FREE MOVEMENT OF DATA IN THE EUROPEAN UNION: OPPORTUNITY OR BIG CHALLENGE IN A USE OF ARTIFICIAL INTELLIGENCE?

Ineta Breskienė[1]

Abstract. This article analyses the current situation in the European Union related to the free movement of data, relationship between personal data, non – personal data and their use in artificial intelligence technology. Despite the European Union's efforts to facilitate the free movement of data, some relevant obstacles are currently being observed. Artificial intelligence technology faces difficulties in using data. Despite the fact that large amounts of data are now increasingly accessible to such technology, its ability to de-anonymize data poses risks of turning simple data into personal data and making its use a challenge for artificial intelligence developers. The issues raised are sensitive and some regulatory changes should be made in the near future in order for the European Union to remain a leader in emerging technologies.
Keywords: Artificial intelligence, personal data, non - personal data, single market, free movement.

INTRODUCTION

Artificial intelligence[2] is one of the most important emerging technologies which is being considered to be strategically and economically significant for the European Union future plans. Artificial intelligence and data are essentially correlated. Without data there is no possibility to develop and compete with artificial intelligence applications in the market. Free movement of data becomes an essential requirement for a successful development of artificial intelligence in the European Union. However, it would not be easy for the European Union to become a leading region in artificial intelligence technology due to a strict legal framework regulation to protect personal data and privacy, which also contains specific sectorical reglamentation. The existing provisions of the European Union law will be applied to artificial intelligence technology regardless its specifics. One of the major obstacles for artificial intelligence to use data freely is the ability of artificial intelligence to

1 *PhD candidate in Law, Vilnius University, Faculty of Law, Department of Private Law, with a dissertation on "Legal Aspects of the Use of Artificial Intelligence". E-mail: ineta.breskiene@tf.vu.lt.*

2 There is no legal term for artificial intelligence which would be set in legal acts. The European Economic and Social Committee (Opinion of the European Economic…, 2017) provides a fairly comprehensive and comprehensible concept of artificial intelligence by emphasizing that it is a very general concept. It states that artificial intelligence is a catch-all term for a large number of sub(fields) such as: cognitive computing (algorithms that reason and understand at a higher (more human) level), machine learning (algorithms that can teach themselves tasks), augmented intelligence (cooperation between human and machine) and artificial intelligence robotics (artificial intelligence imbedded in robots) and the central aim of artificial intelligence research and development is, however, to automate intelligent behaviour such as reasoning, the gathering of information, planning, learning, communicating, manipulating, detecting and even creating, dreaming and perceiving (Opinion of the European Economic..., 2017, p. 3). This article conciders artificial intelligence as independent algorithms which can learn from provided data and teach themselves without needing to be programmed.

analyse data and identify individuals, even if such information is collected in separate databases or is anonymous. The purpose of this work is to analyse and reveal the problematic aspects arising from the regulation of data and its use in the field of artificial intelligence technology in accordance with the legal doctrine, legislation and case law and to discuss what should be done in the future legislation. The subject of this study is focused on the challenges posed by artificial intelligence and its correlation with data protection.

This article further analyses the regulation of the free movement of data in the European Union, the problematic concept of personal data which is identified 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, 2016) (hereinafter referred to as GDPR), artificial intelligence confrontation with some principles set in GDPR. The paper finds out that the aim to creat a single European data sphere and to make the data easily and comfortably accessible and usable for a new technology such as artificial intelligence is possible but limited by strict requirements for the use of personal data and privacy. For the future development of a competetive European artificial intelligence technology the existing regulations should be reviewed, supporting legal acts or quidelines should be provided.

1. FREE MOVEMENT OF DATA IN THE EUROPEAN UNION

Even though currently the European Union has officially established four freedoms (of free movement of people, goods, services and capital), the free movement of data has been called the fifth freedom which complements the existing ones. Recently some important moves have been made towards the single data market and hopfully a better future reglamentation for the use of data. This year the European Commission has published a European strategy for data (A European strategy for data, 2020) (hereinafter referred to as A European strategy for data). The strategy states that the main aim is to create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data (A European strategy for data, 2020, p. 4-5). This strategy is not the first attempt to make a clear vision of a common European Union single data market. A Digital Single Market Strategy for Europe which was published back in 2015, also stated that member States are therefore not able to inhibit the free movement of personal data on grounds of privacy and personal data protection and any unnecessary restrictions regarding the location of data within the European Union should both be removed and prevented (A Digital Single Market Strategy for Europe, 2015, p. 15). The main question is what has been done till now that the free movement of data can be broadly called a freedom without unnecessary restrictions?

Data can be divided into personal data, non-personal data and mixed data. Personal data is an exceptional value in the European Union, and it falls within the scope of the GDPR. Too broad definition

of personal data is a problematic issue regarding the implementation and usage of artificial intelligence which will be discussed further. Non – personal data is regulated by Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Regulation on the free flow..., 2018) (hereinafter referred to as Regulation on the free flow of non-personal data), which is aimed at opening up a better access to electronic data that will contribute to technological progress, including artificial intelligence. This Regulation on the free flow of non-personal data defines the data as other than a personal set in the GDPR. In other words, non – personal data is such data which was previously considered as personal data, but latter was depersonalized and became anonymous, or it may be such data which does not have any interface to an identified or identifiable natural person. Regulation on the free flow of non-personal data complements the existing legislation in data field[3] and tries to create integral and solid legal framework for the free movement of data in the single market.

In mixed data sets it is also very important to identify which data can be used for artificial intelligence without additional requirements. The Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union (Guidance on the Regulation on..., 2019) explains the rules of data use. It says that in the case of a dataset composed of both personal and non-personal data the Regulation on the Free Flow of Non-Personal Data applies to the non-personal data part of the dataset and the GDPR applies to the personal data part of the dataset, but then the non-personal and personal data parts are "inextricably linked"[4], the data protection rights and obligations rising from the GDPR fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset (Guidance on the Regulation on..., 2019). Normally in practice it is technically difficult or very expensive to divide data sets to personal and non – personal data. It seems that basically when using mixed data in artificial intelligence, almost at all times it will be necessary to apply the GDPR requirements.

The European Union's position is very active in creating a single data market. Beside the mentioned Regulations other legal acts concerning data issues have also been adopted[5], making a part of the policy on digital single market. Nevertheless, even thought it seems that the European Union has made the main decisions which facilitate the data movement and are very important for the

3 Regulation on the free flow of non-personal data supplements GDPR, Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Police Directive) and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

4 The term "inextricably linked" first used in the Regulation on the Free Flow of Non-Personal Data is not defined in the same Regulation, nor it is possible to find the meaning in GDPR as well. However Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union the term "inextricably linked" explains as a situation whereby a dataset contains personal data as well as non-personal data and separating the two would either be impossible or considered by the controller to be economically inefficient or not technically feasible (Guidance on the Regulation on..., 2019).

5 For more detailed information see A European strategy for data, 2020, p.4.

artificial intelligence development, going deeper, the use of data in this technology is not so smooth. Does these Regulations[6] really make the data movement easier in a use of artificial intelligence tools and guaranty an easy flow of data? Or does they create obstacles for improvement and it is time to rethink some issues related to artificial intelligence?

2. PERSONAL DATA OR JUST DATA? A THIN LINE OF ASSESSMENT

The availability of large-scale data sets is crucial for the development of artificial intelligence. It is the basis for this technology to learn and achieve results. But what data can be used for artificial intelligence without major constraints? The European Union seeking to become a world leader in smart technologies field announced Regulation on the free flow of non-personal data which is aimed at opening up better access to data that will contribute to technological progress, including artificial intelligence. As it was mentioned before this legislation ensures the free movement of electronic, non-personal data that is not personalized and does not identify specific individuals or groups of individuals as well prohibits data localisation requirements. However, even if such data is anonymised but combinations of artificial intelligence with data make it possible to trace personal data or where personal and non-personal data are inextricably linked, the provisions of the Regulation on the free flow of non-personal data do not apply and the rules applicable to personal data shall apply. Thus, it is necessary to analyse which data are subject to the provisions of GDPR, which also affect the ability of artificial intelligence to use it in the performance of tasks.

GDPR consolidates a very broad definition of personal data. It means any information relating to an identified or identifiable natural person (GDPR, Art. 4 (1)). An identifiable natural person is one who can be identified, directly or indirectly. This takes into account a lot of situations. This extremely broad concept of personal data creates a situation that all data can potentially become personal data in the interaction with artificial intelligence. The European Court of Justice in the case *Patric Breyer (*The European Court of Justice case C582/14 Patrick Breyer v Bundesrepublik Deutschland) explains that the word "indirectly" in the context of personal data indicates that in order for the information to be considered personal it is not necessary that it itself enabled to identify the corresponding person's identity and it is not required that all information would be held by a single person. Accordingly, GDPR recital 26 which also provides an expanded interpretation of the term personal data, stating that the data protection principles should apply to any information about an identified or identifiable natural person. The Article 29 Data Protection Working Party (WP29) has also specified that if the controller intends to keep the data for 10 years it should also assess the possibility to identify and disclose personal data from available data in the ninth year of data retention, in which case all the necessary legal requirements apply for the protection of personal data (Opinion 4/2007 on the concept…, 2007, p. 15). In terms of technological progress, it is clear that data controllers should pay a particular attention to the data provided for artificial intelligence activities.

6 GDPR and Regulation on the Free Flow of Non-Personal Data.

It is possible to distinguish four elements in the concept of personal data, which are closely related and interdependent: the concept of information, the relationship of information with the person, the concept of a natural person and the possibility of identification (Zaleskis, 2019, p. 92-95). Together, as it was mentioned before, these elements presuppose a very broad concept of personal data. In the case under consideration non-personal data may indirectly, in the interaction with other information, identify a natural person and thus become personal data (Bakhoum, *et al*., 2018, p. 199). Data that are not considered personal data, such as metadata, have the potential to fall within the scope of personal data regulation at any time, according to the interactions discussed. When there is a possibility that the identity of a natural person may be revealed in the process of the data and artificial intelligence interaction, GDPR provisions should apply *ex ante* and it also should comply with all requirements (for example, obtaining the data subjects' consent). However, without the disclosure of the natural person's identity by artificial intelligence in the process, this would become a completely unnecessary procedure, becoming only a bureaucratic burden, because it is difficult to predict whether any data may become personal data in the future.

Should the definition of personal data be reviewed in the future? Some authors suggests to keep personal data definition as a threshold of protection, but with a sharper concept, namely, one based on the risk of identification from "0" (zero risk of identification) to "identified", and to treat information with varying degrees of identifiability differently (Schwartz and Solove, 2011, quoted in Purtova, 2018, p. 42). Other author (Purtova, 2018, p. 78-80) claim that there are several options: to narrow the meaning of personal data, or to preserve the broad interpretation of personal data, but reduce the intensity of compliance obligations, for instance by matching the intensity to risks, or to treat all data with the same requirements as for personal data. It is questionable which of these considerations would be the most optimal. Some of these proposals are unlikely to be implemented in accordance with formed case law. Besides the definition of personal data remained the same after GDPR adoption which recently have changed Directive 95/46/EC showing that legislator did not take additional measures to legitimize a different concept or change an extent.

Another issue related with a broad personal data concept is a prohibition of data localisation requirement. The Regulation on the free flow of non-personal data Art. 4 (1) prohibits data localisation requirements unless they are justified on grounds of public security in compliance with the principle of proportionality. The aim is to remove obstacles to non-personal data flow in Member States. The problem is that GDPR does not contain the same broad prohibition on Member States data localisation laws as the Regulation on the free flow of non-personal data, despite the free movement of personal data within the European Union being a central tenant of the GDPR (A new era for EU…, 2019). Art 1 (3) of the GDPR sets that the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. This means that any other restrictions for personal data related with data localisation is possible until it is related with requirements other than personal data protection. This creates legal uncertainty where data in interaction with artificial intelligence may become personal data and after this Member States could still impose data localisation requirements

on personal data for other reasons than those connected with personal data protection (Debussche *et al.*, 2019). This situation may interfere free movement of data because Member States still have a possibility to set data localisation requirements and to disturb cross-border data flows.

According to a recent study ordered by the European Parliament (The impact of the General Data…, 2020, p. 1) numerous artificial intelligence and data protection issues are not answered in the GDPR and data controllers with data subjects should be provided with guidance on how artificial intelligence can be applied to personal data in conformity with GDPR. Future regulation related with artificial intelligence and data should be measured and arising from practice. Any regulatory regime that is designed to govern artificial intelligence needs to take into consideration the GDPR as well as its practical implementation by organisations, to avoid unnecessary duplication of existing and potentially conflicting obligations, ambiguity and legal uncertainty (particularly in heavily regulated sectors) (Artificial Intelligence and Data Protection…, 2020, p.19). It is obvious that the current legal framework is unclear, causing uncertainty and additional legal instruments will be needed in the future. What measures will apply depends on how detailed this problem will be debated and broadcast to decision – making bodies.

3. ARTIFICIAL INTELLIGENCE COMPATIBILITY WITH SOME GDPR PRINCIPLES

Rapid technological development, free movement of data, the exchange of large amounts of data and the unrevealed potential of technology have led to a rather abstract application of GDPR regulation. Only in the use of such technology practical problems and necessary changes become clear. At this stage in the development of artificial intelligence there are several additional challenges. One of the ideas presented in the European strategy for data was the smooth move of data and its use for technologies, but current regulation, especially of the main principles set in GDPR have some gray areas which have to be clarified in the future. Principles are key value indicators which should be followed in applying the provisions of the GDPR. At present, however, these principles pose many uncertainties about their application and compatibility with artificial intelligence technology, their impact on the free movement of data. In this context several principles from GDPR with a significant decisive impact on the use, movement and generation of data in a use of artificial intelligence will be discussed.

Artificial intelligence systems are not well compatible with the storage limitation principle set out in GDPR Article 5 (1) (e), which requires data to be kept in a form that permits the identification of data subjects for no longer than necessary and only for the purposes for which the personal data are processed (General Data Protection Regulation, 2016). GDPR does not provide for specific storage periods. The obligation for the controller to collect, use or store certain data may arise from various legal acts which apply to controllers activities. These time limits arising from legal acts should be considered in line with the principle of storage limitation. Thus, the storage period must be optimal and based on regulatory legislation. For artificial intelligence, which creates a certain end product, it is especially important and relevant to preserve the original information in order to be able to trace, compare and discover what mistakes were made in the development or implementation process

if negative or different results were expected. This is particularly important due to the situation when currently it is difficult to understand the full potential of the artificial intelligence interaction with data. Even with the data controllers' utmost care while dealing with data and by employing all technical and organizational means, the provisions of this principle would still prevail and the data would have to be destroyed.

Another challenge for artificial intelligence systems is compliance with the principle of data minimization set out in paragraph (c) of GDPR Art. 5 (1), which means that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (General Data Protection Regulation, 2016). The data controller should use only the information that is necessary to achieve the purpose and should not be able to collect any additional information that is not provided (even if it arises in the process of learning algorithms). As discussed earlier, artificial intelligence requires large amounts of data to learn, analyse, and make decisions. The variety and amount of data reduces the likelihood of algorithms to act bias and is a guarantee of making more transparent decisions. The requirement for data minimisation hinders free flow of data because by minimizing data to minimum the end product of artificial intelligence technology may be incomplete and not of the best potential it may be. Therefore, already at this stage, the data controller should know very specifically what result should appear and from which data it is intended to be extracted. Due to the specifics of artificial intelligence, it is difficult for the data controller to foresee and predict what artificial intelligence can learn and what results will present as final. In the course of such a process, it is quite likely that not only the purpose may change, but also artificial intelligence may generate, as a result, completely unexpected conclusions and presentations, and in the course of the process, additional data related to the task of artificial intelligence.

Another closely related principle is the purpose limitation principle set in GDPR Art. 5 (1) b which means that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (General Data Protection Regulation, 2016). The purpose of this principle is to limit the data controllers' ability to use the data subjects' personal data in unlimited quantities. As data are collected for certain purposes (defining the purpose of data processing) so firstly, the controller can only collect the data for pre-defined and legitimate purposes, and secondly, the collected data cannot be further processed for those primary purposes in an incompatible way (Zaleskis, 2019, p. 118). In the case of artificial intelligence systems, the data collected from the data subject must be clearly defined and specified, and the necessary information must be explained and provided to the data subject if he or she has to give his or her consent accordingly. However, the process of deploying artificial intelligence systems often requires a variety of personal data that has previously been collected for completely different purposes. For example, the data collected from a Facebook account about a person's activities there is transferred to an artificial intelligence algorithm that determines whether the same person can be mortgaged to secure his obligations (Artificial intelligence and privacy, 2018, p.17). The controller should set sufficiently precise, clear and specific purposes for the processing; very broad purposes for the processing should not be considered appropriate. Therefore, in a situation where previously collected

data could be re-used only in another context, it is necessary to carefully assess whether the purpose is the same. In the case of Facebook such personal data could no longer be used because the purposes of the data are completely different and may have completely different legal consequences for the person; that is why the data subject's consent must be obtained again. The European Parliament underlines that the artificial intelligence developer should always have a clear, unambiguous and informed consent and that artificial intelligence designers have a responsibility to develop and follow procedures for a valid consent, confidentiality, anonymity, fair treatment and due process (A comprehensive European industrial policy*..., 2019*). Taking into account the specific nature of artificial intelligence and its ability to make its own decisions, in some cases it will be difficult to determine at which stage a particular goal has ended and a new one has begun. The consent given by the data subject may only be given for the purposes for which the data subject was informed (General Data Protection Regulation, 2016, Art 4 (11)). In the event of a change of that purpose in the process of artificial intelligence and in the absence of the data subject's consent to another purpose, such consent must be obtained separately.

It should be noted that some of these principles (the principle of purpose limitation and storage limitation) discussed above have several exceptions. In these areas personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (GDPR Art. 5, (b), (e)). The question then arises as to whether the creation and development of artificial intelligence applications using the data could be regarded as one of the exceptions? It is quite likely that the development of artificial intelligence programs in the field of medicine to detect and diagnose different forms of cancer and their prevalence (Newman, 2019) or existing advance in artificial intelligence in radiology (Loria, 2019) suggests that artificial intelligence activities with personal data could indeed be considered as scientific or statistical. Moreover, GDPR recital 159 provides that the processing of personal data for research purposes should be interpreted broadly, including, for example, technological developments, and paragraph 162 provides that any operation of collecting and processing personal data essential for statistical analyses or preparation of statistical results is to be considered as data processed for statistical purposes.The situation could be different with artificial intelligence being used exclusively in the field of commerce; but who could deny the fact that progress or discovery in such an area cannot be applied to the use of artificial intelligence in medicine or any other human welfare activity.

It is already clear that interpreting the principles set in GDPR may take some time. It should be noted that such institution as European Data Protection Board could be more active by providing necessary quidelines.

CONCLUSIONS

1. The European Union tries to create integral and solid legal framework for the free movement of data in the single market. Recently several important regulations were adopted: GDPR and the Regulation on the Free Flow of Non-Personal Data. However, the application of these regulations

in the field of artificial intelligence raises some uncertainties. Legal uncertainty is observed in data protection requirements application for data used in artificial intelligence tools, data localisation requirements, compatibility of the principles set in GDPR with the activities of artificial intelligence. Current legal framework in artificial intelligence and data interaction is not sufficient, causing uncertainty and additional legal instruments will be needed in the future.

2. Artificial intelligence technology is not new in the world, but the rapid growth of data in recent decades has revealed the potential of this technology. Artificial intelligence can use data to create products that can be applied in a variety of areas of life and provide tangible benefits: for example, they are used in health care to detect early stages of cancer. However, one of the most important aspects is related to the fact what data artificial intelligence uses to achieve the goal. The concept of personal data introduced by GDPR Regulation leads to the conclusion that the scope of the Regulation is very wide and can be broadly extended to cover different categories of data: both directly and indirectly related to natural persons. With regard to artificial intelligence, in assessing the ability of this technology to make independent decisions and its unpredictability, it is highly likely that artificial intelligence may link the data provided to it to other available information and thus identify individuals. Therefore, only if there is a possibility that the identity of a natural person may be disclosed, the controller should apply the provisions of the GDPR *ex ante* to the data processed by artificial intelligence and comply with all the requirements.
3. Personal data used by artificial intelligence, or even data that could potentially become personal data, must be subject to the principle of storage limitation, principle of data minimization and the purpose limitation principle. It is difficult to reconcile these principles with the need for artificial intelligence to obtain a variety of data in large quantities. Such a constraint may not only have a significant impact on the development and learning opportunities of artificial intelligence, but also on the overall competitiveness of the European Union in the context of other regions of the world. It should be noted that the GDPR provides a number of exceptions where processing data for longer periods or in the case of purpose limitation, further processing would be allowed if this could be justified in the public interest for archiving, scientific or historical research or statistical purposes. However whether the development of artificial intelligence and its discoveries in various fields (especially science) could not be justified for these purposes remains an open question, as there is still no precedent to justify these objectives.

Bibliography

1. 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). *OJ L 119.*

2. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. *OJ L 303, p. 59.*

3. 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. *OJ L 281.*

4. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *OJ L 201.*

5. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. *OJ L 119.*

6. European Commission. Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions. A European strategy for data. COM(2020) 66 final, accessed 15 May 2020. Accessible via the internet at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>.

7. European Commission. Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions. *A Digital Single Market Strategy for Europe.* COM(2015) 192 final. Accessed 15 May 2020. Accessible via the internet at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192>.

8. European Commission. Communication from the Commission to the European Parliament and the Council. *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*. COM(2019)250 final, accessed 20 May 2020. Accessible via the internet at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN>.

9. European Economic and Social Committee. Opinion of the European Economic and Social Committee on 'Artificial intelligence — The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society' (own-initiative opinion). *OJ C 288.*

10. European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics. *A comprehensive European industrial policy on artificial intelligence and robotics.* Accessed 20 May 2020. Accessible via the internet at: <https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.html>.

11. Article 29 Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data. Accessed 1 June 2020. Accessible via the internet at: <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf>.

12. Ashurst (2019). *A new era for EU data mobility*? Accessed 15 May 2020. Accessible via the internet at: <https://www.ashurst.com/en/news-and-insights/legal-updates/a-new-era-for-eu-data-mobility/>.

13. Bakhoum, M., Gallego, B., C., Mackenrodt, M., O., Namavičienė, G. S. (2018). *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* Springer.

14. Centre for Information Policy Leadership. Hunton Andrews Kurth (2020). *Artificial Intelligence and Data Protection How the GDPR Regulates AI.* Accessed 9 July 2020. Accessible via the internet at: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf>.

15. Debussche, J., Cesar, J., Moortel, I., D. (2019). *Big Data & Issues & Opportunities: Free Flow of Data.* Accessed 10 May 2020. Accessible via the internet at: <https://www.twobirds.com/en/news/articles/2019/global/big-data-issues-and-opportunites-free-flow-of-data#20>.

16. European Parliament (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence.* Accessed 7 July 2020. Accessible via the internet at: <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf>.

17. Loria, K. (2019). *Putting AI in Radiology.* Accessed 29 May 2020. Accessible via the internet at: <https://www.radiologytoday.net/archive/rt0118p10.shtml>.

18. Newman, T. (2019). *Could artificial intelligence be the future of cancer diagnosis?* Accessed 29 May 2020. Accessible via the internet at: https://www.medicalnewstoday.com/articles/325750.php.

19. Purtova, N. (2018). *The law of everything. Broad concept of personal data and future of EU data protection law,* Law, Innovation and Technology, 10:1, 40-81, DOI: 10. 1080/17579961.2018.1452176.

20. The Norwegian Data Protection Authority – Datatilsynet (2018). *Artificial intelligence and privacy*. Accessed 29 May 2020. Accessible via the internet at: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>.

21. Zaleskis, J. (2019). *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė.* Monografy. Vilnius: VĮ Registrų centras.

Case law

22. The European Court of Justice case C582/14 *Patrick Breyer v Bundesrepublik Deutschland*, EU:C:2016:779.