adopted on 6 February 2018, 17/PL WP 251 rev.01
18. file:///C:/Users/UEK/Downloads/Rekomendacja%20profilowanie.pdf, p.8 and 9.
19. M. Mostowik, *Ochrona danych osobowych* .... https://sip.legalis.pl/document-view.seam?documentId=mjxw62zogi3damzzguytgmq&tocid=mjxw62zogi3damzzguytgmq&rowIndex=-1

discrimination on grounds of age, sex, disability, racial or ethnic origin, confession, sexual orientation, etc. An offer leading to discrimination may be considered as producing a significant effect, just as an offer leading to unequal treatment of persons in similar circumstances, however, the mere fact of differentiating the offered conditions of selling products or providing services is admissible as long as the differentiation is based on objective criteria. A legal effect may be considered both influence on the legal status of a given person or influence on the person's rights under a contract.[20]

2. Automated decision-making, including profiling, in relations to customers in the insurance market

After the adoption of GDPR, in Poland works were undertaken on drafting a Sectoral Act,[21] which was to align multiple specific acts with GDPR. Essential amendments introduced by the Sectoral Act affected also provisions of the Act of 11 September 2015 on insurance and reinsurance activity,[22] which is why actors in the insurance industry will be forced to review their processes and procedures with regard to the fulfilment of additional requirements laid down in the discussed provisions. In order to enable the use of the generally prohibited activities of automated decision-making in the insurance sector, the legislator decided to introduce in u.d.u.r. the provisions of Art. 41(1a) and (1b). They constitute a clear statutory basis for the undertaking by insurance companies of the operations of automated decision-making in individual cases, including profiling, as referred to in Art. 22(2) GDPR. This provision makes an independent, clear statutory basis empowering an insurance undertaking to use systems of automated decision-making in individual cases, without the need to obtain consent from data subjects.[23] The discussed provision allows insurance undertakings to make decisions in individual matters, based solely on automated processing, including profiling of personal data, for the following exclusive purposes: 1) in connection with the assessment of insurance risk – Art. 41(1a) item 1 u.d.u.r. and 2) in connection with performing insurance operations referred to in Art. 4(9) items 1 and 2, i.e. in order to determine the causes and circumstances of fortuitous events and to determine the amount of loss and compensation as well as other amounts payable to parties entitled under insurance contracts or insurance guarantee contracts, that is at the stage of performing the insurance contract and adjusting loss – Art. 41(1a) item 2 u.d.u.r.

According to the solution introduced in u.d.u.r., automated decisions made to asses insurance risk may only comprise personal data relating to the insured parties. On the other hand, automated decisions made to perform the above-mentioned insurance operations (e.g. at the stage of loss adjustment) may refer to personal data of the insured parties, policyholders and beneficiaries under an insurance contract.[24]

20. So: A. Mednis, *Prawo ochrony danych* …, p. 218.
21. Act of 21 February 2019 amending certain Acts in order to ensure the application of the 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 (Dz. U. z 2019 r. poz. 730).
22. Consolidated text: Dz. U. z 2018 r. poz. 999, as amended; hereinafter: u.d.u.r.
23. D. Lubasz, *Przetwarzanie danych osobowych w branży ubezpieczeniowej w dobie InsurTech – zagadnienia wybrane* (in:) *InsurTech Nowe technologie w branży ubezpieczeń*, ed. K. Szpyt, Warszawa 2022, p. 123.
24. Ibid., p. 124.

Profiling is often a part of the risk assessment process in insurance undertakings. Insurance undertakings use *Big Data,25* for example, to monitor the practice of driving vehicles by policyholders and use the obtained information to calculate personalized premium rates. In the context of life insurance and personal risk insurance, *Fitbit* or *Withings* bands are used or a fitness tracker in a mobile phone, which monitor key human physical parameters, such as heart rate and blood pressure or the number of steps taken per day. Based on that information, an insurance distributor can assess more precisely the insurance premium and carry out more precise risk assessment relating to specific policyholders. On the other hand, *Octo Telematics* is one in a number of startups specialised in telematics sensors which monitor how policyholders drive a car (the device is installed in motor vehicles and used to track the ride) i.e. the distance travelled, speed, acceleration, braking, etc. In Italy, in turn, *Blackbox* devices are installed in cars tracking speed, braking, acceleration, cornering and the time of the day during the travel, which is determined using satellite technology. The data are sent to the insurance undertaking by GPS, which enables the insurer to take position in respect of the customer's claim.[26]

Due to the amendments introduced in u.d.u.r., insurance undertakings may rely on the prerequisite specified in Art. 9(2) letter (g) GDPR. Eventually, it was provided that an insurance undertaking may process data on the health of the insured parties or beneficiaries under an insurance contract, included in the insurance agreements or declarations made prior to concluding an insurance contract, respectively for the purpose of assessing insurance risk or performing the insurance contract, to the extent necessary considering the purpose and type of insurance. Under Art. 9(2) letter (g) GDPR, processing of "sensitive data" (e.g. on health condition) is legal when this is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Importantly, Art. 9(2) letter (g) GDPR requires not only that a national legal provision should permit processing of a specific category of personal data but also that such processing should be necessary and that the necessity should follow from reasons of substantial public interest. In addition, the provisions: must be proportional to the intended purpose, may not compromise the essence of the right to data protection, and must envisage adequate and concrete measures to protect the fundamental rights and interests of the data subject.[27]

The activities described above, under Art. 41(1a) u.d.u.r., may be performed only provided that the person whom the automated decision concerns is guaranteed the right to obtain relevant explanations about the basis of the decision made, the possibility to question the decision, to express their own position and obtain human intervention.

---

25. *Big data* can be defined as: *"information resources characterised by large volume, high velocity and/or high variety, requiring new processing methods so as to enable more efficient decision-making, discovery of new phenomena (insight discovery) and process optimalisation."* Cited after: Beyer M., Laney D. (2012), The Importance of 'Big data': A Definition, source: https://www.gartner.com/doc/2057415/importance-big-data-definition.

26. Cited after: A. Braun, F.Schreiber, *The Current InsurTech Landscape: Business Models and Disruptive Potential, Institute of Insurance Economics* I.VW-HSG, University of St. Gallen, 2017, p. 56–57. See also: S. Kotecka – Kral, *Zagrożenia związane z przetwarzaniem danych osobowych osób fizycznych w celu profilowania* [in:] A. Dańko-Roesler, M. Leśniak, M. Skory, B. Sołtys, *Ius est ars boni et aequi : księga pamiątkowa dedykowana Profesorowi Józefowi Frąckowiakowi* , Warszawa 2018, p. 563 et seq.

27. J. Byrski, H. Hoser, *Zakres zmian w ustawie o działalności ubezpieczeniowej i reasekuracyjnej w związku z dostosowaniem do unijnych regulacji dotyczących ochrony danych osobowych*, Prawo Asekuracyjne nr 2/2019 p. 76.

It is also legitimate to assume that processing of data on health condition can take place exceptionally in the event of circumstances specified in Art. 35a u.d.u.r., i.e. for the purpose and within the scope necessary to prevent an offence, in case of a reasonable suspicion of committing an offence to the detriment of the insurance undertaking (e.g., in connection with a suspicion of an insurance fraud). Finally, permissibility of processing such categories of personal data may follow from other bases laid down in Art. 9(2) GDPR. In particular, in case of a civil law dispute, processing by an insurance undertaking of data concerning a given person's health condition may be necessary to determine, assert or defend claims, or as a part of administering justice by the courts (Art. 9(2) letter (f) GDPR), however, that legal basis may generally apply only at the stage of judicial proceedings.[28]

The above-mentioned Sectoral Act[29] authorised automated decision-making in individual cases, including profiling, as referred to in Art. 22(2) GDPR, not only by insurance undertakings but also by the Insurance Guarantee Fund (UFG). Under Art. 98d of the Act of 22 May 2003 on compulsory insurance, the Insurance Guarantee Fund and the Polish Motor Insurers' Bureau,[30] UFG can make decisions in individual cases, based on automated decision-making, including profiling, for the purpose of carrying out the tasks referred to in Art. 84(2) item 2 letter (a) and Art 84(3) item 2 letter (a), Arts. 98, 98b, 98c, 102 and 102a of that Act, which provisions relate, among others, to carrying out checks if a compulsory civil liability insurance has been concluded by owners of motor vehicles or farmers, settling liabilities under compulsory insurance, tasks connected to the UFG's function as information centre and maintenance of a computerized database to the extent necessary to identify, verify and counteract violations of interests of the insurance market. Analogous rights to automated decision-making in individual cases, including profiling, were also granted to the Polish Motor Insurers' Bureau within the scope of the tasks performed by that institution, i.e., among others, in relation to the organization of the adjustment of losses caused in the territory of the Republic of Poland by holders of motor vehicles registered abroad.[31]

3. Threats to the customer posed by the activities of profiling and automated decision-making in the insurance market

In the recent years, it is increasingly important for insurance undertakings to have access to public data sets, allowing to gather additional information about customers or to verify the data submitted by customers, among others, for the purposes of detecting fraud in the insurance market. Cooperation between insurance undertakings and public institutions may bring benefits to both parties,[32] and threats to the

28. J. Byrski, H. Hoser, *Zakres zmian*…., p. *77*.
29. See footnote 20.
30. Dz. U. z 2022 r. poz. 2277, 2640.
31. See: Art. 136c and Art. 122(1) item 3 of the Act of 22 May 2003 on compulsory insurance, the Insurance Guarantee Fund and the Polish Motor Insurers' Bureau.
32. „*Cyfryzacja sektora ubezpieczeń w Polsce 2018*", Report prepared by Accenture in cooperation with the Polish Insurance Association, p. 30 et seq. file:///C:/Users/user/Desktop/PIU%20Fintech.pdf . In the Report, one can read that in the United Kingdom distributors invested and created a central digital drivers register (MID – Motor Insurance Database), connected to the Police database. The investment allowed to significantly reduce the number of uninsured drivers, and contributed to the improvement in the detection of fraud in the context of motor insurance. Similar initiatives proved successful in the Netherlands and in other countries.

insurance undertaking's customer. This is the case since combination of the latest achievements in data science and the existing practices of predictive analytics, used by insurance undertakings, may potentially accelerate incredible advancements in the area of efficiency and innovation, offering quantifiable benefits also to customers, however, this type of innovation poses certain threats to the latter. Many such threats are common to all commercial applications of big data sets, i.e.: collection of large amounts of personal data increases the scale of losses relating to breeches of the customer's security; compilation of information from a large number of sources makes it less probable that the restrictions following from consumers' consents to the use of their personal information are going to be respected; and the use of data exploration for the purpose of informing about decisions concerning sales, prices or employment increases the risk that insurance distributors will violate anti-discrimination rules.[33] It is pointed out in literature that, in this respect, the most exposed group are consumers. In the context of implementing new technologies, also in the insurance market, apart from discriminatory aspects, the essential threats are: infringement of consumer privacy, problems with party autonomy in the conclusion of contracts, and the threat of customer segmentation.[34]

In Polish literature of the subject, the sphere of an individual's private life forms a part of the individual's personal interests and is subject to the protection provided under Arts. 23 and 24 of the Civil Code.[35] In literature, certain authors understand the personal interest of private life as everything that, having regard to legitimate isolation of an individual from the society as a whole, serves the development of the individual's physical and mental personality and preservation of the achieved social status. At the same time, within the sphere of private life, authors distinguish the sphere of intimate personal life and the sphere of private personal life.[36] Other voices in literature draw attention to a wide and narrow grasp of privacy. The wide grasp of privacy can be generally reduced to the assumption that the sphere of privacy is a sphere of freedom, encompassing such categories of freedoms as, for example, the freedom of speech, the freedom of religion, the right to personal life, the freedom to decide about one's own life and health, and the right to keep confidential information about oneself. In the narrow grasp, authors point to "information privacy," whose essence boils down to the management by an individual of information about oneself with regard to free decisions about the scope, method of its sharing, and about the methods of communicating the information to other persons. In Polish academic literature, the concept of privacy is dominated by the concept of infor-

33. M.N. Helveston, *Consumer Protection in the Age of big data*, "Washington University Law Review" 2016, vol. 93, issue 3, p. 6–7. For more on consumer discrimination in this regard, see: A. Jabłonowska, M. Kuziemski, A. M. Nowak, H.-W. Micklitz, P. Pałka, G. Sartor, *Consumer Law and Artificial Intelligence Challenges.., p.* 14 et seq., and: M.N. Helveston, *Consumer protection in the age of Big Data*, Washington Uniwersity Law Review, vol. 93/2016, p. 34 et seq.

34. See, for example, N. Helberger, Profiling and targeting consumers in the Internet of Things – A new challenge for consumer law, Institute for Information Law, University of Amsterdam, Electronic copy available at: http://ssrn.com/abstract=2728717

35. A. Kopff understood the personal interest of private life as everything that, having regard to legitimate isolation of an individual from the society as a whole, serves the development of the individual's physical and mental personality and preservation of the achieved social status. At the same time, as a part of the sphere of private life, the author distinguished the sphere of intimate personal life and the sphere of private personal life. See: A. Kopff, *Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne),* SC 1972, t. 20, p. 31–33. On the other hand, M. Safjan is of the opinion that "any definitions of privacy have a general and directional nature" and that "there is no «universal and invariable privacy space." See: M. Safjan, *Prawo do ochrony życia prywatnego, in: Podstawowe prawa jednostki i ich sądowa ochrona (ed. L. Wiśniewski),* Warszawa 1997, p. 128.

36. A. Kopff, *Koncepcja prawa do intymności*, p. 31–33.

mation privacy. Attention is also drawn to the fact that the right to privacy includes also the right to expect that information about an individual as a person will be communicated truthfully.[37] Protection of private life, information protection is currently the most dominant value in the context of widely understood privacy. Recognition of the right to the protection of personal data as personal interest would allow to expand the range of legal remedies by civil law claims, both material and nonmaterial, under Art. 24 of the Civil Code, which would allow to seek protection not only in administrative proceedings but also in civil proceedings."[38] At this point, it is worth highlighting the opinion that "the protective regime envisaged in Art. 23 and 24 of the Civil Code does not constitute an optimal regime of preventing violations to information autonomy in the Internet. Whereas the range of claims for an actually committed violation of personal interests (for making a declaration other than declaration of intention, compensation or «punitive damages» for a social purpose) meets the general standard, preventive or precautionary measures (cease and desist request) are, without specific supplementing provisions, hardly operative in the realities of the information society." The same author argues that the effectiveness of a cease and desist request raises doubts as an invasion of privacy usually takes place before the entitled party takes any remedial actions. He is also of the opinion that, in most situations of infringing personal interests over the Internet, it would be a more efficient solution to seek, at once, removal of the infringement's effects. Nevertheless, the author notes that, for instance, in case of online archiving of defamatory information, we have to do with a persistent state of danger of a continuous unlawful act, which fully justifies a cease and desist request in the understanding of Art. 24 § 1, first sentence, of the Civil Code. He also believes that the right to decide about the permissibility to gather and share personal data does not amount to an independent personal interest. Also another voice in literature indicates that personal data do not constitute a personal interest distinct from privacy. Moreover, restrictive legal provisions on the processing of personal data are a manifestation of the protection of the right to privacy through administrative law instruments, whereas the protection of privacy as personal interest is afforded through civil law instruments.[39] In the context of such variety of opinions, one can only appreciate the approach according to which there is a crossover relationship between the protection of the right to privacy (in the area of constitutional and civil law) and protection of personal data in the administrative area, and that these legal regimes are independent from one another. As a result, situations may happen in which processing of personal data will at the same time constitute an infringement of the right to privacy and, on such occasions, we have to do with cumulative protection. On the other hand, there may be cases in which data processing will not be recognized as infringement of the right to privacy.[40]

37. See K. Michałowska, Prawo do życia rodzinnego na tle ogólnie pojmowanej prywatności jednostki, ZNUEK 2013, Nr 911; p. 53–54 and literature cited therein, in particular B. Kordasiewicz, *Prawo do prywatności. Aspekty prawne i psychologiczne, in: Prawo do prywatności – aspekty prawne i psychologiczne (ed. K. Motyka),* Lublin 2001, p. 85.

38. So: J. Sieńczyło-Chlabicz, *Prawo do ochrony danych osobowych jako dobro osobiste, in: Qui bene dubitat, bene sciet. Księga jubileuszowa dedykowana Profesor Ewie Nowińskiej* (ed. J. Barta, J. Chwalba, R. Markiewicz, P. Wasilewski), Warszawa 2018. The author underlines that this element of privacy is most strongly accentuated in the case-law of the Constitutional Tribunal. She proposes to introduce in the catalogue of personal interests under Art. 23 KC a separate personal interest in the form of the right to protection of personal data, which could significantly enhance the protection of personal data in cyberspace.

39. P. Sobolewski, in: Osajda, Komentarz KC, Art. 23.

40. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2011, p. 178–179.

The right to information autonomy relates to the "right to be forgotten," which may be considered both in the context of public law protection (protection of personal data), especially when it comes to the EU legislation[41] and the CJEU[42] case-law, and in the context of private law protection, as personal interest. The right to be forgotten is vested in natural persons and implies a possibility to request removal of personal data made available, especially in the Internet, in case of one of the prerequisites provided by law, in particular, when the data are no longer necessary for the purposes for which they were gathered or when the entitled person has withdrawn consent to their processing.[43] It is emphasized in literature that this right is not correlated to any distinct ideal interest. "The right to be forgotten" reflects ideal interests that have been already identified and protected by law, such as given name and surname, pseudonym, image, good name, physical and mental integrity and human individuality and, for that reason, it can be fully integrated into the collective concept of privacy, irrespective of the adopted juridical construction of personal interests.[44] However, regardless of constructional and terminological views regarding the Civil Code regime of protecting personal interests, it should be noted that academic authors are in agreement that every person, to the same extent, has the right to be remember and to be forgotten, which means that every person may request both disclosure and rectification or removal from the public domain of any information relating to themselves.[45]

In the sphere of protecting personal data, the law of the European Union and, consequently, Polish law, have adopted a paradigm of protection through information. General disclosure obligations under GDPR and special provisions are supplemented by a number of more specific disclosure requirements under special statutes.[46] The obligation essential in the context of the subject matter analysed in this article is the duty to provide the consumer with information about the fact of submitting the consumer to personalizing procedures with the aid of automated data analysis

41. See, e.g. Recital 1 GDPR: "The protection of natural persons in relation to the processing of personal data is a fundamental right".

42. For more, see: W. Wiśniewska, *Przetwarzanie danych wrażliwych w Internecie a RODO. Omówienie wyr. TS z 24 września 2019 r., C-136/17 (GC et al*), Lex;

43. A. Nowak-Gruca, *Wybrane problemy ochrony dóbr osobistych w epoce postprawdy*, SPP 2022, Zeszyt 3 (66) – 4 (67) 22, p. 13 and literature cited therein.

44. W.J. Kocot, *Charakter prawa „do bycia zapomnianym" – restytucja reputacji w Internecie, in: Opus auctorem laudat. Księga jubileuszowa dedykowana Profesor Monice Czajkowskiej-Dąbrowskiej (ed. I. Matusiak, K. Szczepanowska-Kozłowska, Ł. Żelechowski)*, Warszawa 2019;

45. M. Ilnicki, *Prawo do bycia zapomnianym w kontekście „postzniesławiającej" informacji w sieci Internet*, cz. 2, Pal. 2014, Nr 5–6; p. 106.

46. See: Act of 15 December 2017 on insurance distribution (Dz. U. z 2022 r. poz. 905, 2640). M. Szaraniec, *"Information as a public law instrument of customer (consumer) protection on the economic insurance market. Considerations against the background of the Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (IDD)", (in:) "The influence of the European legislation on national legal systems in the field of consumer protection", A. Viglianisi Ferraro, M. Jagielska and M. Selucka (eds.),* CEDAM 2018, pp. 245–255. M. Szaraniec, *Artificial Intelligence and Big Data in the operation of insurance companies and the situation of their customers (in:) Právo, obchod, ekonomika 9 : zborník príspevkov Law, Commerce, Economy 9 : Collection of Papers / eds. Jozef Suchoža, Ján Husár, Regina Hučková – Košice: Univerzita Pavla Jozefa Šafárika Vydavatel'stvo Šafárik Press, 2019, pp. 521–531;* M. Szaraniec, *Inteligencia artificial y el problema de exclusión de cierta categoría de clientes en el ejemplo del mercado de seguros. Cuestiones seleccionadas (in:) Artificial Intelligence and Human Rights, L. Miraut Martín,M. Załucki (eds.), DYKINSON, Madrid, 2021, pp. 191–200.*

tools. This obligation was introduced under Art. 14(2) letter (g) GDPR (as highlighted above), providing for a general right to being informed about automated processing of data, including about the personalization achieved on that basis. The above-mentioned provision covers in practice an extensive and diverse range of decisions made with the aid of algorithms, analysing personal data and making choices, on that basis, about personalizing certain decisions with regard to a specific individual. Decisions of such type are made, among others, in the insurance market.

GDPR introduced a quite complex management system to ensure that personal data of natural persons are stored and processed in a fair and legal manner, however, this does not solve the problem of unlimited use by insurers of Big Data and Data Analytics, or analytical systems intended to offer advanced methods of pricing or cross-selling.

The evolution of private law of the European Union was largely determined by the focus of its legislation on the integration of the EU internal market. This orientation towards integration of the internal market assumes not only a regulatory nature of the European *acquis* but also a separate approach to the autonomy of legal subjects. In literature, three essential aspects are distinguished in relation to party autonomy that should be preserved during the conclusion of a contract: independence, authenticity and option of choice.[47] Independence implies the capacity to control and make one's own decisions. Authenticity is identified with one's own opinion and can be eliminated by manipulating a person with a view to generating the person's values, wishes, purposes. Finally, in order to preserve independence, it is necessary for a given person to have an adequate range of options to choose from, which should be available to that person.[48] The use by insurance undertakings of Big Data and Data Analytics may be conducive to elimination of one of the three aspects (independence, authenticity, option of choice) and may lead to forfeiture of party autonomy during the conclusion of a contract.

However, consumers of financial services should be aware of the risk posed by *Big Data*. The risks identified by the European supervisory authorities[49] are, among others, the risk of errors deriving from the tools used for analysing big data sets, which may lead to wrong decisions made by providers of financial services. In addition, a growing level of customer segmentation, possible due to *Big Data*, may translate into the availability of certain financial services or products, or into exclusion of certain customers from the market.[50] For another thing, an algorithm personalizing

47. See, for example.: Sax, M., Helberger, N., & Bol, N. (2018). Health as a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices. *Journal of Consumer Policy*, *41*(2), 103–134. https://doi.org/10.1007/s10603-018-9374-3

48. A. Jabłonowska, M. Kuziemski, A. M. Nowak, H.-W. Micklitz, P. Pałka, G. Sartor, *Consumer Law and Artificial Intelligence Challenges..,* p. 14 et seq. and literature cited therein.

49. ESA's Joint Committee published a Report on Big Data, analysing the impact of Big Data sets on consumers and financial institutions. The authors of the Report point out that Big Data brings many benefits to the financial sector and consumers, such as better-adapted products and services, more effective counteraction of fraud or enhanced effectiveness of internal organizational procedures. For more, see: https://www.esma.europa.eu/sites/default/files/library/jc-2018-4_joint_committee_final_report_on_big_data.pdf
On the other hand, Insurance Europe explains that the use of Big Data and predictive modelling enables insurance undertakings to cover new threats, to offer products better suited to consumer needs and to provide better consultancy with regard to preventing losses.
https://www.insuranceeurope.eu/sites/default/files/attachments/Insight%20Briefing%20-%20Big%20data%20analytics%20-%20An%20insurance%20%28r%29evolution.pdf

50. Certain distributors examine operations of customers on social networks or other online portals to assess the probability that claims made by policyholders are honest.

customer-related decisions is based on artificial intelligence and machine learning, that is on solutions assuming evolution of the algorithm over time, as the software is confronted with the subsequent portions of data and the algorithm generates more and more complex internal decision trees.[51] From that point of view, the obligation to disclose the fact that a decision has been made in a personalised manner is to serve, first of all, the purpose of ensuring to the consumer real autonomy vis-à-vis the consumer's evaluation made by a machine system, and to allow the consumer both to oppose to such decision-making in advance and to question the results of the decision-making *ex post*. This assumption is generally reflected in Art. 22 GDPR, providing for a general data subject's "right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[52]

Summary

Against the background of the presented considerations, the following conclusion arises: the right to information autonomy, the right to dispose of one's own personal data, the right to be forgotten in digital reality (4.0), which at an unprecedented scale strips us of privacy and exposes to invigilation, undoubtedly deserve to be legally protected, regardless of the protection provided in other regulations. The problem if the above-mentioned rights are to be derived from overarching human dignity and treated as independent personal interests or as referents of the concept of privacy is undoubtedly meaningful in theoretical terms. However, to a certain degree, just as any other dogmatic disputes, it will remain undecidable. For that reason, from the practical perspective, one should appreciate the significance of any research and discussion contributing to the identification of new dangers and the need to protect new individual interests, emerging against the backdrop of social relations and parallel existence of humans in two worlds: physical and virtual.[53]

The GDPR paradigm of protecting customers through information raises doubts, bearing in mind the uncertainty to what extent the contents of information provided by an entrepreneur to the consumer allow the latter to reasonably understand and accept the decision made by an algorithm. It seems that the correct way to protect consumers in this regard is to develop such protective instruments that, beside the transparency based on the provision of information about the fact of putting in place an automated decision-making process, would allow to give more specific hints allowing an individual (natural person) to understand the reasons behind an automated decision of particular type. Unfortunately, such model of algorithm explainability has not been thus far provided for in any specific legislative act. However, currently, to an ever-widening extent, it is subject to the discussions concerning further directions for development of consumer legislation in the EU.[54]

51. A. Chłopecki, Sztuczna inteligencja – szkice prawnicze i futurologiczne, Warszawa 2018, p. 33–37.
52. So: M. Grochowski, *Ochrona konsumenta a ochrona danych osobowych w „kapitalizmie inwigilacji" (in:) Prawo umów wobec wyzwań cywilizacyjnych. Zagadnienia wybrane*, eds. B. Kordasiewicz, P. Podrecki, R. Siwik, PAN, Warszawa 2020, p. 79 and literature cited therein.
53. So after: A. Nowak-Gruca, *Wybrane problemy ochrony dóbr osobistych w epoce postprawdy*, SPP 2022, Zeszyt 3 (66) – 4 (67) 22.
54. So: M. Grochowski, *Ochrona konsumenta a ochrona danych osobowych,* p. 81 and literature cited therein.

Moreover, although personal autonomy and the right to decide about one's own privacy (that is the mechanisms of consumer protection based on provision of information to an individual and obtainment of the individual's consent) are developed within the framework of the private law paradigm of private autonomy, protection of personal data in contemporary consumer transactions, in large measure, relates to collective interests. Such collective interests, in turn, should be protected by public law instruments based on more direct intervention into the practices of entrepreneurs in respect of consumers' personal data, since private law instruments should, in this context, rather be a supplementary instrument of consumer protection, considering their limited reach and rather disputable effectiveness. From that perspective, private law (both contract law and tort law) is useful as an instrument of protecting individual interests where the situation of an individual is, for various reasons, less typical or where particular interests are dispersed and harder to grasp within a uniform and generalizing framework of public law legislation. It seems that over time the problems arising at the interface of consumer protection and personal data protection will be regulated in EU legislation with an increasing share of public law element – which is indirectly suggested by the legislative proposals published in the last months by the European Commission.[55]

Bibliography

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2011

Beyer M., Laney D. (2012), The Importance of 'Big data': A Definition, source: https://www.gartner.com/doc/2057415/importance-big-data-definition

Braun A., Schreiber F., *The Current InsurTech Landscape: Business Models and Disruptive Potential, Institute of Insurance Economics* I.VW-HSG, University of St. Gallen, 2017

Byrski J., Hoser H., *Zakres zmian w ustawie o działalności ubezpieczeniowej i reasekuracyjnej w związku z dostosowaniem do unijnych regulacji dotyczących ochrony danych osobowych*, Prawo Asekuracyjne nr 2/2019

Chłopecki A., Sztuczna inteligencja – szkice prawnicze i futurologiczne, Warszawa 2018

Chomiczewski W., *Profilowanie w ogólnym rozporządzeniu o ochronie danych,* in: *Polska i europejska reforma ochrony danych osobowych,* eds. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016

Ciechomska M., *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych,* EPS 2017, Nr 5

Helveston M.N., *Consumer Protection in the Age of big data*, "Washington University Law Review" 2016, vol. 93, issue 3

Sieńczyło-Chlabicz J., *Prawo do ochrony danych osobowych jako dobro osobiste,* in: *Qui bene dubitat, bene sciet. Księga jubileuszowa dedykowana Profesor Ewie Nowińskiej* (ed. J. Barta, J. Chwalba, R. Markiewicz, P. Wasilewski), Warszawa 2018

55. Ibid., p. 82. The author points to the Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC and the Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). In his opinion, in these legislative acts, key role was assigned to public law instruments of exerting impact on the market, applied by regulatory authorities on the level of EU and Member States.

Jabłonowska A., Kuziemski M., Nowak A. M., Micklitz H.-W, P. Pałka, G. Sartor, *Consumer Law and Artificial Intelligence Challenges*

Kocot W.J., *Charakter prawa „do bycia zapomnianym" – restytucja reputacji w Internecie,* in: *Opus auctorem laudat. Księga jubileuszowa dedykowana Profesor Monice Czajkowskiej-Dąbrowskiej (ed. I. Matusiak, K. Szczepanowska-Kozłowska, Ł. Żelechowski)*, Warszawa 2019

Konarski X., *Profilowanie danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych osobowych – dotychczasowy i przyszły stan prawny w UE oraz w Polsce*, in: Aktualne problemy prawnej ochrony danych osobowych 2016, ed. G. Sibiga, MoP 2016

Kopff A. , *Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne),* SC 1972, t. 20

Kotecka – Kral S., *Zagrożenia związane z przetwarzaniem danych osobowych osób fizycznych w celu profilowania* [in:] A. Dańko-Roesler, M. Leśniak, M. Skory, B. Sołtys, *Ius est ars boni et aequi : księga pamiątkowa dedykowana Profesorowi Józefowi Frąckowiakowi* , Warszawa 2018

Lubasz D., *Big brother is watching you. Profilowanie i zautomatyzowane podejmowanie decyzji w kontekście zasad legalności i przejrzystości* [in:] Rok GDPR, eds. W.R. Wiewiórowski, H. Wolska, Warszawa 2019, https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3damzzguytgmrohaxdglrr&refSource=search

Lubasz D., *Przetwarzanie danych osobowych w branży ubezpieczeniowej w dobie InsurTech – zagadnienia wybrane* [in:] *InsurTech Nowe technologie w branży ubezpieczeń*, ed. K. Szpyt, Warszawa 2022

Grochowski M., *Ochrona konsumenta a ochrona danych osobowych w „kapitalizmie inwigilacji" (in:) Prawo umów wobec wyzwań cywilizacyjnych. Zagadnienia wybrane*, eds. B. Kordasiewicz, P. Podrecki, R. Siwik, PAN, Warszawa 2020

Ilnicki M., *Prawo do bycia zapomnianym w kontekście „postzniesławiającej" informacji w sieci Internet*, cz. 2, Pal. 2014, Nr 5–6;

Safjan M., *Prawo do ochrony życia prywatnego, in: Podstawowe prawa jednostki i ich sądowa ochrona (ed. L. Wiśniewski),* Warszawa 1997

Szaraniec M., *Inteligencia artificial y el problema de exclusión de cierta categoría de clientes en el ejemplo del mercado de seguros. Cuestiones seleccionadas* [in:] *Artificial Intelligence and Human Rights, L. Miraut Martín,M. Załucki (eds.), DYKINSON, Madrid, 2021*

Helveston M.N., *Consumer protection in the age of Big Data*, Washington Uniwersity Law Review, vol. 93/2016

Mednis A., *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Wrocław 2019

Michałowska K., Prawo do życia rodzinnego na tle ogólnie pojmowanej prywatności jednostki, ZNUEK 2013, Nr 911

Mostowik M., O*chrona danych osobowych w Internecie rzeczy w prawie UE*, Warszawa 2022, https://sip.legalis.pl/document-view.seam?documentId=mjxw62zogi3damzzguytgmq&tocid=mjxw62zogi3damzzguytgmq&rowIndex=-1

Nowak-Gruca A., *Wybrane problemy ochrony dóbr osobistych w epoce postprawdy*, SPP 2022, Zeszyt 3 (66) – 4 (67)

Sax, M., Helberger, N., & Bol, N. (2018). Health as a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices. *Journal of Consumer Policy*, *41*(2),https://doi.org/10.1007/s10603–018–9374–3

Sobolewski P., in: Osajda, Komentarz KC, Art. 23.

Szaraniec M., *"Information as a public law instrument of customer (consumer) protection on the economic insurance market. Considerations against the background of the Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (IDD)",* (in:) *"The influence of the European legislation on national legal systems in the field of consumer protection"*

Viglianisi Ferraro A., Jagielska M. and Selucka M. (eds.), CEDAM 2018, pp. 245–255. M. Szaraniec, *Artificial Intelligence and Big Data in the operation of insurance companies and the situation of their customers (in:) Právo, obchod, ekonomika 9: zborník príspevkov Law, Commerce, Economy 9: Collection of Papers / eds. Jozef Suchoža, Ján Husár, Regina Hučková – Košice: Univerzita Pavla Jozefa Šafárika Vydavatel'stvo Šafárik Press, 2019*

Wiewiórowski W., *Profilowanie osób na podstawie ogólnodostępnych danych,* in*: Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym,* ed. A. Mednis, Warszawa 2013

Wiśniewska W., *Przetwarzanie danych wrażliwych w Internecie a RODO. Omówienie wyr. TS z 24 września 2019 r., C-136/17 (GC et al*), Lex

Profilowanie i zautomatyzowane decyzje dotyczące konsumentów na rynku ubezpieczeń a zagrożenie ich prawa do prywatności i prawa do dysponowania swoimi danymi osobowymi

Innowacja w zakresie dostępu zakładów ubezpieczeń do dużych zbiorów danych, które pozwalają zebrać dodatkowe informacje na temat klienta lub zweryfikować podane przez niego dane może przynieść korzyści obu stron, ale tez generować zagrożenia dla konsumenta. Autorka w artykule wskazuje, że na rynku ubezpieczeń gospodarczych należy rozróżnić profilowanie oraz zautomatyzowane podejmowanie decyzji w zależności od sposobu wykorzystania danych osobowych. Ma to znaczenie dla podejmowania decyzji przez zakłady ubezpieczeń w indywidualnych sprawach względem konsumentów bez ich zgody opierając się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu ich danych osobowych. W zakresie analizowanej problematyki został także zaprezentowany obowiązek przekazania konsumentowi informacji o fakcie poddania go zabiegom personalizującym z wykorzystaniem zautomatyzowanych narzędzi analizy danych. Mechanizmy prywatnoprawne konsumenta oparte na przekazywaniu mu informacji i uzyskiwaniu jego zgody mają dyskusyjną skuteczność. Wydaje się, że ochrona danych osobowych w obecnym obrocie konsumenckim powinna być regulowana instrumentami publicznoprawnymi stosowanymi przez organy regulacyjne na poziomie UE i państw członkowskich.

Słowa kluczowe: profilowanie, zautomatyzowane decyzje, przetwarzanie danych osobowych, duże zbiory danych, prawo do prywatności, autonomia informacyjna konsumenta.

DR HAB. MONIKA SZARANIEC, prof. UEK – Cracow University of Economics, College of Economics, Finance, and Law, Institute of Law
e-mail: monika.szaraniec@uek.krakow.pl
ORCID: 0000-0002-3721-3179