„Krytyka Prawa", tom 13, nr 4/2021, s. 106–118, ISSN 2080-1084, e-ISSN 2450-7938, © 2021 Author.

RASTISLAV FUNTA[1]

Automated Driving and Data Protection: Some Remarks on Fundamental Rights and Privacy[2]

Submitted: 2.07.2021. Accepted: 12.11.2021

Abstract

In case of conventional vehicles, no or very little data was generated. The widespread use of autonomous vehicles, which have a large number of sensors and camera systems in addition to memory modules and carry out permanent data exchange, has the potential to reveal not only the entire living conditions of the passengers, but also those of pedestrians, and others. The increasing networking of vehicles increases efficiency and mobility. On the one hand, this networking is entirely voluntary, but it can also be mandatory, as in the case of the eCall emergency call system. Regulation (EU) 2015/758 made it mandatory for car-manufacturers from March 31, 2018 to equip their vehicles with automatic emergency call system, which in the event of an accident automatically transmits the position and other relevant data to the rescue services. Can this possibility of ubiquitous surveillance may create legal problems.? This increasing role of data requires special attention against the background of data protection based on fundamental rights and privacy.

Keywords: automated driving, data protection, fundamental rights, privacy.

[1] Doc. Dr. Rastislav Funta, Ph.D., LL.M – Janko Jesenský Faculty of Law, Danubius University (Slovakia); e-mail: rastislav.funta@mail.com; ORCID: 0000-0003-4510-4818.

[2] The research has not been supported financially by any institution.

„Krytyka Prawa", tom 13, nr 4/2021, s. 106–118, ISSN 2080-1084, e-ISSN 2450-7938, © 2021 Author.

RASTISLAV FUNTA

Zautomatyzowana jazda samochodem a ochrona danych. Kilka uwag o prawach podstawowych i prywatności[3]

Streszczenie

W przypadku konwencjonalnych pojazdów nie były generowane żadne dane lub tylko niewielka ich ilość. Powszechne korzystanie z pojazdów automatycznych, które oprócz modułów pamięci mają bardzo dużą liczbę czujników i systemów monitoringu i w których stale odbywa się wymiana danych, ma potencjał ujawnienia wszystkich warunków życia nie tylko pasażerów, ale również przechodniów i innych ludzi. Coraz widoczniejsze tworzenie sieci kontaktów między pojazdami pozwala zwiększyć skuteczność i mobilność. Z jednej strony takie tworzenie sieci kontaktów jest całkowicie dobrowolne, ale może się też stać obowiązkowe. To drugie miało miejsce w przypadku systemu połączeń alarmowych eCall. Rozporządzenie (UE) 2015/758 zobligowało producentów samochodów do tego, by począwszy od 31 marca 2018 roku, wyposażali pojazdy w automatyczny system połączeń alarmowych, który w razie wypadku automatycznie przekaże służbom ratowniczym informacje o lokalizacji samochodu oraz inne istotne dane. Czy ta możliwość wszechobecnej ingwilacji może spowodować problemy prawne? Coraz większa rola, którą odgrywają dane, wymaga szczególnej uwagi na tle ochrony danych w oparciu o ochronę danych i prywatność.

Słowa kluczowe: zautomatyzowana jazda samochodem, ochrona danych, prawa podstawowe, prywatność.

[3] Badania nie są finansowane przez żadną instytucję.

 DOI: 10.7206/kp.2080-1084.495

Introduction

The fact that the collection, processing and dissemination of personal data is taking place in more and more areas of life is no longer a surprise. The permanent support of individuals through globally networked technologies is constantly conquering new fields of their deployment. The increasing networking of vehicles aims to increase efficiency and mobility. This increasing role of data requires special attention against the background of data protection[4] based on fundamental rights and privacy.[5]

Data Sensitivity

Conventional passenger vehicles have become data processors. There are sensors for operating the windshield wipers (rain sensors), for operating the headlights (automatic driving light switch), wheel speed (via ABS and ESP sensors) and many more. Obviously, the position data from the navigation system that may be present should be particularly emphasised. There is still no (long-term) storage of this data, although there would be legitimate interests for those involved in the accident and insurance companies if weather conditions, visibility and driving behaviour at the time of the accident are in dispute. Automated driving is not possible without permanent data acquisition and evaluation. The system requires high-precision to track accurate position data. The environment must be accurate with regard to other road users, weather conditions, etc. It should be emphasised that not only data relating to the users of the automated vehicle are generated, but also a lot of 'collateral data'. Vehicles exchange information with one another using the so-called car2car communication. Camera systems for environmental recognition also detect other road users, such as pedestrians, who have no direct reference to the vehicle. Increasing automation of traffic also enables large-scale surveillance of the entire population. This will obviously have an impact on user behaviour. Since vehicles are already equipped with licence plates that (should) identify their owner, anonymity can

4 M. Mesarčík, *Ochrana osobných údajov*, Bratislava 2020.

5 J. Svák, *Ochrana ľudských práv (v troch zväzkoch)*, Bratislava 2011; V. Stehlík, *EU Human Rights Protection Under the Treaty of Lisbon. Human's Rights. The Modern State System's Formation: Theoretical and Practical Aspects*, Kyiv 2009; J. Králik, K. Káliková, *Základná inštitucionálna báza ochrany ľudských práv*, Brno 2007.

hardly be maintained. Even if the vehicle does not directly reveal the name of its user, its identity can be easily determined by analysing the movement profile. Especially for the transition systems that still require intervention by the driver or at least do not exclude it, data about who is driving the vehicle must be recorded. In the interests of state and private law enforcement, it must be established whether the system (or the individual) was responsible in the event of damage.

Legal Basis

European data protection is rooted in Article 8 ECHR (in conjunction with Article 6(3) TEU),[6] as well as in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[7] As a special feature of EU law, the fundamental right to consumer protection (Article 38 of the EU Charter of Fundamental Rights) applies, although it is only a principle within the meaning of Article 52(5) of the EU Charter of Fundamental Rights.[8]

GDPR

According to Article 4(1) EU General Data Protection Regulation (GDPR),[9] personal data is information that relates to an already identified or at least identifiable natural person. Identifiable means that the person can be identified by evaluating an identifier, location data or special features. This legal definition is flanked by recital 26 GDPR. It says that: 'The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such

6 V. Karas, A. Králik, *Právo Európskej únie*, Bratislava 2012.

7 A. Erdösová, *Právny zrod Charty základných práv EÚ – pred a po*, "Bulletin Slovenskej Advokácie" 2010, 9–10; J. Svák, T. Grűnwald, *Nadnárodné systémy ochrany ľudských práv I. zväzok*, Bratislava 2019.

8 J. Jankuv, *Medzinárodné a európske mechanizmy ochrany ľudských práv*, Bratislava 2006; O. Hamulák, D.R. Troitiño, A. Chochia, *La carta de los derechos fundamentales de la union europea y los derechos sociales*, "Estudios Constitucionales" 2018, 1.

9 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) (Text with EEA relevance).

 DOI: 10.7206/kp.2080-1084.495

as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.'

First of all, this means that only personal data should be protected. The focus here is therefore on the protection of the individual.[10] In fact, however, this must be viewed as a particular weak point, especially with regard to automated driving. Due to the rapid technical progress in data processing, the permanent collection of data by service providers may create a hurdle. The exclusion of purely relevant and anonymous data is also a major concern for reasons of privacy. At this point, the question should be: what, in the age of big data, can still be anonymous or not be associated with individuals. The anonymity relates to the individual, but not to groups of individuals, which can be evaluated 'individually anonymously'. The consideration and targeted evaluation of groups of individuals allows conclusions to be drawn about the individual, especially by including other group data, and can thereby restrict his privacy. For instance, if an automated vehicle finds that the vehicle driver needs a break, it can, due to the information from other vehicles regarding their programmed destination (so-called 'car2car communication') predict a certain rest area or recommend another (even less popular one) and thus influence the driver. It remains to be seen how the case law will behave in such situations. The European Court of Justice (ECJ) ruled in the YS et al. case[11] that 'personal data' should be interpreted broadly in the light of the privacy protection standard in Article 1 Data Protection Directive. However, compared to Article 1 Data Protection

[10] M. Daňko, P. Žárská, *Data Protection vs. Intellectual Property*, [in:] R. Funta (ed.), *Počítačové právo, UI, ochrana údajov a najväčšie technologické trendy*, Brno 2019; J. Lazar, A. Dulak, D. Dulaková-Jakúbeková, M. Jurčová, K. Kirstová, M. Novotná, P. Muríň, *Občianske právo hmotné 2. Záväzkové právo: Právo duševného vlastníctva*, Bratislava 2018.

[11] C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, ECLI:EU:C:2014:2081.

Directive, Article 1 GDPR is more limited and no longer contains an explicit reference to the protection of privacy.[12]

Use of Data

Data obtained by the state can only be used if this is necessary in accordance with Article 6(1)(e) in conjunction with 6(3) GDPR for the performance of a public task or if this is done in the exercise of public authority. A public task would be, for instance, the maintenance and enforcement of road safety. The personal data must be processed in a lawful manner. Only data may be collected that is necessary. It may only be stored for as long as is absolutely necessary. The most important principle for all of these points is the maintenance of integrity and confidentiality. Unauthorised third parties must be prevented from accessing the data.[13] In relation to the driver of an automated vehicle, this means that it must first be clear to him or her which authority his or her data is sent to and why this authority may need that data. This prevents misuse of data and the person concerned knows where he can assert his information rights (Article 13 GDPR). It must be also recognisable to the individual that the authority only receives the data that are absolutely necessary for compliance with the legitimate purpose. If the traffic authority collects position data to determine the volume of traffic, it has no legitimate interest in receiving and using the names and addresses of the individuals. Particular user-specific data are problematic against the background of the legitimate purpose and data minimisation. Modern vehicles can not only record position data, but also draw conclusions about their current status by analysing driver behaviour (fatigue detection). For systems in which recourse to the vehicle driver is still possible in emergency situations or there is a possibility of overriding, it would be reasonable to argue that such data would be communicated permanently and directly to the police and driving licence authorities against the background of general road safety. If necessary, it will be the task of the highest (constitutional) courts and European courts to establish a practical link between basic freedoms[14] and road safety in connection with the interests of criminal prosecution.[15] Data storage is also of particular importance. On the one hand, it must be clarified whether, where

12 D.J. Svantesson, *The (Uncertain) Future of Online Data Privacy*, "Masaryk University Journal of Law and Technology" 2015, 2.

13 G. Karácsony, *Managing Personal Data in a Digital Environment – Did GDPR's Concept of Informed Consent Really Give Us Control?*, [in:] R. Funta (ed.), *Počítačové právo, UI, ochrana údajov a najväčšie technologické trendy*, Brno 2019.

14 L. Trellová, *Právo na súkromie v judikatúre Európskeho súdu pre ľudské práva*, Bratislava 2008.

15 L. Klimek, J. Záhora, K. Holcr, *Počítačová kriminalita v európskych súvislostiach*, Bratislava 2016.

 DOI: 10.7206/kp.2080-1084.495

and for how long data may be stored. The resulting data must be allowed to be temporarily stored. In addition, a special justification for the storage is required. Permanent storage without cause may not be possible in view of the storage limitation and the legitimate purpose.

Use of Data by Private Individuals

Initially the focus was on the use of data by public bodies and authorities, but now we have to switch our focus to private services. For instance, companies have an interest in information about road users, as this has great economic value (also the private automobile manufacturers who offer the corresponding vehicles and ensure that they are networked).[16] There is also no need to explain more broadly that companies are already creating large data archives in order to be able to approach customers individually[17] and provide them with 'appropriate' advertising. From the data protection point of view, it is questionable that there are more opportunities for companies to obtain data than for public bodies. According to Article 6(1) GDPR, data processing is possible if the person concerned has given its consent. After that, the consent must be given in an informed and unambiguous manner. Article 7(2) GDPR states that the request for consent must be made in an understandable and easily accessible form and in clear, simple language. From the data protection point of view, it is particularly difficult that Recital 50 GDPR expressly enables data to be processed for purposes other than those for which they were originally collected, provided that they are compatible with the original purposes.[18]

Privacy by Design and Privacy by Default

Article 25 GDPR speaks of data protection through technology design and data protection-friendly default settings. The English, more concise terms of privacy by design and privacy by default have been established for this purpose. On the one hand, this is based on the idea of designing (i.e. programming) data processing systems in such a way that they only obtain really necessary data or that a technology is chosen that requires the least amount of data to be disclosed.[19] This

16 T. Peráček, *The Perspectives of European Society and the European Cooperative as a Form of Entrepreneurship in the Context of the Impact of European Economic Policy*, "Online Journal Modelling the New Europe" 2020, 34.

17 M. Šebesta, P. Šebestová, T. Braxtor, S. Kopčaková, *Perspektíva vývoja práva obchodných spoločností*. Bratislava 2019.

18 M. Rotenberg, J. Scott, J. Horwitz, *Privacy in the Modern Age: The Search for Solutions*, New York 2015.

19 J. Míšek, *Moderní regulatorní metody ochrany osobních údajů*, Brno 2020.

can be done, for instance, using automatic pseudonymisation. For data transmission, it is also possible to choose technologies that, unlike cellular-based transmissions (via SIM card), do not require a sender/receiver assignment. On the other hand, this means that without the person concerned who has voluntarily declared data releases, the system settings are preprogrammed in the most privacy-friendly way. In relation to a vehicle, this means that no more data than absolutely necessary for operation is processed at the factory upon delivery and initial start-up by the driver. Only with the above-mentioned aspects of consent can the data release be expanded.

Special Problem: Data from Third Parties

In the previous considerations, the analysis of data usage was initially limited to the data and information from the driver of the vehicle. However, two other groups will also be detected by the vehicle's sensors. On the one hand, there are those passengers who do not turn on any functions and who also do not set a target or otherwise influence the course of the journey, i.e. only ride along. Many vehicles are already using weight sensors to determine whether the seat belts are fastened for all the seats that are loaded. In modern vehicles, this does not only apply to the driver's seat, but also to the other seats. Unless additional identification options are registered by other sensors, such anonymous weight data will probably not fall within the scope of the GDPR, so as soon as additional data are combined. On the other hand, through the use of camera systems, which cover the area around the automated vehicles as extensively as possible, data about other road users, such as other drivers and passers-by, but also about individuals not participating in the traffic, are recorded. Personal data obtained in this way is subject to the protection of the GDPR. An example here may be a child playing in their parents' private garden, which, since the fence to the street is not opaque, is included in the data processing of the vehicle. If necessary, it forwards this data to a central system for evaluation purposes. It stores this information (video with time/date and location) for the purpose of preserving evidence in the event of an accident. This raises the question of the general admissibility of unjustified surveillance of third parties.[20] In 2014, the ECJ ruled in a case of unjustified surveillance of the public environment of private property, making it inadmissible against the background of the fundamental right of third parties to the protection of privacy.[21] This legal assessment

[20] B. Šramel, P. Horváth, *Internet as the Communication Medium of the 21st Century: Do We Need a Special Legal Regulation of Freedom of Expression on the Internet?*, "The Lawyer Quarterly" 2021, 1.

[21] C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, ECLI:EU:C:2014:2428.

 DOI: 10.7206/kp.2080-1084.495

can be transferred to camera systems for automated driving, so that a general ban would be drawn from it. However, since camera systems are necessary for the operation of such vehicles, a general ban is not effective. One solution could be to justify data processing via Article 6(1)(d) GDPR, as a requirement to protect a vital interest, i.e. protection against (physical) damage in the event of an accident. It is questionable whether such extensive monitoring, especially with the future ubiquity[22] of such vehicles, can still be based on this basis. A further justification could be in Article 6(1)(f) GDPR. This way is discussed, for instance, for so-called 'dash cams'. These are such cameras that permanently record what is happening around the vehicle solely for possible damage in road traffic. Their legitimacy is disputed. In this regard, the German Federal Court of Justice ruled that although permanent recording was not permitted under data protection law, such a record could, after weighing up the conflicting interests, be usable in civil litigation.[23] This decision was ruled based on the old Federal Data Protection Act and not on the GDPR. However, the German Federal Court of Justice also expressly refers to Article 25 GDPR that in favour of its usability (the recording only lasts for a short time and if there are no accidents automatically overwrites itself). The requirement is therefore that the system only stores the relevant data as shortly as possible and removes identifying features independently if possible (privacy by design) through digital retouching or making the data available only in the event of an accident.

Rights of Data Subjects

Articles 13 and 14 GDPR grant extensive rights to information, and Article 15 GDPR provides a right of access by the data subject. This is followed by a right to rectification (Article 16 GDPR), right to erasure (Article 17 GDPR) and right to restriction of processing (Article 18 GDPR). Even damages can be claimed under Article 82 GDPR, whereby not only the person concerned is favoured, but every (in conjunction with the other provisions of the GDPR) person can be actively legitimised. Finally, there is a right to data portability. The claim for damages according to Article 82 GDPR should be dealt with in more detail at this point. A natural person must have suffered material or immaterial damage due to a violation of the GDPR by the person responsible or the processor. The concept of damage is to be interpreted broadly against the background of Recital 146 GDPR. The GDPR does not use the term

22 O. Yara, A. Brazheyev, L. Golovko, V. Bashkatova, *Legal Regulation of the Use of Artificial Intelligence: Problems and Development Prospects*, "European Journal of Sustainable Development" 2021, 1.

23 BGH, 15.05.2018, Az. VI ZR 233/17.

'data subject', i.e. the person whose data is protected, but that of the (natural) person. Consequently, the circle of those protected is larger, it includes both the 'affected' person and third parties, although it is disputed how far the circle of third parties should be drawn. From a vehicle (traffic) perspective, this would be the driver or passenger as the 'affected party' and obviously the other party involved in the accident, as a third party. In any case, according to Article 82(3) GDPR, there is a possibility of exemption from liability[24] by providing evidence of non-responsibility. An example may be as follows: The person has a 'fitness tracker' which had recorded and evaluated health data about himself. Since the person responsible for the use of the data did not take sufficient data security precautions, a third party was able to view, copy and forward this data.[25] If the person concerned is interested in an insurance contract, then a private health insurance company receives information about a special previous damage to the person and excludes the resulting medical treatment costs. Something similar can occur in the context of a loan agreement if the lender has received unlawful data that affects the credit rating of the person. In both cases, the person responsible violated Article 5(1)(f) GDPR, according to which he has to guarantee the integrity and confidentiality of the data. The person suffered direct material damage.[26] A similar example can be seen in the case of road traffic. A driverless vehicle has an accident and the passengers are injured because the data it has to use has been manipulated or was in any case incorrect.[27] Subject to 'classic' claims for damages in the event of traffic accidents it is questionable whether a claim may not also exist under Article 82(1) GDPR. Here, we speak about violations of Article 5(1)(d) and (f) GDPR. The person responsible or the data processor has not protected the accuracy of the data and the integrity of it, so that damage to individuals has occurred. Immaterial damage is also conceivable if, for instance, mental illness is provoked by the accident. The fact that faulty data processing will always have caused the damage in case of driverless vehicles raises doubts. In fact, it should be noted that only data processing that is subject to the protection of the GDPR is protected, i.e. that it must be personal data within the meaning of Article 4(1) GDPR that has been incorrectly

---

24 G. Marchant, R. Lindor, *The Coming Collision Between Autonomous Vehicles and the Liability System*, "Santa Clara Law Review" 2012, 4.

25 R. Funta, *Economic and Legal Features of Digital Markets*, "Danube: Law, Economics and Social Issues Review" 2019, 2.

26 M. Lohmann, *Liability Issues Concerning Self-driving Vehicles*, "European Journal of Risk Regulation" 2016, 2.

27 A. Zakharchenko, T. Peráček, S. Fedushko, Y. Syerov, O. Trach, *When Fact-Checking and 'BBC Standards' Are Helpless: 'Fake Newsworthy Event' Manipulation and the Reaction of the 'High-Quality Media' on It*, "Sustainability" 2021, 2.

 DOI: 10.7206/kp.2080-1084.495

processed, stored, etc.[28] Direct identification data, such as name, age and gender, are less likely to trigger traffic accidents.

Article 20 GDPR, flanked by Recital 68 GDPR, standardises the right of the person concerned to take data with them when changing service provider, so--called data portability. The aim and purpose of this right is to keep the effort and costs of such a change low, not least for reasons of competition.[29] The aim is to avoid the situation that the person concerned does not refrain from using a service provider that is more attractive to him or her for purely pragmatic reasons. A classic example represents e-mail account data, such as address books or profiles in social networks,[30] which one would like to transfer to other service providers. Obviously, the areas of application of Article 20 GDPR are not limited to these services. Data portability is also an essential factor in the field of vehicle-based mobility. The focus here is particularly on changing vehicles. The driver or user of a (driverless) vehicle will want to replace it at some point. During the time, large amounts of data have been produced (during the use of the vehicle), such as popular destinations or routes, as well as information like seat position, radio station, setting of the air conditioning system, etc. An individual driving profile (driving behaviour) may also have been recorded and evaluated.[31] In order to be able to guarantee a simple change to other manufacturers or mobility providers too, data portability is required.

Concluding Remarks

Article 40(2) GDPR standardises the possibility for associations of data processors to set up their own binding rules of conduct that concern their handling of data and data subjects. These codes of conduct can then be approved by the competent supervisory authority in accordance with Article 40(4) GDPR. The supervisory authority also monitors the exercise of these rules in accordance with Article 41(1) GDPR. However, it is questionable whether personal data can actually be used in a data protection-friendly manner.

---

28 R. Polčák, *Právo informačních technologií*, Praha 2018.

29 V. Šmejkal, *Výzvy pro evropský antitrust ve světě vícestranných online platforem*, "Antitrust: Revue Soutěžního Práva" 2016, 4.

30 P. Plavčan, R. Funta, *Some Economic Characteristics of Internet Platforms*, "Danube: Law, Economics and Social Issues Review" 2020, 2.

31 S. Fedushko, O. Mastykash, Y. Syerov, T. Peráček, *Model of User Data Analysis Complex for the Management of Diverse Web Projects During Crises*, "Applied Sciences" 2020, 24.

As shown, the provisions of the GDPR are not yet fully suitable to take sufficient account of the data protection interests of users in regard to automated vehicle systems. In particular, clear regulations regarding the processing and storage of third-party data are required if their anonymity cannot be adequately ensured. Further legislation and judicial specification will be required. For instance, a legal regulation regarding data processing in automated driving would consider the processing and storage of third-party data via Article 6(1)(c) GDPR as a 'necessary legal obligation'. The companies will probably try to make the use of their services dependent not only on data processing, but also on their own data storage. In view of the data processing principles discussed above, this is at least questionable. As discussed above, numerous obstacles in the implementation of automated vehicles and the inadequacy of legal regulations can be recognised. Automated driving will develop, and it remains to be seen whether the legal requirements can keep pace with this development.

Bibliography

Daňko M., Žárská P., *Data Protection vs. Intellectual Property*, [in:] R. Funta (ed.), *Počítačové právo, UI, ochrana údajov a najväčšie technologické trendy*, Brno 2019.

Erdösová A., *Právny zrod Charty základných práv EÚ – pred a po*, "Bulletin Slovenskej Advokácie" 2010, 9–10.

Fedushko S., Mastykash O., Syerov Y., Peráček T., *Model of User Data Analysis Complex for the Management of Diverse Web Projects During Crises*, "Applied Sciences" 2020, 24.

Funta R., *Economic and Legal Features of Digital Markets*, "Danube: Law, Economics and Social Issues Review" 2019, 2.

Hamulák O., Troitiño D.R., Chochia A., *La carta de los derechos fundamentales de la union europea y los derechos sociales*, "Estudios Constitucionales" 2018, 1.

Jankuv J., *Medzinárodné a európske mechanizmy ochrany ľudských práv*, Bratislava 2006.

Karácsony G., *Managing Personal Data in a Digital Environment – Did GDPR's Concept of Informed Consent Really Give Us Control?*, [in:] R. Funta (ed.), *Počítačové právo, UI, ochrana údajov a najväčšie technologické trendy*, Brno 2019.

Karas V., Králik A., *Právo Európskej únie*, Bratislava 2012.

Klimek L., Záhora J., Holcr K., *Počítačová kriminalita v európskych súvislostiach*, Bratislava 2016.

Králik J., Králiková K., *Základná inštitucionálna báza ochrany ľudských práv*, Brno 2007.

Lazar J., Dulak A., Dulaková-Jakúbeková D., Jurčová M., Kirstová K., Novotná M., Muríň P., *Občianske právo hmotné 2. Záväzkové právo: Právo duševného vlastníctva*, Bratislava 2018.

Lohmann M., *Liability Issues Concerning Self-driving Vehicles*, "European Journal of Risk Regulation" 2016, 2.

 DOI: 10.7206/kp.2080-1084.495

Marchant G., Lindor R., *The Coming Collision Between Autonomous Vehicles and the Liability System*, "Santa Clara Law Review" 2012, 4.
Mesarčík M., *Ochrana osobných údajov*, Bratislava 2020.
Míšek J., *Moderní regulatorní metody ochrany osobních údajů*, Brno 2020.
Peráček T., *The Perspectives of European Society and the European Cooperative as a Form of Entrepreneurship in the Context of the Impact of European Economic Policy*, "Online Journal Modelling the New Europe" 2020, 34.
Polčák R., *Právo informačních technologií*, Praha 2018.
Plavčan P., Funta R., *Some Economic Characteristics of Internet Platforms*, "Danube: Law, Economics and Social Issues Review" 2020, 2.
Rotenberg M., Scott J., Horwitz J., *Privacy in the Modern Age: The Search for Solutions*, New York 2015.
Stehlík V., *EU Human Rights Protection Under the Treaty of Lisbon. Human's Rights. The Modern State System's Formation: Theoretical and Practical Aspects*, Kyiv 2009.
Svák J., Grűnwald, T., *Nadnárodné systémy ochrany ľudských práv I. zväzok*, Bratislava 2019.
Svák J., *Ochrana ľudských práv (v troch zväzkoch)*, Bratislava 2011.
Svantesson D.J., *The (Uncertain) Future of Online Data Privacy*, "Masaryk University Journal of Law and Technology" 2015, 2.
Šebesta M., Šebestová P., Braxtor T., Kopčaková S., *Perspektíva vývoja práva obchodných spoločností*, Bratislava 2019.
Šmejkal V., *Výzvy pro evropský antitrust ve světě vícestranných online platforem*, "Antitrust: Revue Soutěžního Práva" 2016, 4.
Šramel B., Horváth P., *Internet as the Communication Medium of the 21st Century: Do We Need a Special Legal Regulation of Freedom of Expression on the Internet?*, "The Lawyer Quarterly" 2021, 1.
Trellová L., *Právo na súkromie v judikatúre Európskeho súdu pre ľudské práva*, Bratislava 2008.
Yara O., Brazheyev A., Golovko L., Bashkatova V., *Legal Regulation of the Use of Artificial Intelligence: Problems and Development Prospects*, "European Journal of Sustainable Development" 2021, 1.
Zakharchenko A., Peráček T., Fedushko S., Syerov Y., Trach O., *When Fact-Checking and 'BBC Standards' Are Helpless: 'Fake Newsworthy Event' Manipulation and the Reaction of the 'High-Quality Media' on It*, "Sustainability" 2021, 2.