OBSAH

Vedecké články

Odborné články

Vedecké články

ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLII
2/2023

JURISDICTION OF THE COURT IN PRE-TRIAL PROCEEDINGS IN THE CZECH REPUBLIC

JUDr. Bc. Denisa Coufalová, PhD.

Univerzita Palackého v Olomouci, Právnická fakulta
Katedra trestního práva
denisa.coufalova7@seznam.cz

Abstract: The article focuses on the topic of determining the jurisdiction of the court in pre-trial criminal proceedings. In the past, the Constitutional Court of the Czech Republic issued an important ruling which raised interpretative issues concerning the determination of the local jurisdiction of the court in pre-trial proceedings. In the context of this ruling, the draft new Criminal Procedure Code submitted by the Commission for the New Criminal Procedure Code will be analysed. The aim of the article is to answer the question whether the proposed wording of the new legislation provides a solution to the problematic issues related to the Constitutional Court's ruling in question. For the time being, the recodification of the criminal procedural law has been postponed, but the text submitted by the Commission may serve for possible future amendments to the effective Criminal Procedure Code, so it is still desirable to deal with the materials produced by the Commission.

Keywords: pre-trial proceedings, criminal proceedings, jurisdiction of the court, judge for pre-trial proceedings, recodification of the Criminal Procedure Code

Introduction

Determining the jurisdiction of the court in pre-trial proceedings, or more precisely, determining local jurisdiction, has in the recent past

aroused controversy in Czech professional discourse.[1] This was due to the fact that the current legislation is not very consistent. In the course of the recodification work on the new Criminal Procedure Code, the Constitutional Court of the Czech Republic (hereinafter referred to as the "Constitutional Court") intervened in the then established interpretation and practice and made a fundamental decision which set a uniform direction for the future procedure of criminal law enforcement authorities in connection with determining the jurisdiction of the court in pre-trial proceedings.[2] This article will briefly outline the impact of the Constitutional Court's decision on practice and theory. It will also highlight problematic issues concerning the legal regulation of the jurisdiction of the court in pre-trial proceedings, which are linked to the interpretation of the Constitutional Court. Last but not least, the proposed legislation submitted by the Commission for the New Criminal Procedure Code (the "Commission") in the framework of the recodification work on the new Criminal Procedure Code will be analysed. **The draft text of the new Criminal Procedure Code has so far not been favorably received**,[3] however, the text of the proposal itself is likely to be used for further amendments to the existing Criminal Procedure Code. For this reason, it remains worthwhile to address the effectiveness and quality of the proposed legislation drafted by the Commission. The main aim of this article is to provide an answer to the question of whether the proposed legislation provides a solution to the current problematic aspects linked to an important ruling of the Constitutional Court. The setting of the jurisdiction of the court in pre-trial proceedings is closely related to the new institution of **the pre-trial judge** under consideration and directly affects the functionality of this subject of criminal proceedings[4]

[1] POCHYLÁ, Veronika. Přípravné řízení de lege ferenda: Soudce práv a svobod. *Trestněprávní revue*, 2017, vol. 11-12, p. 260.

[2] ŘÍHA, Jiří. Rozhodování soudce v přípravném řízení a jeho příslušnost – současnost a budoucnost. *Státní zastupitelství*, 2017, vol. 5, p. 13.

[3] Cf. information on the Czech Justice website, [cit. 24 August 2023] available from: https://www.ceska-justice.cz/2023/05/poslanci-a-senatori-nechteji-novy-trestni-rad-davaji-prednost-upravam-toho-stareho/ or https://www.ceska-justice.cz/2023/05/novy-trestni-rad-je-ve-snemovne-nepruchodny-potvrdil-blazek/.

[4] ŠČERBA, Filip. Pravomoc soudce pro přípravné řízení. *Trestněprávní revue,* 2021, vol. 3, p. 125.

1. Jurisdiction of the court in de lege lata pre-trial proceedings

Under Article 38(1) of the Charter of Fundamental Rights and Freedoms ("CFR"), the jurisdiction of the court and the judge is established by law. The Criminal Procedure Code [5] regulates the jurisdiction of the court in pre-trial proceedings in Section 26, which provides that the district court in whose district the public prosecutor who filed the relevant proposal is active (local jurisdiction) is competent to carry out acts in pre-trial proceedings. The court before which the public prosecutor lodged the application becomes competent to carry out all acts of the court throughout the pre-trial proceedings.[6] In relation to the general provisions of the Code of Criminal Procedure governing subject matter and local jurisdiction (§ 16, § 17 and § 18 of the Code of Criminal Procedure), § 26 of the Code of Criminal Procedure is *lex specialis.*[7]

1.1 Jurisdiction of the court in pre-trial proceedings

With the establishment of the Czech Republic on 1 January 1993, the judicial system was preserved and continued to be conceived as a four-part system (district courts, regional courts, high courts, the Supreme Court of the Czech Republic).[8] Jurisdiction of the court to act in pre-trial proceedings was introduced by Act No. 558/1991 Coll. with effect from 1 January 1992. The wording of Section 26 of the Code of Criminal Procedure was amended by Act No 292/1993 Coll., effective as of 1 January 1994. The explicit wording was supplemented to state that it refers to the **district court**. The intention was, inter alia, to speed up proceedings. Therefore, only the Regional Court, not the High Court, was newly competent as a court of second instance. The amendment also introduced the establishment of the court's jurisdiction throughout

[5] Act No. 141/1961 Coll., on Criminal Procedure (Criminal Procedure Code), as amended.

[6] Unless the case is transferred due to the jurisdiction of another prosecutor acting outside the jurisdiction of this court (Art.26(2) of the Criminal Procedure Code).

[7] HERANOVÁ, Simona. In: JELÍNEK, Jiří a kol. *Trestní právo procesní*. 5. aktualizované a doplněné vydání. Praha: Leges, 2018, p. 209.

[8] ŘÍHA, Jiří. Rozhodování soudce v přípravném řízení a jeho příslušnost…, See footnote 7.

the pre-trial proceedings after the first petition was filed by the public prosecutor. We are thus familiar with this institution even today.[9]

There are exceptions to the rule that the district court is always the court with subject-matter jurisdiction to carry out acts in the pre-trial phase, regardless of the nature of the offence being prosecuted.[10] The Criminal Procedure Code provides for special jurisdiction for certain acts. Section 158e(4) of the Criminal Procedure Code provides for the jurisdiction of the High Court, or the judge of the High Court in whose district the prosecutor of the prosecutor's office filing the application is active, to approve the use of an agent.[11]

1.2 Local jurisdiction of the court and respect for the right to a lawful judge

The interpretation of Section 26 of the Code of Criminal Procedure did not raise doubts or other negative reactions in judicial practice and professional literature for some time (until approximately 2014). However, it was the practice of regional and supreme prosecutors' offices that gradually began to attract criticism. In fact, higher prosecutors could submit their motions for pre-trial actions to all district courts located within their jurisdiction. The Higher State Prosecutor's Office in Olomouc could therefore choose any district court in Moravia. Quite logically, the fear of a deliberate abuse of Article 26 of the Code of Criminal Procedure grew, since the local jurisdiction of the court to decide on the pre-trial proceedings was based solely on the discretion

[9] ŘÍHA, Jiří. Rozhodování soudce v přípravném řízení a jeho příslušnost…, s. 13; § Section 26(2) of the Criminal Procedure Code: *'The court with which the public prosecutor has filed a motion pursuant to paragraph 1 shall become competent to perform all acts of the court throughout the entire preparatory proceedings, unless the case is transferred due to the jurisdiction of another public prosecutor acting outside the jurisdiction of that court*.' This is an expression of the principle of perpetuatio fori, or continuing jurisdiction (PROVAZNÍK, Jan. Právo na zákonného soudce v přípravném řízení trestním. In: KYSELOVSKÁ, Tereza, SPRINGINSFELDOVÁ, Nelly, KŘÁPKOVÁ, Alica, KADLUBIEC, Vojtěch, CHORVÁT, Michal, DRLIČKOVÁ, Klára (eds.), Sborník z konference COFOLA 2017, Brno: Masarykova univerzita v Brně, Právnická fakulta, 2017, p. 241).

[10] DURDÍK, Tomáš. In: DRAŠTÍK, Antonín, FENYK, Jaroslav a kol. *Trestní řád. Komentář.* I. díl. Praha: Wolters Kluwer ČR, a.s., 2017, p. 203.

[11] In the context of the judge's decision on a complaint against a decision of a prosecutor and a police authority pursuant to Section 146a of the Code of Criminal Procedure, the determination of the jurisdiction of the court is not governed by Section 26 of the Code of Criminal Procedure. In such cases, the court acts as a second instance authority and Section 146a of the CC is special in relation to Section 26 of the CC (DURDÍK, Tomáš. In: DRAŠTÍK, Antonín, FENYK, Jaroslav a kol. *Trestní řád. Komentář.* I. díl. Praha: Wolters Kluwer ČR, a.s., 2017, p. 206).

of the prosecutor working at the regional or chief prosecutor's office. Thus, prosecutors could choose according to their "good experience" with particular judges, as they naturally knew in advance the work schedule of the courts in question.[12] It should be noted, however, that no abuse has been proven and the Constitutional Court has not found any violation of fundamental human rights.[13]

The local jurisdiction of the court in pre-trial proceedings is firmly linked to the obligation to respect the right to a lawful judge. I will then outline the importance of respecting the right to a lawful judge in the context of this topic and the impact of the above practice on the activities of the Constitutional Court. More precisely, I will analyse the Constitutional Court's reactions to the criticised legislation, which resulted in two important judgments. The analysis will also include the unresolved issues raised by the first ruling in particular.

1.2.1 The issue of local jurisdiction of the court in pre-trial proceedings in connection with respect for the right to a lawful judge

Respect for the right to a lawful judge in pre-trial proceedings is more specific than in court proceedings and entails the possibility of serious errors that often cannot be corrected. In the first place, the principle applies that a violation of fundamental human rights in criminal proceedings cannot be established where there have been partial errors or breaches of the law, but the proceedings as a whole have been fair. This is a conclusion drawn from the case law of the European Court of Human Rights ("ECtHR").[14] In relation to the right to a lawful judge, the situation is different. The result is not material, which means that it is irrelevant that the illegal judge did some act substantively correct.[15] According to the Constitutional Court, *"the constitutional principle of a lawful judge cannot be circumvented, whatever the reasons for doing so; still less can it be obscured by reference to the 'otherwise substantive correctness' of a decision that was issued in violation of it, ..."*[16] Thus, once it is established that all the acts were decided by a court or judge not having local jurisdiction,

[12] ŘÍHA, Jiří. Rozhodování soudce v přípravném řízení a jeho příslušnost…, p. 13.

[13] Cf. the Resolution of the Constitutional Court of 17 September 2012, Case No. I.ÚS 2632/12 or the Resolution of the Constitutional Court of 21 May 2015, Case No. III.ÚS 2717/13.

[14] E.g. ECtHR judgment of 20 October 2016, Dvorski v. Croatia, no. 25703/11 or ECtHR judgment of 29 November 2016, Lhermitte v. Belgium, no. 34238/09.

[15] PROVAZNÍK, Jan. Právo na zákonného soudce v přípravném řízení trestním…, p. 244.

[16] Ruling of the Constitutional Court of 7 September 2009, Case No. I. ÚS 1922/09, paragraph 15.

the evidence obtained will be seriously flawed and, as a consequence, absolutely ineffective.

Second, the defence only learns about the conduct of the pre-trial proceedings after a delay. This is all the more so if the acts were carried out by a court with no local jurisdiction, which is a significant limitation on the objection of the court's lack of local jurisdiction.[17] The Constitutional Court imposes on the accused (more precisely, on the person against whom the proceedings are being conducted) the requirement of timely raising the objection of an unlawful judge, which it expressed, for example, in its ruling of 6 June 2002, Case No III ÚS 711/01. According to the Constitutional Court, the objection *"... cannot be confused with a procedural means of overturning ex post a decision already made*." The objection must be raised immediately after the accused becomes aware of the existence of the facts justifying it.

1.2.2 The significance of the ruling of the Constitutional Court of 19 April 2016, Pl. ÚS 4/14 and its impact on application practice

In 2014, a group of members of the Chamber of Deputies of the Parliament of the Czech Republic submitted a proposal to repeal Section 15(3), second sentence, and (5) of Ministry of Justice Decree No. 23/1994, on the Rules of Procedure of the State Prosecutor's Office, the establishment of branches of certain State Prosecutor's Offices and details of acts performed by legal waiters, as amended (hereinafter referred to as the "Rules of Procedure of the State Prosecutor's Office"). It is therefore the sub-legislative regulation regulating the jurisdiction of the public prosecutor's office that has been challenged, not Article 26 of the Code of Criminal Procedure.[18] The core of the problem was seen in the fact that the contested legal regulation of the court's jurisdiction for decision-making in pre-trial proceedings was derived from the jurisdiction of the public prosecutor's office, which, however, is not established by Act No. 283/1993 Coll., on the Public Prosecutor's Office (hereinafter also referred to as "the Public Prosecutor's Office

[17] It should be noted that I am not referring here to a situation where the defence knows from the outset that a court with no local jurisdiction is acting in the case and deliberately "saves" the objection for the end of the pre-trial proceedings in order to render any evidence obtained useless (PROVAZNÍK, Jan. Právo na zákonného soudce v přípravném řízení trestním… p. 245-246).

[18] VICHEREK, Roman. Anketa: Jak by podle vašeho názoru měla být v budoucím trestním řádu upravena příslušnost soudu v přípravném řízení trestním? *Trestní právo,* 2018, vol. 3, p. 2.

Act"), but by the Rules of Procedure of the Public Prosecutor's Office, i.e. by a "mere" decree.[19]

The Constitutional Court ruled on this proposal of a group of MPs in a landmark ruling of 19 April 2016, Pl. In the Ruling, the Constitutional Court applied "*the principle of the priority of constitutionally consistent interpretation of a legal regulation or its individual provision over its derogation, with the proviso that it is the duty of all public authorities to interpret and apply the law with regard to the requirement to protect fundamental rights and freedoms*." By this Ruling, the Constitutional Court established that if the relevant petition is filed by a prosecutor of a regional or supreme prosecutor's office, the general rules of jurisdiction of courts in the Code of Criminal Procedure apply and the local jurisdiction of the district court is determined according to the criteria set out in Article 18 of the Code of Criminal Procedure. This interpretation is constitutionally consistent and in accordance with Article 38(1) of the CFR.[20] That interpretation, however, raised **new procedural problems**. The Constitutional Court did not even hint at a solution to the disputed issues raised, although a number of problems were pointed out in the so-called separate votum. Thus, to this day, no clear solution or procedure has been established for some of the problematic aspects.

1.2.3 Interpretive problems associated with the Ruling

One of the problems linked to the Award is its **prospective effect** (*ex nunc*), which is explicitly mentioned in paragraph 120 of the Award. This means that in proceedings where the jurisdiction of the court has already been established pursuant to Article 26(2) of the CPC, although it was established contrary to its conclusions, according to the Constitutional Court, the conclusions arising from the Ruling cannot be applied retrospectively. It can thus be said that the Constitutional Court has thus approved the previously established local jurisdiction of the court for pre-trial proceedings and that this jurisdiction, established according to previous practice, is not affected by any defect.[21] If at the time before the issuance of the Ruling the local jurisdiction pursuant to Section 26(1) of the Criminal Procedure Code was established at the district court, but it did not meet the requirements of the Ruling, in order

[19] PROVAZNÍK, Jan. Právo na zákonného soudce v přípravném řízení trestním…, p. 242.

[20] VICHEREK, Roman. Anketa: Jak by podle vašeho názoru měla být v budoucím trestním řádu upravena příslušnost soudu v přípravném řízení trestním? *Trestní právo,* 2018, vol. 3, p. 2.

[21] PROVAZNÍK, Jan. Právo na zákonného soudce v přípravném řízení trestním… p. 247-248.

to preserve the right to a lawful judge, the first immediately subsequent motion to perform an act in the pre-trial proceedings had to be filed with a court that met the criteria set out in the Ruling. For the period preceding the Ruling, the right to a lawful judge remains.[22]

Another problem arose in connection with **the determination of the court with local jurisdiction** for the first act in pre-trial proceedings pursuant to Section 18 of the Code of Criminal Procedure. In particular, the amount of effort that the prosecuting authorities had to expend to determine the court with territorial jurisdiction was problematic, if the criteria under Article 18 of the Code of Criminal Procedure were not entirely clear in the case.[23] On this issue, the Constitutional Court provided guidance in a later ruling.[24] The requirements for justifying the choice of the court with territorial jurisdiction will be lower at the beginning of the pre-trial phase due to the very nature of the early stage of the proceedings, lack of relevant information, etc. However, this does not mean that the prosecuting authorities are not obliged to give proper reasons for the choice of the court with territorial jurisdiction for pre-trial proceedings. Some 'relief' is granted to the prosecuting authorities where the local jurisdiction of the court is quite clear (e.g. the act clearly took place within the jurisdiction of one court). In this situation, no special justification is needed.

Another problematic aspect related to the Ruling was that the Ruling did not even present a solution to the possible emergence of **competence disputes** related to the application of Article 18 of the CPC in cases where the procedure according to the criteria in question would be ambiguous. The increased risk of conflicts of competence is all the more serious in the context of the short time limits in the pre-trial proceedings for the performance of acts. If a decision is taken on an application for remand in custody, where a decision must be taken within 24 hours of its submission, and the court will not consider itself competent to decide, it will be virtually impossible to resolve such a competence dispute within the statutory time limit.[25]

A possible future problem could be the interpretation of Section 26(2) of the CPC, which allows the principle of continuing jurisdiction to be broken in a situation where a case is transferred due to the jurisdiction of another prosecutor acting outside the jurisdiction of the

[22] Resolution of the Constitutional Court of 13 December 2016, Case No. II.ÚS 3327/16.
[23] PROVAZNÍK, Jan. Právo na zákonného soudce v přípravném řízení trestním… p. 248.
[24] Ruling of the Constitutional Court of 31 January 2017, Case No. II ÚS 4051/16.
[25] ŘÍHA, Jiří. Rozhodování soudce v přípravném řízení a jeho příslušnost…, p. 13.

court where the first proposal in the case was filed. Such situations will probably not be frequent, but their occurrence cannot be ruled out.[26]

The ruling also did not address the procedure in the case of filing a proposal with the court where the judge whose criminal activity is to be heard sits. Alternatively, there is some other reason why the case should not be heard in that court because all judges are disqualified. In such circumstances, the procedure of applying to another district court for a writ of certiorari would certainly be justified. However, after the Ruling, such a possibility is not allowed. An analogous use of Article 25 of the Code of Civil Procedure is offered as a solution.[27] The public prosecutor would, before filing a motion to take action, seek to remove the case from the court where the filing of the motion would be inappropriate or illegal, even though under the rules for assessing local jurisdiction that court would otherwise have jurisdiction to take action. The transfer of the case to another district court would be decided by the regional court, which would be jointly superior to both district courts. This would be a kind of preventive use of analogy, which is in principle permissible in criminal procedural law.[28]

Above, I have highlighted the issues that arose after the publication of the Ruling. I will also outline whether, and if so how, the Commission for the New Criminal Procedure Code has dealt with the above-mentioned interpretative problems in the framework of the recodification work on the new Criminal Procedure Code.

2. Jurisdiction of the court in pre-trial proceedings de lege ferenda

In connection with the recodification of the Criminal Procedure Code, it is proposed to maintain the current situation in the future and to leave the subject matter jurisdiction of the court in pre-trial proceedings in favour of district courts. The legal regulation thus set up is well established, but in connection with the considerations on the

[26] PROVAZNÍK, Jan. Právo na zákonného soudce v přípravném řízení trestním… p. 249.

[27] § Section 25 of the Code of Criminal Procedure regulates the institution of withdrawal and transfer of a case: "For important reasons, a case may be withdrawn from the competent court and transferred to another court of the same type and level; the decision on withdrawal and transfer shall be taken by the court which is the closest joint superior of the two courts."

[28] ŘÍHA, Jiří. Rozhodování soudce v přípravném řízení a jeho příslušnost…, p. 13.

creation of the institute of **a judge for pre-trial proceedings** it acquires a new dimension.[29]

Draft paragraph text of the new Criminal Procedure Code[30] (hereinafter referred to as the "Draft CPC") in Section 26 (c8) (1) provisionally regulates the jurisdiction of the court to perform acts in pre-trial proceedings in such a way that "*the district court, whose local jurisdiction shall be determined in accordance with the general rules, shall have jurisdiction to perform acts in pre-trial proceedings in which the prosecutor of the district prosecutor's office is competent to supervise the maintenance of legality (hereinafter referred to as "supervision")*." The second paragraph states that *"the district court at the seat of the regional court or its branch, the local jurisdiction of which shall be determined in accordance with the general rules, shall have jurisdiction to carry out acts in pre-trial proceedings in which the public prosecutor of the regional or chief public prosecutor's office is competent to exercise supervision; in the case of the Municipal Court in Prague, the District Court for Prague 1 shall have jurisdiction, in the case of the Regional Court in Prague, the District Court Prague-East shall have jurisdiction, in the case of the Regional Court in Plzeň, the District Court Plzeň-City shall have jurisdiction and in the case of the Regional Court in Brno, the Municipal Court in Brno shall have jurisdiction."* At first glance, the wording differs from the current legislation in Section 26 of the Criminal Procedure Code.

2.1 Subject Matter Jurisdiction of the Court or the Preservation of Tradition or a Bold Change?

According to the Draft CPC, subject-matter jurisdiction remains with the district courts, with no exceptions. The Commission based itself on the existing system of courts in force in our territory since 1994. A change in the subject matter jurisdiction of the court to carry out acts in pre-trial proceedings would require a reform of the judiciary. However, the Commission could not have envisaged this when preparing the recodified Criminal Procedure Code, as the Ministry of Justice of the Czech Republic has no plans to change the judicial system in the foreseeable future.[31]

[29] ŘÍHA, Jiří. Rozhodování soudce v přípravném řízení a jeho příslušnost…, p. 13.

[30] Available from: https://www.justice.cz/web/msp/rekodifikace-trestniho-prava-procesniho.

[31] ŘÍHA, Jiří. Trestní soudnictví v zahraničí – mezinárodní srovnání. *Trestněprávní revue*, 2015, č. 5, p. 105.

Despite the fact that the Commission's proposal does not allow for a differently set subject matter jurisdiction of the trial court than the district court, there are opinions among current criminal law experts and criminal law practitioners that a differently set subject matter jurisdiction would be preferable. I will now briefly outline the views in question.

Establishing the jurisdiction of the court in pre-trial proceedings according to the jurisdiction of the prosecutor supervising the pre-trial proceedings and, in connection with this, filing a motion for the performance of an act should be considered precisely with regard to the nature and type of seriousness of the crime under consideration. The pre-trial judge would thus be able to carry out his or her tasks more efficiently, as this situation would better reflect the complexity of the case.[32] Not only the district courts, but also the regional and supreme courts could be competent in the pre-trial proceedings. This setting of jurisdiction is logical and practical. On the other hand, it may seem illogical that in cases of more serious crime, the complexity of such cases is taken into account by the supervision of legality in the pre-trial proceedings by the prosecutor of the regional prosecutor's office, but the nature of the crime is not taken into account in relation to the court's decision-making in the pre-trial proceedings. There are also opinions in the professional discourse that only the regional court should be competent to act in pre-trial proceedings, regardless of the type of seriousness of the case. The division of jurisdiction between district and regional courts is inappropriate because of the potential for disputes over subject matter jurisdiction.[33] The determination of subject-matter jurisdiction in favour of the regional courts is intended to be more convenient on the grounds that the decision-making of judges in pre-trial proceedings may be more difficult than that in the main trial. Decisions must be swift and take into account the case law of the Czech courts and the ECtHR. This relates to the reasons why a judge specialised in criminal law should decide in pre-trial proceedings, not a civil judge. If, in a small district court, the criminal judges are excluded from deciding on the main trial by performing an act in the pre-trial proceedings, a situation could arise where a civil judge would have to decide on the main trial, since the possible bias of all the judges of the criminal division is not a reason for another court to decide on

[32] POCHYLÁ, Veronika. Přípravné řízení de lege ferenda… p. 260.

[33] GŘIVNA, Tomáš. Anketa: Jak by podle vašeho názoru měla být v budoucím trestním řádu upravena příslušnost soudu v přípravném řízení trestním? *Trestní právo,* 2018, vol. 3, p. 2.

the case. There are indeed district courts with fewer than twelve judges. These courts account for one third of the total number of courts. By contrast, there are also district courts with fifty judges. The introduction of county court jurisdiction is intended to be more logical and economical in that it could be 'spread' over several locations, regardless of the existing division of the country.[34] For example, there are two criminal judges at the District Court in Písek, but they simultaneously handle both the criminal and civil agendas. The civil judges also have accessibility. It is highly surprising that the District Court in Prachatice has only one criminal judge, while two other judges simultaneously handle the civil agenda and participate in deciding the T-related agenda (Nt, Tm, Rod, etc.). At the Náchod District Court, two criminal judges decide and one judge deals with both the criminal and civil agenda.[35]

It is also proposed to retain the subject matter jurisdiction of the court in pre-trial proceedings in those district courts in whose district the regional court is located. This alternative makes sense in view of the location of the detention facilities, which are located in or near regional towns. This would eliminate the costs associated with transporting defendants in custody to court. However, the disadvantage of this option may be that it would exacerbate the disparities between district courts. The district courts located in the regional cities would become larger, as a result of which more judges would have to be assigned by the work schedule to deal only with the pre-trial agenda. In other words, these 'large' district courts would have to have several (perhaps more than ten) pre-trial judges.[36] Of the 75 district courts + 10 district courts in Prague and the Municipal Court in Brno (86 in total), the largest district courts are currently the Municipal Court in Brno (76 judges), the District Court in Ostrava (76 judges) and the District Court in Karviná (48 judges).[37] Under this option, the pretrial agenda would be heard in fourteen district courts.

However, most of the above-mentioned options for subject-matter jurisdiction are inappropriate for the time being, in particular because of the current distribution of the judicial system. Concentration of the

[34] VÁVRA, Libor. Anketa: Jak by podle vašeho názoru měla být v budoucím trestním řádu upravena příslušnost soudu v přípravném řízení trestním? *Trestní právo,* 2018, vol. 3, p. 2.

[35] Information is available from the court work schedules for 2023 available on the website of the Ministry of Justice of the Czech Republic justice.cz.

[36] ŘÍHA, Jiří. Příslušnost soudu v přípravném řízení – možnosti a úskalí budoucí právní úpravy. *Trestní právo*, 2018, vol. 3, p. 9.

[37] Czech Judiciary 2021: Annual Statistical Report. Ministry of Justice, 2022 [online]. [cit. 24 August 2023] Available from: https://justice.cz/web/msp/statisticke-udaje-z-oblasti-justice.

pre-trial agenda in regional courts would significantly increase the burden not only on regional courts but also on the superior courts as second instance bodies (the Supreme Court if the superior courts were also competent). The number of cases decided in pre-trial proceedings is considerable and one can foresee really significant consequences, not excluding financial costs (e.g. for transporting files, general travel costs, costs of upgrading technology, etc.). It should also be borne in mind that a pre-trial judge sitting at a regional court could be faced with a difficult situation where he or she simultaneously receives requests to participate in proceedings under Article 158a of the Code of Criminal Procedure at locations which are quite far apart within his or her area of jurisdiction. A similar situation could also apply to the option of concentrating the agenda in the district courts in whose district the regional court is located.[38] The implementation of any of the options would also have an impact on the staffing of police departments. Imagine a situation where a journey of several tens of kilometres would have to be made to the court for each receipt of a decision or criminal file, which would mean that police officers would spend a lot of time travelling instead of working on cases.

If the court system were to be reformed in the future, two or more small district courts could be merged, reducing the number of these district courts and making the court caseload more balanced. The introduction of the institution of the pre-trial judge would also be easier, and the services and substitutability of judges would also be more manageable. The obstacle of judges being excluded from hearing a case in the main trial would also be removed, as a single judge could deal with the pre-trial agenda. The organisational change introduced by the amendment to Act No 6/2002 Coll. on Courts and Judges, as amended, could provide a solution. For the smaller district courts established by law, the pre-trial agenda would be transferred to the larger district courts adjacent to the smaller ones.[39]

According to the explanatory report to the new Criminal Procedure Code ,[40] the current concept of the court's subject matter jurisdiction in pre-trial proceedings should therefore be maintained and only district courts will have subject matter jurisdiction. As stated in Section

[38] ŘÍHA, Jiří. Příslušnost soudu v přípravném řízení – možnosti a úskalí…, p. 9.

[39] Ibid.

[40] The explanatory report to the new Criminal Procedure Code and the text of the new Criminal Procedure Code are available on the website of the Department of Criminal Law of the Faculty of Law of Charles University in Prague: Documents | Law Faculty of Charles University (cuni.cz).

26(2)(c8) of the Draft CPC, in cases where the regional and chief prosecutors' offices will have jurisdiction in the pre-trial proceedings, the district court will also have jurisdiction, but the district court will be the one that is located in the district of the regional court or its branch.[41] This option should prevent the overloading of regional courts, high courts and the Supreme Court, which would very likely occur with the option of determining jurisdiction according to the jurisdiction of the prosecutor's office and with the concentration of the agenda only in regional courts. This is a **rational compromise** that could serve as an incentive to amend the effective Criminal Procedure Code if the recodification of the Criminal Procedure Code does not take place yet.[42]

2.2 Local jurisdiction of the court in pre-trial proceedings under the draft new Criminal Procedure Code

From the outset of its work on the new Criminal Procedure Code, the Commission envisaged a local jurisdiction regime linked to the general rules for determining the local jurisdiction of the court to hear and determine a case, which are set out in Article 18 of the current Criminal Procedure Code.[43] Thus, the Draft CPC explicitly expresses what is now only apparent from the above-mentioned rulings of the Constitutional Court. The first criterion is the place where the offence was committed, the second criterion is the accused's place of residence or work, and the third criterion is the place where the offence was committed.[44] Pursuant to Section 26 (c8) (1) of the Draft CPC, if the prosecutor of the district prosecutor's office will supervise the pre-trial proceedings, the local jurisdiction of the court will be determined according to the general rules. According to Article 26 (c8)(2) of the Draft CPC, if the prosecutor of a higher prosecutor's office (regional or supreme) will supervise the pre-trial proceedings, the *"local jurisdiction shall be the district court at the seat of the regional court or its branch, whose local jurisdiction shall be determined in accordance with the general rules."*

[41] Explanatory Report to the New Criminal Procedure Code - Commentary to Section 26 (c8) of the Draft Criminal Procedure Code, pp. 23-24. Available from: Documents | Law Faculty of Charles University (cuni.cz).

[42] ŘÍHA, Jiří. Příslušnost soudu v přípravném řízení – možnosti a úskalí…, p. 9.

[43] ŘÍHA, Jiří. Příslušnost soudu v přípravném řízení – možnosti a úskalí…, p. 9.

[44] Explanatory Report to the New Criminal Procedure Code - Commentary to Section 26 (c8)(1) and (2) of the Draft Criminal Procedure Code, p. 24. Available from: Documents | Law Faculty of Charles University (cuni.cz).

In order to resolve the issue of jurisdictional disputes, it was suggested that in case of doubt as to jurisdiction, the court should nevertheless decide on the prosecutor's motion to take action and at the same time take other actions that cannot be delayed. The obligation of the court to act even in the case of doubt about jurisdiction applies until the correct court is determined (Article 26 (c8)(4) of the Draft CPC).[45] It can be noted that this wording of the legislation covers a gap in the area on which the Constitutional Court did not comment in its Ruling. Even a court with no local jurisdiction is obliged to take the necessary steps to ensure that the statutory time limits for the performance of acts are complied with. A dispute over jurisdiction must not be detrimental to the speed of proceedings. A dispute over jurisdiction raised by a judge will determine the competent court in the future, and the acts of the court without jurisdiction cannot subsequently be regarded as ineffective.[46] It should be noted that the legal form presented is not ideal. The possibility for the court before which the public prosecutor has filed the application to decide on grounds of urgency allows, de facto and de jure, that the public prosecutor may make the choice of court at his or her discretion.[47]

In order to resolve cases of doubts about the impartiality of judges and situations in which all judges of a given court are excluded, the above-mentioned proposal for the analogous use of the current Article 25 of the Criminal Procedure Code (the so-called delegation). According to § 31 (c13) (2) of the Draft CPC, the solution for these circumstances will be newly regulated directly in the law under the institute of withdrawal and assignment: *"In pre-trial proceedings, a case may be transferred to another court of the same type and level for important reasons, in particular for the reason referred to in paragraph 1(a), before the public prosecutor submits a motion to the*

[45] "Any doubt as to jurisdiction shall not relieve the court with which the public prosecutor has filed a request for action of its obligation to rule on such request within the statutory time limit and to carry out other necessary actions which cannot be delayed until another competent court has been designated."

[46] Explanatory Report to the New Criminal Procedure Code - Commentary to Section 26 (c8)(1) and (2) of the Draft Criminal Procedure Code, p. 25. Available from: Documents | Law Faculty of Charles University (cuni.cz); The fact that acts performed by an incompetent court will not automatically be considered ineffective will not be written into the law. Nevertheless, this idea will be taken into account. Later on, the deciding court will be free to consider whether or not there has been tampering by the prosecutor (ŘÍHA, Jiří. Příslušnost soudu v přípravném řízení – možnosti a úskalí…, p. 9).

[47] GŘIVNA, Tomáš. Anketa: Jak by podle vašeho názoru měla být v budoucím trestním řádu upravena příslušnost soudu v přípravném řízení trestním? *Trestní právo,* 2018, vol. 3, p. 2.

competent court to perform the act; the public prosecutor shall submit the motion to transfer the case to the nearest jointly superior court." The demonstrative example given in Section 31 (c13) (1) (a) of the Draft CPC applies precisely to the exclusion of all judges of a given court from deciding a case. In contrast to the 2008 Substantive Intent of the new Criminal Procedure Code, other court personnel are no longer explicitly mentioned. By inserting the second paragraph into Section 31 (c13) of the Draft CPC, the Court of Criminal Procedure is thus responding to exceptional situations (allegedly in units per year), where the public prosecutor, based on his doubts about the impartiality of judges of a certain court, may file a motion to the regional court, which will designate another court to act in the pre-trial proceedings and subsequently "assign" the case to it. The referral of the case shall be decided by *"the regional court in whose district the district court otherwise having local jurisdiction according to the general rules is located."* In designating a new court, the regional court should not choose a court from the other side of the country. It should assign the case to the court nearest to the one that would otherwise have local jurisdiction. As far as other court staff are concerned, the court's organisational arrangements should be made, as this is not a reason to break the statutory judge rule.[48] This is a special and **optional procedure**, different from the institution of withdrawal and transfer of the case, which has been described as inappropriate and insufficient to ensure the objectivity and confidentiality of the proceedings. Thus, the withdrawal and transfer of the case does not apply even by analogy.

The existing legislation containing the principle of *perpetuatio fori* has been retained in Section 26 (c8)(5) of the Draft CPC.[49] The change in this legislation was the addition of references to provisions concerning decisions on the jurisdiction of the court in cases of jurisdictional disputes and the withdrawal and transfer of a case, including a new treatment of situations relating to the exclusion of judges.

The proposed text of the new Criminal Procedure Code submitted by the Commission is clearly not perfect. The intention was to reach an

[48] For example, the judge himself is the accused, the judge has a close relationship to the accused, the judge is an interested person, the risk of disclosure of classified information, etc. (Explanatory Report to the New Criminal Procedure Code - Commentary to Section 26 (c8) (1) and (2) of the Draft Criminal Procedure Code, pp. 26-27.

[49] "The court designated pursuant to paragraphs 1 to 3 shall become competent to carry out all acts of the court throughout the pre-trial proceedings; this is without prejudice to sections 30 and 31/c12 and section c13."

acceptable compromise, respecting the right to a lawful judge and the necessary preservation of that right.[50] First of all, the Commission's efforts to resolve the interpretation problems associated with the publication of the Constitutional Court's ruling should be highlighted, which in my opinion has been successful. It is indeed difficult to find a flawless and ideal solution. Each option brings with it possible pitfalls and scope for unfair practices. The successful compromise produced by the Commission **may inspire an amendment to the current regulation** of the jurisdiction of the court in pre-trial proceedings in the event that the recodification of the Code of Criminal Procedure is postponed until a later date.

3. Comparison with Slovak legislation

The Slovak Republic is cited as a model for inspiration when considering a change from a four-member court system to a three-member system.[51] For this reason, the legal situation in Slovakia concerning the jurisdiction of the court in pre-trial proceedings will now be outlined.

In Slovakia, the recodification of criminal procedural law took place in 2005. It brought with it several new institutes, including **the pre-trial judge** (*sudca pre prípravné konanie*).[52] With the new Criminal Procedure Code effective as of 1 January 2006 (Act No. 301/2005 Coll., Criminal Procedure Code, as amended, hereinafter referred to as the "CP"), the three-part judicial system - district courts, regional courts and the Supreme Court of the Slovak Republic - was confirmed. A significant change was that, in addition to the district courts, the

[50] ŘÍHA, Jiří. Příslušnost soudu v přípravném řízení – možnosti a úskalí…, p. 9.

[51] ŘÍHA, Jiří. Trestní soudnictví v zahraničí – mezinárodní srovnání. *Trestněprávní revue*, 2015, no. 5, p. 105.

[52] MARKOVÁ, Veronika. Zásada sudcu pre prípravné konanie a niektoré vybrané aplikačné problémy. In HRUŠÁKOVÁ, Milana, PROVAZNÍK, Jan, VALDHANS, Jiří (ed.). *Dny práva 2017, část IX., Zásady trestního práva hmotného i procesního a jejich uplatňování v praxi.* Brno: Masarykova Univerzita, 2018, p. 206. The position of the pre-trial judge is defined in Section 10(3) of the Criminal Procedure Code as a judge of the court of first instance who, before the commencement of criminal prosecution and in preliminary proceedings, decides on interference with fundamental human rights and freedoms, on complaints against decisions of the prosecutor and in other cases provided for in the Criminal Procedure Code. Its status and competence vary depending on the stage of the proceedings at which it carries out its activities (MARKOVÁ, Veronika. Zásada sudcu pre prípravné konanie…, p. 207). For example, the Pre-Trial Judge is empowered under Section 348(1)(a) and (2) of the Criminal Procedure Code to issue a criminal warrant, which he does in his capacity as a single judge.

regional courts no longer ruled at first instance. The first instance agenda was transferred only to the district courts (with the exception of the Specialised Criminal Court). There are 54 district courts in Slovakia, and not every district town is the seat of a district court.[53]

The **district courts** decide by a single judge or in panels on all remaining offences not listed in section 14 of the Criminal Procedure Code. The district courts have a judge for pre-trial proceedings, and the jurisdiction of the court in pre-trial proceedings is laid down in Article 24 of the Code of Criminal Procedure (see below). They are divided into 'ordinary' district courts (54), district courts in the seat of the regional court (8) and district courts referred to in a special law (3), which decide in the first instance on military offences (cf. Article 16(2) of the Code of Criminal Procedure).[54]

The Specialised Criminal Court was created in 2009 as a successor to the Special Court (*Špeciálny súd*). The Specialised Criminal Court decides on criminal and other cases provided for in the Criminal Procedure Code. The Specialised Criminal Court is a court of first instance and has the status of a regional court.[55] It is the only one of its kind, decides in panels of three judges and has nationwide jurisdiction.[56] Section 14 of the Criminal Procedure Code contains an exhaustive list of offences falling within the jurisdiction of the Specialised Criminal Court (e.g. damage to the financial interests of the European Union or premeditated murder). At the same time, the competence of the Office of the Special Prosecutor is thus determined (*Úrad špeciálnej prokuratúry*).[57] If it occurs that the Specialized Criminal Court is unable to make a decision in a particular case (due to the exclusion of judges, etc.), the Regional Court in Banská Bystrica will exercise its jurisdiction.[58] Appeals against decisions of the

[53] ŘÍHA, Jiří. Trestní soudnictví v zahraničí…, p. 105.

[54] Ibid.

[55] Slovakia – national specialised courts. [cit. 24 August 2023] Available from: https://e-justice.europa.eu/content_specialised_courts-19-sk-sk.do?member=1.

[56] ŘÍHA, Jiří. Trestní soudnictví v zahraničí…, p. 105.

[57] PALKOVIČ, Jaroslav. In ČENTÉŠ, Josef a kol. *Trestný poriadok – Veľký komentár*. 3. aktualizované vydanie. Bratislava: EUROKÓDEX, 2017, p. 40.

[58] Section 91 of Act No. 757/2004 Coll., Act on Courts and on Amendments and Additions to Certain Acts, as amended: *"If there is no panel established at the Specialised Criminal Court or if for any other reason the Specialised Criminal Court is unable to exercise its jurisdiction pursuant to this Act or a special act, it shall be exercised by the Regional Court in Banská Bystrica; the panel of the Regional Court shall in such a case consist of three judges, one of whom shall be the chairman of the panel."*

Specialised Criminal Court are decided by the Supreme Court of the Slovak Republic.

The jurisdiction of the court for acts in pre-trial proceedings is therefore regulated by Section 24 of the Criminal Procedure Code, which is a special provision in addition to the general provisions on the subject matter and local jurisdiction of the court (Sections 15, 16 and 17 of the Criminal Procedure Code).[59] The rules determining the jurisdiction of the court for proceedings on the merits are combined with the specifics of pre-trial proceedings.[60] As a general rule, the **district court** which would be competent to hear the indictment proceedings shall be competent to hear the case in the first instance (Article 24(1) of the Code of Criminal Procedure). If the **district court at the seat of the regional court** is competent to hear the case in the first instance (Article 16(1) of the Code of Criminal Procedure), it shall also be competent to hear the pre-trial proceedings (Article 24(2) of the Code of Criminal Procedure). If the district courts are competent in the first instance under Section 16(2) of the Criminal Procedure Code to decide on military offences, they also decide on acts in the pre-trial proceedings. In the cases referred to in Article 16(5) of the Criminal Procedure Code falling within the competence of the Specialised Criminal Court, only the Specialised Criminal Court takes pre-trial measures (Article 24(3) of the Criminal Procedure Code).[61] The above list shows four variants of the jurisdiction of the courts in pre-trial proceedings, in three cases it is a district court and in one case it is a court in the capacity of a regional court.

Slovakia has therefore abandoned the concept of court jurisdiction for pre-trial proceedings as it applies in the Czech Republic. They have introduced a three-judge court system, which, however, entails a complex distinction as to which court will hear the case at first instance. There is a certain disadvantage and a negative side to this complicated division of cases, as the preliminary proceedings often involve a recharacterisation of the offence as a different offence, which, in the case of the Slovak legislation, may also change the jurisdiction of the court to carry out acts in the pre-trial proceedings.[62] The Slovak system is made up of a number of rules and is actually more complex

[59] PALKOVIČ, Jaroslav. In ČENTÉŠ, Josef a kol. *Trestný poriadok…*, p. 54.

[60] ŘÍHA, Jiří. Trestní soudnictví v zahraničí…, p. 105.

[61] Section 24(4) of the Civil Procedure Code also provides for special jurisdiction for exhaustively enumerated acts.

[62] ŘÍHA, Jiří. Příslušnost soudu v přípravném řízení – možnosti a úskalí…, p. 9.

than it may seem. In fact, it does not take advantage of the three-part system, which is supposed to eliminate jurisdictional disputes. On the contrary, the Slovak concept rather increases the risk of jurisdictional disputes, with regard to the four types of cases (as mentioned above), where the jurisdiction is given to three types of district courts and the Specialised Criminal Court. For this reason in particular, Slovakia is not the most suitable model for future reform of the Czech criminal justice system.[63]

Conclusion

De lege ferenda, the Commission's intention was to clarify the rules on the jurisdiction of the court in pre-trial proceedings so as to leave no doubt as to the application of the relevant rules and to cover the resolution of legal issues not covered by the current Criminal Procedure Code. The Commission has opted for a sensible compromise designed to respect the right to a lawful judge and to address the contentious issues raised by the publication of the Ruling.

The district courts should continue to have subject-matter jurisdiction over pre-trial proceedings, as any other solution would require a reform of the judiciary and a change from a four-part system to a three-part system. An intermediate step between the current situation and judicial reform could be an organisational change made by an amendment to the Courts and Judges Act, which would consist in transferring the pre-trial agenda from small district courts to larger district courts adjacent to the small ones.

The current link between the determination of the local jurisdiction of courts in pre-trial proceedings and the general rules on the determination of the local jurisdiction of courts in criminal proceedings should be retained and newly enshrined in law. It should be newly written into the law that if a prosecutor of a higher prosecutor's office (regional or supreme) exercises supervision in pre-trial proceedings, the district court at the seat of the regional court or its branch will have local jurisdiction. Its local jurisdiction shall be determined in accordance with the general rules (together with specifics for certain regional courts).

In order to resolve jurisdictional disputes, it was suggested that even if there is doubt about jurisdiction, the court should nevertheless rule on

[63] ŘÍHA, Jiří. Trestní soudnictví v zahraničí…, p. 105.

the prosecutor's motion to take action and at the same time take other actions that cannot be delayed. The obligation of the court to act even in the event of doubt as to jurisdiction is to remain in force until the competent court has been determined. This jurisdictional dispute will be raised by a judge of a court which does not feel it has jurisdiction. In situations in which all judges of a given court are excluded from deciding, the public prosecutor will be able to apply to the regional court to determine which court will take the required action in the case. The Commission has also maintained the rule of continuing jurisdiction of the court in pre-trial proceedings.

Although the form of legislation presented by the Commission is not perfect, it can be assessed as a very successful attempt to find acceptable solutions to current problematic issues and to incorporate these solutions into the new Criminal Procedure Code. Alternatively, the proposed legislation is suitable for use in amending the current Criminal Procedure Code, as the recodification of the Criminal Procedure Code is unlikely to be implemented in the near future.

The Slovak legislation on the jurisdiction of the court in pre-trial proceedings has been analysed as a possible source of inspiration for the recodification of Czech criminal procedural law. The judicial system in Slovakia is a three-part system compared to the Czech Republic. In pre-trial proceedings, three types of district courts and one specialised court with national jurisdiction are competent to carry out acts in pre-trial proceedings. The division of cases is complicated and the advantages of a three-judge court system, which should minimise jurisdictional disputes, are not actually used. Rather, they increase the risk of jurisdictional disputes. Therefore, the Slovak legislation is not the most appropriate model for a possible judicial reform in the Czech Republic.

Použitá literatura

1. ČENTÉŠ, Josef a kol. *Trestný poriadok – Veľký komentár*. 3. aktualizované vydanie. Bratislava: EUROKÓDEX, 2017, 971 s. ISBN 978-80-8155-070-6.
2. DRAŠTÍK, Antonín, FENYK, Jaroslav a kol. *Trestní řád. Komentář.* I. díl. Praha: Wolters Kluwer ČR, a.s., 2017, 1383 s. ISBN 978-80-7552-600-7.
3. GŘIVNA, Tomáš. Anketa: Jak by podle vašeho názoru měla být v budoucím trestním řádu upravena příslušnost soudu v přípravném

řízení trestním? *Trestní právo* [online databáze], 2018, [cit. 24. srpna 2023]. Dostupné z: databáze noveaspi.cz.
4. JELÍNEK, Jiří a kol. *Trestní právo procesní*. 5. aktualizované a doplněné vydání. Praha: Leges, 2018, 864 s. ISBN 978-80-7502-278-3.
5. MARKOVÁ, Veronika. Zásada sudcu pre prípravné konanie a niektoré vybrané aplikačné problémy. In HRUŠÁKOVÁ, Milana, PROVAZNÍK, Jan, VALDHANS, Jiří (ed.). *Dny práva 2017, část IX., Zásady trestního práva hmotného i procesního a jejich uplatňování v praxi*. Brno: Masarykova Univerzita, 2018, 437 s. ISBN 978-80-210-9046-0.
6. POCHYLÁ, Veronika. Přípravné řízení de lege ferenda: Soudce práv a svobod. *Trestněprávní revue* [online databáze], 2017 [cit. 24. srpna 2023]. Dostupné z: databáze beck-online.cz.
7. PROVAZNÍK, Jan. Právo na zákonného soudce v přípravném řízení trestním. In: KYSELOVSKÁ, Tereza, SPRINGINSFELDOVÁ, Nelly, KŘÁPKOVÁ, Alica, KADLUBIEC, Vojtěch, CHORVÁT, Michal, DRLIČKOVÁ, Klára (eds.), *Sborník z konference COFOLA 2017*, Brno: Masarykova univerzita v Brně, Právnická fakulta, 2017, 1811 s. ISBN 978-80-210-8928-0.
8. ŘÍHA, Jiří. Příslušnost soudu v přípravném řízení – možnosti a úskalí budoucí právní úpravy. *Trestní právo* [online databáze], 2018, [cit. 24. srpna 2023]. Dostupné z: databáze noveaspi.cz.
9. ŘÍHA, Jiří. Rozhodování soudce v přípravném řízení a jeho příslušnost – současnost a budoucnost. *Státní zastupitelství* [online databáze], 2017, [cit. 24. srpna 2023]. Dostupné z: databáze noveaspi.cz.
10. ŘÍHA, Jiří. Trestní soudnictví v zahraničí – mezinárodní srovnání. *Trestněprávní revue* [online databáze], 2015 [cit. 24. srpna 2023]. Dostupné z: databáze beck-online.cz.
11. ŠČERBA, Filip. Pravomoc soudce pro přípravné řízení. *Trestněprávní revue* [online databáze], 2021 [cit. 24. srpna 2023]. Dostupné z: databáze beck-online.cz.
12. VÁVRA, Libor. Anketa: Jak by podle vašeho názoru měla být v budoucím trestním řádu upravena příslušnost soudu v přípravném řízení trestním? *Trestní právo* [online databáze], 2018, [cit. 24. srpna 2023]. Dostupné z: databáze noveaspi.cz.
13. VICHEREK, Roman. Anketa: Jak by podle vašeho názoru měla být v budoucím trestním řádu upravena příslušnost soudu v přípravném řízení trestním? *Trestní právo* [online databáze], 2018, [cit. 24. srpna 2023]. Dostupné z: databáze noveaspi.cz.
14. Nález Ústavního soudu ze dne 6. června 2002, sp. zn. III. ÚS 711/01.
15. Nález Ústavního soudu ze dne 7. září 2009, sp. zn. I. ÚS 1922/09.

16. Nález Ústavního soudu ze dne 19. dubna 2016, sp. zn. Pl. ÚS 4/14.
17. Nález Ústavního soudu ze dne 31. ledna 2017, sp. zn. II. ÚS 4051/16.
18. Usnesení Ústavního soudu ze dne 17. září 2012, sp. zn. I.ÚS 2632/12.
19. Usnesení Ústavního soudu ze dne 21. května 2015, sp. zn. III. ÚS 2717/13.
20. Usnesení Ústavního soudu ze dne 13. prosince 2016, sp. zn. II.ÚS 3327/16.
21. Rozsudek ESLP ze dne 20. října 2016, Dvorski proti Chorvatsku, č. 25703/11.
22. Rozsudek ESLP ze dne 29. listopadu 2016, Lhermitte proti Belgii, č. 34238/09.
23. Zákon č. 301/2005 Z. z., trestný poriadok, v znení neskorších predpisov
24. zákon č. 757/2004 Z. z., zákon o súdoch a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov.
25. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
26. Zákon č. 558/1991 Sb., kterým se mění a doplňuje trestní řád a zákon o ochraně státního tajemství.
27. Zákon č. 292/1993 Sb., kterým se mění a doplňuje zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), zákon č. 21/1992 Sb., o bankách, a zákon č. 335/1991 Sb. o soudech a soudcích.
28. Zákon č. 6/2002 Sb., o soudech a soudcích, ve znění pozdějších předpisů.
29. Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.
30. Vyhláška č. 23/1994 Sb., o jednacím řádu státního zastupitelství, zřízení poboček některých státních zastupitelství a podrobnostech o úkonech prováděných právními čekateli, ve znění pozdějších předpisů.
31. Návrh TŘ ve stavu ke dni 14. října 2022 [online], justice.cz, [cit. 13. května 2023]. Dostupné z: https://tpp.justice.cz/.
32. Důvodová zpráva k Návrhu TŘ [online]. Dostupné z: https://www.prf.cuni.cz/.
33. České soudnictví 2021: Výroční statistická zpráva. Ministerstvo spravedlnosti, 2022 [online]. Dostupné z: https://justice.cz/web/msp/statisticke-udaje-z-oblasti-justice.
34. Slovensko – vnitrostátní specializované soudy. Dostupné z: https://e-justice.europa.eu/content_specialised_courts-19-sk-sk.do?member=1.

ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLII
2/2023

NADOBÚDANIE VLASTNÍCTVA K POĽNOHOSPODÁRSKEJ PÔDE V ZMYSLE PRÁVNEJ ÚPRAVY FRANCÚZSKEJ REPUBLIKY[1]

JUDr. Ľudovít Máčaj, PhD.

Univerzita Komenského v Bratislave, Právnická fakulta
Katedra správneho a environmentálneho práva
ludovit.macaj@flaw.uniba.sk

Nadobúdanie vlastníctva k poľnohospodárskym pozemkom v zmysle právnej úpravy Francúzskej republiky

Článok sa zameriava na možnosti prevodu vlastníctva k poľnohospodárskej pôde v zmysle právnej úpravy Francúzskej republiky. Približuje postavenie poľnohospodárskej pôdy a jej ochrany ako súčasti životného prostredia, ale aj ako predmetu právnych vzťahov. Existujú osobité dôvody, pre ktoré sa zákonodarca rozhodol priznať poľnohospodárskej pôde toto postavenie. Následne článok uvádza postup, ktorý je potrebné dodržať za účelom prevodu vlastníctva k týmto pozemkom. Poľnohospodárske pozemky nepredstavujú tovar a bežný predmet právnych vzťahov, ale zasluhujú si zvláštnu ochranu, ku ktorej tento postup smeruje. Osobitné postavenie má v tomto prípade orgán SAFER, ktorého aktivita je zameraná na ochranu vidieka a poľnohospodárstva v regiónoch. Jeho činnosť je osobitá aj v rámci celej Európskej únie. Článok nakoniec porovnáva túto právnu úpravu so situáciou v Slovenskej republike a prináša niekoľko úvah.

Acquisition of ownership of agricultural land in accordance with the legislation of the French Republic

The article focuses on the possibilities of transferring ownership to agricultural land in terms of the legislation of the French Republic. It approximates the local definition of agricultural land and its protection as part of the environment, but also as a subject of legal relations. There

[1] Príspevok bol spracovaný v rámci riešenia grantu č. APVV-19-0494 s názvom „Efektívne pozemkové úpravy“ udeleného Agentúrou na podporu výskumu a vývoja (APVV).

are special reasons why the legislator decided to grant agricultural land this status. Subsequently, the article states the procedure that must be followed to transfer ownership of these plots of land. Agricultural land is not a commodity and a common object of legal relations, but it deserves the special protection that this procedure leads to. In this case, the SAFER body has a special position, whose activity is focused on the protection of the countryside and agriculture in the regions. Its activity is unique even within the entire European Union. Finally, the article compares this legal arrangement with the situation in the Slovak Republic and brings several considerations.

Kľúčové slová: ochrana pôdy, nadobúdanie vlastníctva, Francúzsko, komparácia

Keywords: land protection, acquisition of property, France, comparison

Úvod

Problematika nadobúdania vlastníckeho práva k pozemkom predstavujúcim poľnohospodársku pôdu je témou, ktorá rezonuje v politických a spoločenských debatách vo viacerých štátoch. Je to samozrejmé, keďže je hlavným zdrojom a základným výrobným prostriedkom pre poľnohospodárstvo, lebo sa na nej produkuje rastlinná výroba, rovnako predstavuje základ pre rozvoj živočíšnej výroby.[2] Hoci podiel poľnohospodárstva na celkovom hrubom domácom produkte štátov v poslednej dobe kontinuálne klesá (aj keď s niekoľkými výnimkami)[3], celospoločenský význam je stále výrazný. A to najmä s ohľadom na rozvoj vidieka a lokálnu ekonomiku, čo sú však skutočnosti ťažko merateľné.

Francúzska republika je členským štátom Európskej únie s najväčšou územnou rozlohou (a to aj v prípade, ak berieme do úvahy len metropolitné Francúzsko). Podiel poľnohospodárstva na ekonomike tohto štátu je dlhodobo nízky, pričom k veľkému poklesu celospoločenského významu poľnohospodárstva došlo najmä v druhej

[2] ŠTEFANOVIČ, M.: *Pozemkové právo*. Bratislava: EUROUNION, 2010, s. 82.

[3] Agriculture, forestry and fishing. The World Bank Data. Dostupné na: https://data.worldbank.org/indicator/NV.AGR.TOTL.ZS [cit. 25.09.2023].

polovici dvadsiateho storočia.[4] V posledných dvadsiatich rokoch sa pohybuje na úrovni 1,32 – 1,85 %, hoci v ostatných rokoch má mierne stúpajúcu tendenciu.[5] Napriek týmto okolnostiam je však spoločenský význam poľnohospodárstva v republike naďalej výrazný, čo môžeme sledovať aj v prípade rôznych politických otázok a problémov, ako sú napríklad štrajky poľnohospodárov.[6] Práve s týmto osobitým postavením poľnohospodárstva v štáte súvisí aj skutočnosť, že pozemky predstavujúce poľnohospodársku pôdu majú priznané osobité postavenie a ochranu v tom zmysle, že nie sú považované za tovar a bežný predmet právnych vzťahov.

V tomto prípade ide o dlhodobo prezentovaný a podporovaný pohľad na poľnohospodársku pôdu ako predpoklad vykonávania poľnohospodárskej výroby. *Problematika obhospodarovania pôdy a poľnohospodárskej pôdy sa potom javila ako neoddeliteľná od rozvoja a obnovy poľnohospodárstva, ako aj jeho kapacity produkovať značné objemy kvalitných potravinárskych výrobkov*.[7]

Cieľom tohto článku je preto vymedzenie osobitného postavenia pozemkov predstavujúcich poľnohospodársku pôdu v zmysle francúzskej právnej úpravy, a to najmä s ohľadom na nadobúdanie tohto vlastníctva. Nepôjdeme pritom do prílišných detailov, ktoré by prekračovali možný rozsah, práve naopak, snažíme sa v krátkosti a prehľadnosti poukázať na osobitosti tohto systému.

V článku pracujeme s hypotézou, že francúzska právna úprava ochrany poľnohospodárskej pôdy je dostatočne účelná a efektívna pre dosiahnutie účelu ochrany tejto pôdy ako zložky životného prostredia, no najmä nástroja poľnohospodárstva. V závere článku túto hypotézu verifikujeme, alebo prípadne spochybníme.

---

[4] V roku 1955 malo Francúzsko 2,3 milióna poľnohospodárskych podnikov. v roku 2003 ich zostávalo len 590 000. V roku 2000 žili farmách dva milióny ľudí, čo je štyrikrát menej ako v roku 1955. Porovnajte: DESRIERS, Maurice. L'agriculture française depuis cinquante ans: des petites exploitations familiales aux droits à paiement unique. *Agreste cahiers*, 2007, 2: 3-14.

[5] Share of agriculture, fisheries and forestry in GDP in France from 2003 to 2022. Statista.com. Dostupné na: https://www.statista.com/statistics/1107173/share-of-agriculture-in-french-gdp/ [cit. 25.09.2023].

[6] Napríklad porovnajte: Manifeste agricole à Paris. Dostupné na: https://www.ladepeche.fr/2023/02/08/manifestation-agricole-a-paris-prix-de-lenergie-pesticides-secheresse-pourquoi-les-agriculteurs-sont-ils-en-colere-10984238.php [cit. 25.09.2023].

[7] TORRE, A. – WALLET, F. – HUANG, J.: Le foncier agricole, nouvel enjeu des politiques d'aménagement de l'espace. In *Économie rurale*, 2023, č. 383, s. 8.

1. Poľnohospodárska pôda podľa francúzskej právnej úpravy

Ako najdôležitejší pojem na úseku ochrany poľnohospodárskej pôdy, v prvom rade ako predmetu vlastníctva, ale rovnako tak aj ako zložky životného prostredia, môžeme označiť samotnú poľnohospodársku pôdu *(le foncier agricole)*. V tomto prípade sa jedná o vymedzenie druhovej kvality zemského povrchu, teda príslušnej kultúry, ktorá sa tam na určitom pozemku nachádza.

Na účely evidencie pozemkového vlastníctva sa však využívajú aj osobitné jednotky. Základným nástrojom pre evidenciu poľnohospodárskej pôdy vo Francúzsku sú tzv. jednotky SAU (*la surface agricole utile*), teda úžitkové poľnohospodárske plochy (ďalej len „SAU“). Slúžia na vymedzenie druhu pozemku a evidenciu poľnohospodárskej pôdy. SAU však nie sú pojmom s legálnou definíciou, napriek tomu tento pojem využívajú viaceré právne predpisy na tomto úseku.

Rovnako sa môžeme stretnúť aj s pojmom tzv. celkovej poľnohospodárskej plochy (la surface agricole totale, ďalej len „SAT“), ktorý sa však používa väčšmi v celkových súvislostiach a pri zohľadnení celkovej výmery poľnohospodárskej pôdy využívanej k poľnohospodárskej výrobe na určitom území. Môžeme sa s ním teda stretnúť napríklad pri európskej regulácii nariadeniami a smernicami.

Celková výmera poľnohospodárskej pôdy vo Francúzsku sa do značnej miery odlišuje v závislosti od toho, o aký región sa jedná. V prípade metropolitného Francúzska sa však jedná o pomerne vysoký podiel, a to v priemere 52 %.[8]

Z hľadiska legislatívy možno konštatovať, že francúzska právna úprava je založená na veľkých kódexoch jednotne a komplexne vymedzujúcich určitú oblasť spoločenských vzťahov. V porovnaní so slovenskou právnou úpravou, ktorá sa nachádza v mnohých právnych predpisoch čiastkovo upravujúcich určitú problematiku, ide teda o pomerne jednotnú právnu úpravu. Tá je zároveň dostatočne všeobecná, aby nemusela podliehať príliš častým novelizáciám, a na druhej strane sa v značnej miere vyhýba definíciám a pojmológii, čo je tradíciou väčšmi v prípade Slovenskej republiky.

[8] Najvyšší podiel poľnohospodárskej pôdy využívanej na poľnohospodársku výrobu majú regióny Normandie, Pays de la Loire a Centre – Val de Loire, s podielom 68 až 69%. Je možné porovnať – Identité agricole des régions. Dostupné na: https://www.insee.fr/fr/statistiques/5039859?sommaire=5040030 [cit. 25.09.2023].

Pokiaľ teda rozoberáme francúzsku právnu úpravu na úseku nakladania a využívania poľnohospodárskej pôdy, na prvom mieste musíme zmieniť Vidiecky zákonník a zákonník námorného rybolovu (*Code rural et et de la pêche maritime*), ďalej len „Vidiecky zákonník". Aj v tomto prípade teda ide o právny kódex, ktorý patrí do medzi viaceré francúzske špecializované kódexy. Pôvodne sa nazýval iba Vidiecky zákonník. Vo svojej prvej forme bol vydaný už počas Tretej republiky, hoci diskusie o jeho prijatí existovali ešte oveľa skôr. Neskôr ho nahradili novšie vidiecke kódexy, pričom významným bol najmä vidiecky zákonník dnes označovaný aj ako starý (*ancien*), prijatý v roku 1955. Nový a dosiaľ posledný vidiecky zákonník bol prijatý v roku 1982, ktorý sa vyvíjal postupne od roku 1980. Ten prechádzal a dodnes prechádza mnohými novelizáciami, pričom v roku 2010 sa v dôsledku novelizácie stal kódexom vidieckeho a námorného rybolovu, keď do jeho obsahu dostali aj ustanovenia o námornom rybolove.

2. Ochrana pôdy a ochrana vlastníctva pôdy

Vo väčšine štátov vyspelého sveta patrí poľnohospodárska pôda k statkom, ktoré si zaslúžia osobitné postavenie a opateru štátu a spoločnosti. Inak povedané, nenakladá sa s ňou ako s bežnou vecou a nepredstavuje tovar v hospodárskom slova zmysle.[9] Je to spôsobené tým, že poľnohospodárska pôda (spolu s lesnou pôdou) predstavuje vyčerpateľný a v zásade neobnoviteľný zdroj pre pôdohospodárstvo toho-ktorého štátu. Jednotlivé štáty preto prijímajú osobitú legislatívu na tomto úseku, ktorá má viesť k jej ochrane.

V zásade môžeme rozoznávať dva prístupy k tejto ochrane. Prvým je ochrana poľnohospodárskej pôdy ako zložky životného prostredia, ako aj zvláštneho druhu ekosystému, ktorý na tejto pôde vzniká v dôsledku poľnohospodárskej aktivity človeka. Samozrejme, aj táto ochrana sa odlišuje v závislosti od toho, o aký druh pôdy sa na danom pozemku jedná.

Na druhej strane môžeme vnímať ochranu poľnohospodárskej pôdy aj ako ochranu práv viažucu sa ku konkrétnym pozemkom, ako veciam, inak povedané, k predmetom rôznych práv (najmä vlastníckych a iných vecných práv, ale rovnako tak aj užívacích a iných práv). Táto ochrana

[9] PAVLOVIČ, M.: Vplyv ústavnej ochrany pôdy na vývoj pozemkového práva. In *Půda v právních vztazích - aktuální otázky*. Brno : Masarykova univerzita, 2019, s. 44.

je v mnohých prípadoch nevyhnutná na zabezpečenie starostlivosti a ochrany poľnohospodárskej pôdy, tak ako ju opisujeme vyššie.

Jednotlivé štáty za týmto účelom prijímajú rôzne opatrenia, ktoré sa týkajú napríklad spôsobom nakladania s vlastníctvom pozemkov predstavujúcich poľnohospodársku pôdu. Na Slovensku to bolo najmä v súvislosti s ustanoveniami zákona č. 140/2014 Z. z. o nadobúdaní vlastníctva poľnohospodárskeho pozemku a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.[10] Tento predpis zavádzal tzv. ponukový systém predkupných práv k poľnohospodárskym pozemkom, ktoré bolo nevyhnutné dodržať pri prevodoch ich vlastníctva. Tento systém bol však zrušený v súlade s nálezom Ústavného súdu Slovenskej republiky sp. zn. PL. ÚS 20/2014 zo 14. novembra 2018, ktorý poukázal na rozpor predmetných ustanovení s Ústavou Slovenskej republiky. Na druhej strane v predmetnom čase začala Európska komisia voči Slovenskej republike konanie v danej veci, keďže vznikli podozrenia, že daná legislatíva je v rozpore s právom Európskej únie, a to konkrétne so základnými slobodami vnútorného trhu (voľný pohyb tovarov, služieb, kapitálu a osôb).

V momentálnej situácii preto Slovenská republika nadobúdanie vlastníctva poľnohospodárskej pôdy osobitne nereguluje, s výnimkou zákonného pravidla, podľa ktorého *nadobúdať poľnohospodársky pozemok do vlastníctva nemôže štát, občan štátu, fyzická osoba s pobytom alebo právnická osoba so sídlom v štáte, ktorého právny poriadok neumožňuje občanom Slovenskej republiky, fyzickým osobám s pobytom v Slovenskej republike ani právnickým osobám so sídlom v Slovenskej republike nadobúdať vlastníctvo k poľnohospodárskemu pozemku*.[11]

Na druhej strane je však potrebné uviesť, že mnohé iné členské štáty Európskej únie disponujú vlastnou legislatívou na úseku ochrany poľnohospodárskej pôdy, ktorá nebola a nie je spochybňovaná ani inštitúciami Európskej únie. Jedným z takých prípadov je aj legislatíva Francúzskej republiky, na ktorú sa v ďalšom texte viacej zameriavame.

[10] PAVLOVIČ, M.: Ústavné východiská pre reguláciu trhu s pôdou. In *Comenius* [elektronický dokument]. – č. október (2021).

[11] S výnimkou členských štátov Európskej únie. Porovnajte: § 7 ods. 1 a 2 zákona č. 140/2014 Z. z.

3. Postavenie organizácie SAFER pri ochrane vidieckej pôdy vo Francúzsku

Inštitucionálnym základom ochrany pôdy vo Francúzsku je organizácia SAFER (*Société d'aménagement foncier et d'établissement rural*), teda spoločnosť pre obhospodarovanie pôdy a rozvoj vidieka. Jej postavenie je špecifické – nemôžeme ju považovať za štátny orgán, najbližšie má asi k určitému hybridnému samosprávnemu orgánu. Vo svojej podstate ide o neziskovú[12] verejnú spoločnosť, s poslaním ochrany všeobecného záujmu, pod dohľadom príslušných ministerstiev poľnohospodárstva a financií. Územná pôsobnosť jednotlivých organizácií sa popri tom vzťahuje na celé územie metropolitného Francúzska, ako aj na tri zámorské územia.

Organizácie SAFER umožňujú rôznym, najmä podnikateľským projektom – či už poľnohospodárskym, remeselným, servisným, obytným alebo environmentálnym – usadiť sa vo vidieckom prostredí. Projekty musia byť v súlade s miestnymi politikami a musia spĺňať všeobecný záujem. Ide teda o akúsi snahu o kontrolovaný a riadený spôsob rozvoja vidieka v snahe zabezpečiť ochranu verejného záujmu pri vykonávaní rôznych aktivít.

Ich vznik sa datuje do šesťdesiatych rokov, konkrétne do roku 1960 a 1962, v súvislosti s prijatím tzv. Zákonov o orientácii poľnohospodárstva (*les lois d'orientation agricole*).[13] Konkrétne sa jedná najmä o zákon č. 60-808 z 5. augusta 1960 o orientácii pôdohospodárstva, ktorý okrem iných poľnohospodárskych reforiem (vytvorenie vyššieho poľnohospodárskeho školstva, ďalších organizácii poľnohospodárov, značiek kvality a podobne)[14] vytvoril právny predpoklad pre ich vznik a činnosť.

Konkrétna právna úprava postavenia a činnosti organizácie SAFER sa však nachádza v už vyššie zmienenom Vidieckom zákonníku, a to konkrétne v jeho knihe I., hlave IV s názvom *Les sociétés d'aménagement foncier et d'établissement rural*. Ten predpokladá ich založenie pre ochranu poľnohospodárskych, prírodných a lesných oblastí. Ich intervencie sú zamerané na *podporu zakladania, udržiavania a konsolidácie poľnohospodárskych alebo lesníckych činností tak, aby dosiahli životaschopný ekonomický rozmer* s ohľadom

[12] Článok L141-7 Vidieckeho zákonníka.

[13] Qu'est-ce qu'une Safer ? In Safer.fr. Dostupné na: https://www.safer.fr/les-safer/quest-ce-quune-safer/ [cit. 25.09.2023].

[14] Zákon č. 60-808 z 5. augusta 1960 o orientácii poľnohospodárstva vo vyhlásenom znení.

na kritériá regionálneho hlavného plánu poľnohospodárskych činností, ako aj zlepšenie rozdelenia pozemkov. Ich činnosť by však rovnako mala prispievať ku rozmanitosti krajiny, ochrane prírodných zdrojov a udržiavaniu biologickej diverzity, k trvalo udržateľnému rozvoju vidieckych oblastí či zabezpečeniu transparentnosti trhu s pôdou.[15]

Činnosť organizácií SAFER vychádza zo základného predpokladu, že vidiecky priestor predstavuje spoločný priestor, pri ktorého využívaní vystupuje do popredia verejný, spoločný záujem. To, ako sa využíva nie je preto len záujmom vlastníka prípadne iných oprávnených osôb, ale aj štátu a spoločnosti. Práve kvôli týmto dôvodom pri prevodoch vlastníctva poľnohospodárskej pôdy, ako aj iných druhov vidieckych pozemkov organizácia SAFER organizuje dialóg. V rámci konzultačných a rozhodovacích orgánov (technický výbor, správna rada, vládni komisári) sa zainteresovaní miestni aktéri navzájom radia. Všetky prijaté rozhodnutia potvrdzuje štát.

Organizácie SAFER sú organizované na základe miestnej príslušnosti, v závislosti od konkrétnej oblasti, v ktorej vyvíjajú svoju aktivitu. V každom z regiónov metropolitného Francúzska (13 regiónov) a v troch z piatich regiónov v rámci zámorských území existuje jedna organizácia SAFER, na čele ktorej stojí prezident a riaditeľ. Vnútorne sa člení na départementálne služby, so sídlom v každom départemente, na čele ktorých stojí ich vlastný vedúci.[16] V rámci celej republiky sú organizované prostredníctvom Národnej federácie SAFER (*la Fédération nationale des SAFER*).[17]

V rámci organizácie SAFER patrí najdôležitejšia rola *technickému výboru (le comité technique)*. Ten skúma spisy záujemcov o kúpu pozemku alebo inej vidieckej nehnuteľnosti. Jedná sa o prípady, kedy je na predaj určitý poľnohospodársky, alebo iný vidiecky pozemok, prípadne farma. V tejto situácii nie je možné predmetné nehnuteľnosti predať ihneď priamo, prípadne ich previesť na základe iného právneho úkonu bez toho, aby bola o tom informovaná miestne príslušná organizácia SAFER . Pri prevode teda výbor vydá stanovisko, ktorá z ponúk najlepšie zapadá do miestnej štruktúry a do cieľov miestnej organizácie SAFER.

[15] Článok L141-1 Vidieckeho zákonníka.

[16] Contactez la Safer de votre région. In Safer.fr. Dostupné na: https://www.safer.fr/contacts-safer/ [cit. 25.09.2023].

[17] Notre histoire. In Safer.fr. Dostupné na: https://www.safer.fr/les-safer/notre-histoire/ [cit. 25.09.2023].

Z organizačného hľadiska sa technický výbor skladá zo zástupcov poľnohospodárskych organizácii (poľnohospodárske komory, banky a poľnohospodárske vzájomné poisťovne, reprezentatívne poľnohospodárske zväzy), zástupcov miestnej samosprávy (obecná rada a združenia starostov) či zástupcov štátnej správy (riaditeľ správy pôdohospodárstva v départemente, či riaditeľ správy verejných financií). V niektorých organizáciách SAFER môžu byť členmi aj ďalší predstavitelia (regionálnej rady, notárov, organizácie na ochranu životného prostredia, či združenia vlastníkov lesa alebo rôzne vidiecke majetkové združenia.[18]

Ďalším významným orgánom v rámci organizácie SAFER je správna rada (*le conseil d'administration*). Situácia je tu podobná ako v prípade rôznych obchodných spoločností, keďže správna rada zastupuje jednotlivých členov ako svojich súkromných akcionárov. Táto správna rada rozhoduje po konzultácii a spolupráci s technickým výborom a predstavuje skôr výkonný a riadiaci orgán danej organizácie SAFER, pretože rozhodovanie o otázkach pôdohospodárstva spočíva na technickom výbore.

Dôležitou organizačnou súčasťou organizácie sú aj vládni komisári, ako splnomocnenci štátnej správy pre určitý úsek. *Vládnymi komisármi sú zástupcovia ministerstiev, ktoré majú na starosti poľnohospodárstvo a financie. Zabezpečujú súlad pokynov prijatých spoločnosťou SAFER s politikou územného plánovania definovanou verejnými orgánmi*.[19] Zjednodušene môžeme uviesť, že úlohou vládnych komisárov je zabezpečiť a kontrolovať zákonnosť činnosti a rozhodovania jednotlivých organizácii SAFER.

Keďže sa jedná o právnickú osobu súkromného práva, je možné SAFER aj zrušiť. Takýto postup je však možný len po ukončení postupov, ktorých cieľom je dať držiteľom prednostných predkupných práv možnosť ich uplatniť. Inak povedané, je to možné až vtedy, keď už nebude vykonávať svoju činnosť, teda oprávnenia a povinnosti v zmysle Vidieckeho zákonníka a iných právnych predpisov.[20]

Záverom k vnútornej organizáciu SAFERu môžeme uviesť, že je veľmi komplikované nájsť paralelu medzi jeho postavením a právnickými osobami tak, ako ich poznáme podľa slovenského právneho poriadku. Aj vzhľadom na francúzsky právny systém sa jedná

[18] Qu'est-ce qu'une Safer ? In Safer.fr. Dostupné na: https://www.safer.fr/les-safer/quest-ce-quune-safer/ [cit. 25.09.2023].

[19] Tamže.

[20] Článok L143-8 Vidieckeho zákonníka.

o veľmi zvláštny druh subjektu založeného na základe osobitných právnych predpisov, tak ako je uvedené vyššie. V našom, slovenskom chápaní sa jedná o právnickú osobu súkromného práva, založenú jej členmi, ktorých združuje. Na druhej strane disponuje viacerými verejnomocenskými oprávneniami, ktoré sa prejavujú najmä pri pôsobnosti a právomoci rozhodovať vo veciach verejného záujmu, napríklad o možnosti nakladať s vlastníctvom najmä poľnohospodárskej pôdy, ako aj iného vidieckeho majetku. Z hľadiska tradičného chápania slovenskej vedy správneho práva by sme túto organizáciu, vzhľadom na mnohé jej osobitosti, mohli zaradiť medzi subjekty ostatnej verejnej správy, aj keď je pravdou, že vykazuje mnohé znaky záujmovej samosprávy (napr. poľnohospodárskych organizácií), či bežnej obchodnej spoločnosti súkromného práva. V ďalšom texte sa venujeme jej pôsobnostiam a právomociam pri nakladaní s vlastníctvom poľnohospodárskej pôdy.

4. Úlohy organizácie SAFER pri nakladaní s vlastníctvom poľnohospodárskej pôdy

Aj keď je pravdou, že organizácie SAFER majú v rámci trhu s poľnohospodárskou pôdou, ako aj inými vidieckymi nehnuteľnosťami významnú kontrolnú funkciu za účelom dosiahnutia vyššie uvedených cieľov, nedá sa povedať, že by priamo riadili či organizovali trh s pôdou. Pozemky predstavujúce poľnohospodársku pôdu, ako aj iné vidiecke nehnuteľnosti naďalej predstavujú predmet súkromnoprávnych vzťahov a vlastnícke právo k ním je ústavne chránené, a to jednak ústavou tzv. piatej republiky, ako aj Deklaráciou práv človeka a občana, na ktorú ústava bezprostredne odkazuje.

Pri prevodoch vlastníctva poľnohospodárskej pôdy platí pravidlo, že ich predpokladom je legalizácia tohto prevodu príslušným notárom, bez ktorej zmluva nenadobudne účinnosť. O každom predaji poľnohospodárskej pôdy musí notár legalizujúci transakciu informovať miestny SAFER.[21] SAFER má potom dva mesiace na schválenie alebo zamietnutie transakcie. V tých prípadoch, keď transakcia nezodpovedá cieľom misie SAFER, organizácia uskutoční diskusie s predávajúcim a kupujúcim, aby sa pokúsili dosiahnuť vzájomnú dohodu, ktorá by lepšie zodpovedala cieľom SAFER.

[21] Článok L141-1-1 Vidieckeho zákonníka.

SAFER totiž v prvom rade predstavuje akýsi zmierovací orgán, ktorého cieľom je prioritne smerovať k dohode medzi zmluvnými stranami, ktorá by rešpektovala ciele organizácie pri rozvoji vidieka na danom území, rozvoji poľnohospodárstva, environmentálnych cieľoch a ďalších verejných a spoločných záujmoch.

Ak nedôjde medzi nimi k dohode, SAFER môže uplatniť predkupné právo.[22] SAFER uplatní svoje predkupné právo, ak existujú environmentálne ciele, ktoré je potrebné chrániť a navrhovaná zmluva by ich nerešpektovala, alebo ak sú prítomné očakávania, že existujú špekulatívne ciele predajcu či kupujúceho (napr. cena je príliš vysoká alebo príliš nízka) alebo veľkosť pozemku príliš veľká (SAFER sa snaží obmedziť rozširovanie fariem, a to najmä vytváraním veľkých lánov a obhospodarovaných plôch).

Vidiecky zákonník priamo ustanovuje ciele, ku ktorých dosiahnutiu by malo smerovať využitie tohto predkupného práva. Ide o:

a) umiestnenie, presídlenie, zotrvanie poľnohospodárov na určitom území,

b) hospodárska konsolidácia fariem a lepšie využívanie pozemkov,

c) ochrana rovnováhy využívania pozemkov,

d) boj proti špekuláciám s pôdou,

e) zachovanie existujúcich životaschopných fariem, ak sú ohrozené oddeleným prevodom pôdy a obytných alebo hospodárskych budov,

f) rozvoj a ochrana lesa,

g) ochrana životného prostredia,

i) ochrana a rozvoj prímestských poľnohospodárskych a prírodných oblastí.[23]

Ak sa príslušná organizácia SAFER rozhodne využiť svoje predkupné právo, následne sa pokúsi nájsť iné vlastnícke usporiadanie, ktoré lepšie vyhovuje cieľom SAFER-u, napr. predať pozemok inému kupujúcemu, či ho prenajať.[24]

Je potrebné tiež uviesť, že vo väčšine prípadov dochádza k prevodu vlastníctva na základe zmluvy bez toho, aby miestne príslušná organizácia SAFER využila svoje predkupné právo a zasahovala do určitého prevodu. Je to tak až v 89 % prípadov.[25] Z pôsobnosti SAFER a jeho uplatňovania predkupného práva sú taktiež úplne vyňaté niektoré

[22] Článok L143-1 Vidieckeho zákonníka.

[23] Článok L143-2 Vidieckeho zákonníka.

[24] CIAIAN, P. a kol.: Sales market regulations for agricultural land in EU member states and candidate countries. St.Paul : CEPS, 2012, s. 4.

[25] Nos 2 métiers. In Safer.fr. Dostupné na: https://www.safer.fr/les-safer/nos-2-metiers/ [cit. 25.09.2023].

druhy prevodov vlastníctva, ako napríklad predkupné právo nemožno uplatniť na nákupy existujúcich poľnohospodárov na danom mieste, kde dochádza k prevodu vlastníctva, na stavebné pozemky so stavebným záväzkom alebo na kúpu poľnohospodárskych pozemkov v rámci rodinných vzťahov, ani na väčšinu predajov lesných pozemkov.[26]

Úlohy organizácie SAFER sa však neviažu nevyhnutne len na uplatňovanie predkupného práva v prípadoch prevodov vlastníctva poľnohospodárskej pôdy. Aj práve v súvislosti s uplatnením tohto predkupného práva prichádza do úvahy aj vykonávanie ďalších oprávnení, ako je napríklad správa nadobudnutého majetku, jeho prenájom či prípadne predaj tretím subjektom. SAFER okrem iného funguje aj ako sprostredkovateľ predaja vidieckych nehnuteľností. Inak povedané, k celému procesu prevodu vlastníctva je možné pristúpiť aj priamym oslovením organizácie SAFER, ktorej úlohou je následne predmetné nehnuteľnosti predať.

Záverom k vymedzeniu úloh a pôsobností organizácie SAFER pri nakladaní s vlastníctvom poľnohospodárskej pôdy a súvisiaceho vidieckeho majetku musíme uviesť, že táto organizácia ich uplatňuje v prvom rade prostredníctvom svojho predkupného práva pri nakladaní s predmetným majetkom. Toto predkupné právo však musíme chápať vo vzájomných súvislostiach s postavením a činnosťou celej organizácie, ktorá predmetné nehnuteľnosti môže zároveň aj spravovať, nakladať s nimi či pôsobiť ako sprostredkovateľ pri ich predaji.

Hoci ide v tomto prípade o činnosť organizácie, ktorá vzniká na základe zákona, na druhej strane treba uviesť, že činnosť SAFER nepredstavuje štátnu reguláciu. Síce pri tomto rozhodovaní má svoje významné miesto verejný záujem definovaný v právnych predpisoch, na prvom mieste vo Vidieckom zákonníku, stále platí základné pravidlo, podľa ktorého sa pri tejto činnosti jedná o uplatňovanie práv miestnych subjektov združených v príslušnej organizácií a ich rozhodovanie o budúcnosti využívania vidieckej krajiny.

5. Komparácia úloh organizácie SAFER so slovenskou právnou úpravou

Pri porovnaní právnej úpravy Slovenskej republiky a Francúzskej republiky na úseku nadobúdania vlastníctva a ochrany poľnohospo-

[26] Tamže.

dárskej pôdy môže dôjsť k výsledku, že obidva štáty pristupujú k tejto otázke úplne odlišne.

Ako je uvedené vyššie, podľa súčasného (september 2023) platného a účinného právneho stavu zákonodarca vlastníka poľnohospodárskych pozemkov, resp. iných súvisiacich nehnuteľností takmer nijako neobmedzuje pri nakladaní s nimi. Určitú výnimku predstavuje spomenuté pravidlo reciprocity, podľa ktorého nemôže vlastníctvo k poľnohospodárskym pozemkom nadobúdať fyzická osoba alebo právnická osoba z toho štátu, ktorý obdobné obmedzujúce pravidlá stanovuje pre slovenské subjekty.

Ani francúzsky právny poriadok v zásade nestanovuje obmedzujúce pravidlá pre subjekty nadobúdajúce vlastníctvo k poľnohospodárskej pôde, alebo súvisiacim vidieckym nehnuteľnostiam. Na druhej strane však zakladá zvláštne organizácie SAFER disponujúce predkupným právom, ktoré sú oprávnené zasiahnuť do mnohých prevodov vlastníctva týchto nehnuteľností, čím do značnej miery limitujú nakladanie s vlastníctvom.

Rozdiely však môžeme badať nielen v konkrétnej právnej úprave, ale aj celkovom zameraní a cieľov regulácie trhu s pôdou. Vo Francúzsku totiž nielen poľnohospodárska pôda, ale aj v zásade celý vidiecky priestor predstavuje predmet verejného záujmu. Aj každá nehnuteľnosť, ktorá sa na ňom nachádza, musí byť v stave súladnom s tým, ako si spoločnosť predstavuje jeho ďalší rozvoj – a to je niečo, čo sa odvíja v prvom rade od vlastníctva. Každý potenciálny kupujúci totiž mieni nadobudnúť vlastníctvo k určitej nehnuteľnosti s nejakým úmyslom, ktorý nemusí byť v súlade s verejným záujmom.

Práve preto príslušné právne predpisy umožňujú organizácii SAFER uplatniť svoje predkupné právo v prípadoch, ak má podozrenie, že príslušný prevod vlastníckeho práva k vidieckym nehnuteľnostiam môže mať špekulatívne pozadie, vážne ohroziť vidiecke prostredie, narušiť vývoj cien nehnuteľností, alebo spôsobiť iné nepriaznivé následky, ktoré predpokladá zákon. Inak povedané, pri rozhodovaní, či uplatní svoje predkupné právo, musí organizácia SAFER preskúmať navrhovanú zmluvu aj z obsahového hľadiska a skúmať nielen jej zákonnosť, ale aj správnosť, v zmysle vhodnosti, účelnosti, prospešnosti.

Hoci sa na prvý pohľad tento prístup môže javiť ako prílišne prísny, obmedzujúci práva vlastníkov vidieckych nehnuteľností, treba ho chápať v širšom kontexte. A to najmä skutočnosti, že celý vidiecky priestor predstavuje predmet verejného záujmu, ktorý štát a spoločnosť

úmyselne a cielene vytvára. Je to niečo obdobné, ako poznáme v prípade zastavaného územia obce pri územnom plánovaní – aj pri vidieckom priestore by mal predsa štát cielene plánovať, k čomu bude vidiecka krajina využívaná a ako budú vyvažované rôzne záujmy viacerých subjektov.

Keď by sme pri tejto komparácii brali do úvahy aj predchádzajúcu slovenskú právnu úpravu v zákone č. 140/2014 Z. z. o nadobúdaní vlastníctva poľnohospodárskeho pozemku a o zmene a doplnení niektorých zákonov v znení neskorších predpisov pred tým, než jeho väčšia časť bola zrušená na základe nálezu Ústavného súdu Slovenskej republiky, prišli by sme k záveru, že aj vtedajší slovenský zákonodarca sa snažil vyberať cestou systému predkupných práv. Na rozdiel od francúzskeho modelu však nevytváral priestor na vznik určitej nezávislej organizácie, ale priamo určoval subjekty, ktoré boli oprávnené prioritne nadobudnúť vlastníctvo k poľnohospodárskemu pozemku, či už išlo o poľnohospodára z rovnakej alebo susednej obce, prípadne iné subjekty. Za účelom transparentného predaja poľnohospodárskych pozemkov dokonca Ministerstvo pôdohospodárstva a rozvoja vidieka Slovenskej republiky prevádzkovalo jednotný Register zverejňovania ponúk prevodu vlastníctva poľnohospodárskeho pozemku.[27]

Môže nám preto oprávnene vzniknúť otázka, aké sú zásadné odlišnosti medzi francúzskym modelom a slovenským modelom podľa predchádzajúcej právnej úpravy, keďže francúzsky model funguje už desaťročia bez veľkých problémov, zatiaľ čo zmienený slovenský model bol účinný len niekoľko rokov, vyvolávajúc mnoho otázok o súlade s Ústavou Slovenskej republiky, ako aj právom Európskej únie?

Pokúsime sa preto poukázať na najvýraznejšie rozdiely a zvýrazniť niektoré dôležité stránky francúzskej právnej úpravy:

1. V centre záujmu francúzskej právnej úpravy je verejný záujem jednak pri vykonávaní poľnohospodárskej činnosti, ako aj pri celkovom rozvoji vidieka. Záujem na rozvoji vidieka teda predstavuje prioritný a objektívny cieľ.
2. V rámci právnej regulácie nejde prioritne o obmedzovanie možností nadobúdania vlastníctva poľnohospodárskych pozemkov či iných súvisiacich vidieckych nehnuteľností, napríklad preferovaním nadobúdateľov z tej istej, alebo susednej obce. Obmedzujúce, alebo prípadne zvýhodňujúce

[27] Dodnes dostupný online na: https://pozemky.mpsr.sk/ [cit. 25.09.2023].

kritériá sa teda nevzťahujú priamo na subjekt nadobúdateľa, ale na účel a využitie predmetných nehnuteľností.

3. Aj francúzsky model ako spôsob regulácie využíva systém predkupných práv, obdobne ako to bolo v prípade spomínanej predchádzajúcej slovenskej právnej úpravy. Na rozdiel od nej však legislatíva prítomná vo Vidieckom zákonníku a ďalších právnych predpisoch nepôsobí na prevodcu natoľko obmedzujúco – svoj záujem previesť vlastníctvo nemusí oznamovať či zverejňovať do príslušného registra. V tomto prípade postačuje kontaktovanie miestne príslušnej organizácie SAFER, ktorá na základe vyššie zmienených objektívnych kritérií miestneho rozvoja sama rozhodne, či bude svoje predkupné právo uplatňovať, prípadne či bude v rámci tohto prevodu vlastníckeho práva k vidieckym nehnuteľnostiam vystupovať ako sprostredkovateľ, alebo nie. Nie je preto potrebné kontaktovať a oslovovať ďalšie subjekty.
4. Na druhej strane je však potrebné zároveň konštatovať, že aktivity príslušnej organizácie SAFER pôsobia v praxi oveľa efektívnejšie a účinnejšie, ako to bolo v prípade predchádzajúcej slovenskej právnej úpravy. Ak totiž svoje predkupné právo neuplatnil žiadny z preferovaných potenciálnych nadobúdateľov, ako napríklad poľnohospodár – záujemca z tej istej obce, prípadne susednej obce alebo ďalší, vlastnícke právo k poľnohospodárskemu pozemku mohol nadobudnúť v zásade ktokoľvek, samozrejme v rámci zákonných limitov. Títo zároveň pri rozhodovaní, či svoje predkupné právo uplatnia alebo nie, boli vedení len svojim vlastným, teda súkromným záujmom vlastníka, prípadne aj podnikateľa, ak zároveň predstavovali aj podnikateľov v poľnohospodárstve. Na druhej strane, organizácia SAFER je pri uplatňovaní svojho predkupného práva viazaná verejným záujmom a samozrejme zákonnými požiadavkami.
5. Tiež treba poukázať na to, že uplatnenie predkupných práv SAFER môže niekedy pôsobiť prílišne limitujúco. Samozrejme stále existuje riziko, že právomoci tejto organizácie môžu byť zneužité alebo uplatňované diskriminačne, čo v praxi môže viesť k nemožnosti nadobudnutia vlastníctva poľnohospodárskeho pozemku alebo inej vidieckej nehnuteľnosti osobou, ktorá bude „v nemilosti“ osôb vykonávajúcich funkcie v orgánoch SAFER. Preto je potrebné vždy podrobiť činnosť týchto organizácii verejnej vonkajšej kontrole.

Záverom tejto komparácie môžeme uviesť, že spôsob, ako francúzska legislatíva chráni vidiecke nehnuteľnosti a práva k nim viažuce na jednej strane je pomerne silným a efektívnym spôsobom, na druhej strane však výrazne operuje s verejným záujmom a všeobecne stanovenými podmienkami.

Záver

Pozemky predstavujúce poľnohospodársku pôdu nie sú bežným predmetom právnych vzťahov. Ako sme uviedli už vyššie v texte, z dôvodu ich účelového využitia požívajú zvláštnu ochranu – jednak pri ich ochrane a starostlivosti o nich, ale rovnako tak aj pri nakladaní s ich vlastníctvom.

Každý štát je pri tejto ochrane limitovaný viacerými faktormi. Na prvom mieste to je ochrana vlastníckeho práva, ktoré nemôže byť bezdôvodne obmedzované, najmä nie v rozpore s testom proporcionality. Na druhej strane je to právo Európskej únie, ktoré v zmysle zakladajúcich zmlúv neumožňuje diskriminovať subjekty z iných členských štátov, alebo neprimerane zvýhodňovať subjekty z jedného členského, aj keď „domáceho" štátu.

Ako sme uviedli v predchádzajúcich kapitolách, francúzsky zákonodarca k riešeniu problematiky pristúpil inak – cez ochranu verejného záujmu. Aj tu však vychádzame z pravidla, ktoré môžeme nájsť aj v Ústave Slovenskej republiky, podľa ktorého vlastníctvo zaväzuje. A to najmä v prípadoch, kedy má značný presah aj do práv štátu a spoločnosti.

V úvode článku sme si stanovili ako cieľ vymedziť osobitné postavenie pozemkov predstavujúcich poľnohospodársku pôdu v zmysle francúzskej právnej úpravy, a to najmä s ohľadom na nadobúdanie tohto vlastníctva. Za účelom dosiahnutia tohto cieľu sme bližšie popisovali vymedzenie pozemkového vlastníctva a najmä postavenie a pôsobnosti organizácie SAFER pri nakladaní s vlastníctvom poľnohospodárskych pozemkov a vidieckych nehnuteľností.

Rovnako sme si stanovili hypotézu v znení: francúzska právna úprava ochrany poľnohospodárskej pôdy je dostatočne účelná a efektívna pre dosiahnutie účelu ochrany tejto pôdy ako zložky životného prostredia, no najmä nástroja poľnohospodárstva. Tu musíme konštatovať, že došlo k verifikácii predmetného tvrdenia, na základe skutočností uvedených v predchádzajúcich kapitolách článku.

Francúzsky model regulácie nakladania s poľnohospodárskymi pozemkami a inými vidieckymi nehnuteľnosťami predstavuje dostatočne efektívny systém, keďže úlohy organizácie SAFER pri ochrane verejného záujmu sú jasne dané právnymi predpismi. Neznamená to, že tento model nemá nedostatky, ale určite ho môžeme považovať za účinný.

Tieto skutočnosti by preto mohli predstavovať určitú inšpiráciu aj pre slovenského zákonodarcu pri prijatí právnej úpravy, ktorá by nahradila dnes už neúčinnú reguláciu v zmysle zákona 140/2014 Z. z. o nadobúdaní vlastníctva poľnohospodárskeho pozemku a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. V prvom rade je potrebné dbať na zvýraznenie a ochranu verejného záujmu, a to aj s poukázaním na ústavnú ochranu pôdy v zmysle čl. 44 Ústavy Slovenskej republiky. A na druhej strane, pri prevodoch vlastníctva je potrebné regulačné kritériá, kľudne aj vo forme predkupných práv, nastaviť spôsobom, ktorý nebude priamo viazaný na osoby prevodcu, alebo nadobúdateľa.

Použitá literatúra

1. CIAIAN, P. a kol.: *Sales market regulations for agricultural land in EU member states and candidate countries*. St.Paul : CEPS, 2012. 31 s., Dostupné na: https://ageconsearch.umn.edu/record/120249/ (cit. 25.09.2023). DOI 10.22004/ag.econ.120249.
2. DESRIERS, M.: *L'agriculture française depuis cinquante ans: des petites exploitations familiales aux droits à paiement unique*. In *Agreste cahiers*, 2007, 2: 3-14. Dostupné na: https://www.statista.com/statistics/1107173/share-of-agriculture-in-french-gdp/ (cit. 25.09.2023).
3. PAVLOVIČ, M.: Ústavné východiská pre reguláciu trhu s pôdou. In *Comenius* [elektronický dokument]. - č. október (2021). Dostupné na: http://alis.uniba.sk:9909/lib/item?id=chamo:381542&fromLocationLink=false&theme=EPC (cit. 25.09.2023).
4. PAVLOVIČ, M.: Vplyv ústavnej ochrany pôdy na vývoj pozemkového práva. In *Půda v právních vztazích – aktuální otázky*. Brno : Masarykova univerzita, 2019, s. 43-76.
5. ŠTEFANOVIČ, M.: *Pozemkové právo*. Bratislava : EUROUNION, 2010. 312 s.
6. TORRE, A. – WALLET, F. – HUANG, J.: Le foncier agricole, nouvel enjeu des politiques d'aménagement de l'espace. In *Économie rurale*, 2023, č. 383, s. 8.

https://journals.openedition.org/economierurale/10896. DOI https://doi.org/10.4000/economierurale.10896.

Právne predpisy

1. Zákon č. 140/2014 Z. z. o nadobúdaní vlastníctva poľnohospodárskeho pozemku a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
2. Vidiecky zákonník a zákonník námorného rybolovu. Dostupný vo francúzskom jazyku: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071367/ [cit. 25.09.2023].
3. Zákon č. 60-808 z 5. augusta 1960 o orientácii pôdohospodárstva, ktorý okrem iných poľnohospodárskych reforiem. Dostupný vo francúzskom jazyku: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000508777 [cit. 25.09.2023].

Iné zdroje

1. Agrikultúra, forestry and fishing. The World Bank Data. Dostupné na: https://data.worldbank.org/indicator/NV.AGR.TOTL.ZS [cit. 25.09.2023].
2. Share of agriculture, fisheries and forestry in GDP in France from 2003 to 2022. Statista.com. Dostupné na: https://www.statista.com/statistics/1107173/share-of-agriculture-in-french-gdp/ [cit. 25.09.2023].
3. Manifeste agricole à Paris. Dostupné na: https://www.ladepeche.fr/2023/02/08/manifestation-agricole-a-paris-prix-de-lenergie-pesticides-secheresse-pourquoi-les-agriculteurs-sont-ils-en-colere-10984238.php [cit. 25.09.2023].
4. Identité agricole des régions. Dostupné na: https://www.insee.fr/fr/statistiques/5039859?sommaire=5040030 [cit. 25.09.2023].
5. Safer.fr. Dostupné na: https://www.safer.fr/ [cit. 25.09.2023].

ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLII
2/2023

PLATFORMOVÁ EKONOMIKA: VÝZVY A PRÍLEŽITOSTI PRE EFEKTÍVNU PRÁVNU OCHRANU ZAMESTNANCOV

JUDr. Ádám Sípos, BSc (Hons)

Univerzita Komenského v Bratislave, Právnická fakulta
Katedra pracovného práva a práva sociálneho zabezpečenia
adam.sipos@flaw.uniba.sk

Platformová ekonomika: Výzvy a príležitosti pre efektívnu právnu ochranu zamestnancov

Tento príspevok sa venuje aktuálnej problematike platformovej ekonomiky v kontexte slovenského pracovného práva. Z formálnej stránky je príspevok rozdelený do troch hlavných častí. V prvej časti sa venujeme definícii základných pojmov a zanalyzujeme súčasný stav platformovej ekonomiky *in genere*. Druhá časť príspevku sa zameriava na stav *de lege lata* slovenského pracovného práva vo vzťahu k platformovej práci a rieši problémy spojené s platformovou ekonomikou, akým je napríklad *uberizácia* pracovnoprávnych vzťahov a nelegálna práca. V poslednej časti sa detailnejšie zaoberáme legislatívnymi krokmi Európskej únie, ktoré majú vytvoriť komplexný a širokoplošný systém ochrany pracovných a sociálnych práv pracovníkov digitálnych platforiem. Cieľom tohto príspevku je analyzovať súčasný právny rámec ochrany platformových pracovníkov a zamyslieť sa nad otázkou, či tradičné ochranné mechanizmy slovenského pracovného práva postačujú na komplexnú ochranu pracovníkov v rámci platformovej ekonomiky. Prínosom tejto práce je zhodnotenie súčasného právneho stavu a identifikácia potenciálnych oblastí na zlepšenie ochrany pracovníkov v rámci platformovej ekonomike v Slovenskej republike.

The platform economy: challenges and opportunities for effective legal protection of employees

This paper deals with the current issue of the platform economy in the context of Slovak labour law. Formally, the paper is divided into three main parts. In the first part we define the basic concepts and analyze the

current state of the platform economy *in genere*. The second part of the paper focuses on the *de lege lata* state of Slovak labour law in relation to platform labour and addresses the problems associated with the platform economy, such as the *uberization* of labour relations and illegal work. In the last part, we examine in more detail the legislative steps taken by the European Union to create a comprehensive and broad-based system of labour and social rights protection for digital platform workers. The aim of this paper is to analyze the current legal framework for the protection of platform workers and to reflect on the question whether the traditional protection mechanisms of Slovak labour law are sufficient to comprehensively protect workers in the today's platform economy. The contribution of this paper is to assess the current legal situation and identify potential areas for improvement of the protection of workers in the platform economy in the Slovak Republic.

Kľúčové slová: platformová práca, uberizácia, právna ochrana, pracovnoprávny vzťah, obchodnoprávny vzťah, nová pracovnoprávna legislatíva

Keywords: platform work, uberization, legal protection, employment relationship, commercial relationship, new labour legislation

Úvod

K jedným z najväčších premien pracovného trhu za uplynulé desaťročie patrí nepochybne rapídny nástup online digitálnych platforiem. Z pohľadu odborníkov z oblasti pracovného práva je evidentné, že vývoj na pracovnom trhu spojený s rastom technologických inovácií v 21. storočí, najmä v „*post-covidovom*" období, prináša mnohé vplyvy, ktoré nemožno prehliadať, a ktoré ovplyvňujú samotné pracovnoprávne aspekty tohto nového fenoménu. V tomto kontexte sa dá poukazovať na aktuálne právne výzvy z oblasti ochrany osobných údajov pracovníkov, právo zamestnancov na odpojenie ako aj na prudký vzostup nových neštandardných foriem práce, ktoré vybočujú z tradičného rámca pracovnoprávnych vzťahov. Keďže novodobé formy práce operujú s prakticky neprehliadnuteľným kvantom inovácií, ktoré sa rýchlo vyvíjajú vo všetkých možných smeroch, je mimoriadne dôležité, aby kompetentné orgány Európskej únie (ďalej len ako „EÚ") spolu so zákonodarcami jednotlivých členských štátov EÚ dostatočne rýchlo a efektívne zareagovali na nové sociálnoekonomické fenomény, ktoré sú výsledkami globalizácie

a digitalizácie výkonu práce ako takej. Práca na digitálnych platformách ponúka pracujúcim subjektom príležitosť vykonávať prácu z ktoréhokoľvek miesta a v akomkoľvek vhodnom čase prijať prácu resp. pracovnú úlohu, ktorá vyhovuje ich rôznym preferenciám a možnostiam. Je potrebné však poukázať na skutočnosť, že vykonávanie spomínanej formy pracovnej činnosti so sebou prináša aj určité riziká, ktoré sa týkajú právneho postavenia spomínaných subjektov, otázky ich spravodlivej finančnej kompenzácie, ich pracovnoprávnej ochrany ako aj iných sociálnych benefitov. Príležitosti a riziká, ktorým pracovníci platforiem čelia, sa v súčasnom sociálno-ekonomickom prostredí pomerne rýchlo menia, a preto je vytvorenie účinného a komplexného právneho rámca nevyhnutnosťou pre ich dôstojnú právnu ochranu. Tento nový koncept pracovného procesu viedol nielen k narušeniu jestvujúcich obchodných modelov, ale aj k narušeniu klasického vnímania pracovnoprávnych vzťahov ako takých. Hlavným zámerom tohto príspevku je sústredenie sa na špecifický segment rozsiahleho systému neštandardných foriem prác, a to konkrétne problematike výkonu práce na digitálnych platformách a snažiť sa pouvažovať nad aktuálnou a komplexnou otázkou: *Sú tradičné ochranné inštitúty slovenského pracovného práva dostačujúce na komplexnú ochranu pracovníkov platforiem?*

1. Platformová ekonomika – nová dimenzia pracovných možností

V kontexte súčasnej digitálnej a globalizovanej ére sme svedkami rozsiahleho dynamického nárastu nových elektronických resp. digitálnych pracovných foriem, ktoré prinášajú ďalšie príležitosti a pracovné miesta, ktoré sú dostupné prostredníctvom platforiem rôznych online aplikácií. Pred samotnou analýzou postavenia platformovej práce v podmienkach slovenského právneho poriadku vysvetlíme obsah predmetného pojmu. Nové formy pracovných činností, ktoré sú výsledkami vyššie spomenutého procesu sú v jurisprudencii označované ako „*neštandardné práce"* (angl. non-standard work)[1] a práve jednu ich podkategóriu tvorí „*platformová práca"* (angl. platform work).[2] Tento termín však iba čiastočne

[1] ILO: *Non-standard employment around the world: Understanding challenges, shaping prospects*. Geneva:International Labour Office,2016, s. 39.

[2] PORUBAN, A. Skupinové zamestnávanie ako nový model práce. In*: Sdílená ekonomika sdílený právní problém?* Praha: Wolters Kluwer, 2017, s. 89.

zahrňuje širší zväzok anglických pojmov, medzi ktoré patria termíny akým je *crowd-work*,[3] *gig-economy*[4] ako aj *on-demand economy*.[5] Chceme poukázať na skutočnosť, že veľmi často sa pojem „*zdieľaná ekonomika"* (angl. shared economy) uvádza v aplikačnej praxi ako všeobecne schválený rámec pre jednotný komplex špecifickejších typov neštandardných pracovných činností. Tento konceptuálny výraz sa vyvíja z rozsiahlejšieho základu, v rámci ktorého vznikajú špecifické a užšie formy neštandardnej práce, ktoré disponujú kvalitatívne rozdielnymi (aj keď často minimálnymi) črtami resp. charakteristikami. Je však nutné zdôrazniť, že v aplikačnej praxi sa možno často stretávať s prelínaním resp. prekrývaním obsahu vyššie spomínaných pojmov, pretože niektoré pracovné aktivity neštandardných prác vykonávaných fyzickými osobami sa môžu v rôznych ohľadoch zhodovať s viacerými termínmi súčasne. Príkladom tejto situácie môže byť kuriér pracujúci pre rozvozovú spoločnosť, ktorý využíva mobilnú aplikáciu spoločnosti a občas poskytuje svoje služby na svojom vlastnom bicykli (napríklad počas víkendov). Jeho pracovné aktivity vykazujú prvky *platformovej práce* ako aj *zdieľanej ekonomiky*, avšak jeho prácu by bolo možné subsumovať aj do kategórií akým je *gig economy* a *on-demand economy*.

V pomerne krátkom časovom rámci došlo k sériu nepriaznivých udalostí, ktoré následne prerástli do rozsiahlej a veľmi komplexnej viacrozmernej globálnej krízy. V priebehu posledných rokoch obyvatelia európskeho kontinentu boli vystavení nielen náročným následkom smrteľnej globálnej pandémie, ale aj negatívnym dôsledkom stále trvajúcej ruskej vojenskej invázie na Ukrajine. Súčasná energetická kríza, zvýšená migrácia a rapídna inflácia sú výsledkom reťazovej reakcie, ktorej pôvod spočíva práve v prísnych protipandemických opatreniach a neistote v oblasti regionálnej bezpečnosti, ktoré ju spustili. Zo spomínaných faktorov vznikali predpoklady pre súčasnú hospodársku recesiu, ktorá vyvoláva neistotu

[3] Forma práce, ktorá spočíva v prenesení práce, vykonávanej povereným pracovníkom (zamestnancom, SZČO alebo samostatnou firmou), na vopred nedefinovanú, zvyčajne početnú skupinu osôb prostredníctvom otvorenej výzvy, ktorá sa zvyčajne uskutočňuje cez internet. Pozri: ILO: *Digital labour platforms and the future of work: Towards decent work in the online world.* Geneva: ILO, 2018, s. 3.

[4] Nový atypický ekonomický model zahrnujúci krátkodobé, ale zároveň ekonomicky významné aktivity, ktoré sa opakujú s rôznou pravidelnosťou.

[5] Tento ekonomický systém spočíva v dostupnosti a ochote subjektov realizovať ekonomické aktivity na základe konkrétnych objednávok, pričom dodržiavajú požadovaný rozsah a časový rámec pracovných úloh.

vo veľkej časti obyvateľstva nášho regiónu. Práve tieto uvedené dôvody viedli k rýchlemu vzostupu popularity platformovej práce, čo potvrdzujú aj štatistiky.[6] V súčasnosti je takmer 30 miliónov ekonomicky aktívnych jednotlivcov na rôznych digitálnych platformách. Očakáva sa, že do roku 2025 sa tento počet zvýši na 43 miliónov. Spomínaný 52 % nárast naznačuje, že platformová ekonomika bude zohrávať kľúčovú úlohu pri podporovaní hospodárskeho rastu EÚ a znížení nezamestnanosti na kontinente.

Počas pandémie COVID-19 došlo k výraznému zvýšeniu aktivít na digitálnych platformách, pričom výkon predmetnej činnosti sa v tomto období stala primárnym príjmom pre mnohých. Predmetný vývoj bol čiastočne spôsobený zvýšeným dopytom po doručovaní hotového jedla a potravinových produktov. Zároveň je dôležité zdôrazniť, že platformová práca sa stala hnacím motorom inovácií a znižovaní nezamestnaností *in genere*.[7] V súčasnej „post-covidovej" ére platformová práca v oblasti dopravy a taxislužieb zabezpečuje mnohým migrantom stály príjem a tým aj ekonomickú a sociálnu stabilitu.[8] Vo väčšine prípadov je práca na platformách doplnkovým zdrojom príjmu vo vzťahu k „hlavnému" zamestnaniu. Nemožno však prehliadnuť, že pre určité skupiny platformových pracovníkov sa táto forma práce stala hlavným zdrojom príjmu. Výhody platformových prác, ako je napríklad flexibilita a relatívne nízke nároky na kvalifikáciu pracovníkov, spolu s jednoduchým výberovým procesom, robia z platformovej práce veľmi atraktívnu formu ekonomickej činnosti. S narastajúcou popularitou tejto pracovnej formy sa však stáva nevyhnutným zabezpečiť účinnú reguláciu, ktorá momentálne v Slovenskej republike a ani na úrovni EÚ nie je dostatočne uspokojivá.

---

6 RADA EÚ. *Infografika – Pracovníci digitálnych platforiem v EÚ* [online]. Consilium Europa, 2023 [cit. 09-09-2023]. Dostupné na: https://www.consilium.europa.eu/sk/infographics/digital-platform-workers/

7 RADA EÚ. *Pravidlá EÚ týkajúce sa práce pre platformy* [online]. Consilium Europa, 2023 [cit. 09-09-2023]. Dostupný na: https://www.consilium.europa.eu/sk/policies/platform-work-eu/

8 ILO. *Decent work in the platform economy* [online]. Geneva:International Labour Office,2022, s. 22. [cit. 09-09-2023]. Dostupné na: https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---relconf/documents/meetingdocument/wcms_855048.pdf a KOWALIK, Z., LEWANDOWSKI, P., KACZMARCZYK, P. Job Quality Gaps between Migrant and Native Gig Workers: Evidence from Poland.In: *IZA Discussion Paper Series*, Bonn: Institute of Labor Economics,2023, No. 16216. s.10.

2. Platformová práca v podmienkach „klasického“ slovenského pracovného práva

V súčasnom *stave de lege lata* slovenský právny poriadok ponúka relatívne širokú škálu možností pre pracovníkov digitálnych platforiem pri výbere právneho statusu pre výkon ich činností v rámci platformovej ekonomiky. V zmysle slovenského pracovného práva môže osoba vykonať prácu na digitálnej platforme ako zamestnanec v pracovnom pomere[9] alebo ako „dohodár“ na základe dohôd o prácach vykonaných pracovného pomeru.[10] V prípade, ak vykonaná práca nevykazuje znaky závislej práce zmysle ustanovenia § 1 ods. 2 Zákona č. 311/2001 Z. z. Zákonník práce (ďalej len ako „ZP“) t. j. ak subjekt danú prácu nevykonáva vo vzťahu nadriadenosti zamestnávateľa, osobne pre zamestnávateľa, podľa pokynov zamestnávateľa, v jeho mene, v pracovnom čase určenom zamestnávateľom, tak môže vykonávať danú ekonomicky významnú činnosť vo vzťahu k platformám v obchodnoprávnom režime.[11] V aplikačnej praxi však často dochádza k nesprávnej klasifikácii platformových pracovníkov. Táto nesprávna kvalifikácia môže mať čisto náhodný charakter, avšak v mnohých prípadov ide o vedomé konanie zo strany platforiem alebo v niektorých prípadoch aj zo strany pracovníkov. Nie je tajomstvom, že väčšina subjektov pôsobiacich v rámci platformových prác vykonáva svoju činnosť ako samostatne zárobkovo činné osoby (ďalej len ako „SZČO“). Podľa odhadov Európskej komisie k prvej polovici roku 2023 bolo približne 5 a pol milióna pracovníkov nesprávne zaklasifikovaných ako podnikateľov napriek skutočnosti, že spĺňajú všetky kvalifikačné znaky na to, aby boli označení za zamestnancov.[12] Táto štatistika je alarmujúca vzhľadom na to, že každý piaty človek pracujúci v platformovej ekonomike v rámci EÚ je pozbavený resp. limitovaný v realizácii svojich práv vyplývajúcich z pracovnoprávnych predpisov. Napriek tomu, že v čase písania tohto príspevku nie je možné presne určiť počet takto nesprávne zaradených subjektov

[9] § 41 a nasl. *Zákona č. 311/2001 Z. z. Zákonník práce* (ďalej len ako „ZP“)

[10] § 223 a nasl. ZP

[11] Ako podnikateľ v zmysle ustanovení § 2 ods. 2 *Zákona č. 513/1991 Zb. Obchodný zákonník* (spravidla v postavení SZČO).

[12] RADA EÚ. *Pravidlá EÚ týkajúce sa práce pre platformy* [online]. Consilium Europa, 2023 [cit. 09-09-2023]. Dostupné na: https://www.consilium.europa.eu/sk/policies/platform-work-eu/

v rámci Slovenskej republiky, je dôvodne predpokladať[13], že pomer nesprávne zakvalifikovaných platformových pracovníkov nie je na ústupe. Domnievame sa, že „tradičné“ právne inštitúty slovenského pracovného práva neberú do úvahy špecifický charakter platformovej práce, ktorá v mnohých inštanciách môže vykazovať definičné znaky viacerých „klasických“ inštitútov pracovného práva a v niektorých situáciách aj obchodného práva. Je potrebné si uvedomiť, že *in genere* platformová práca disponuje rozdielnymi charakteristikami ako iné „typické“ formy práce. Medzí hlavné diferencujúce znaky patrí skutočnosť, že v danom prípade výkon práce je vždy realizovaný priamo na digitálnych platformách resp. ich prostredníctvom. Pracovník platformy pri splnení svojich pracovných úloh konštante zanecháva svoje digitálne stopy a môže byť (a spravidla aj je) *de facto* bez prerušenia monitorovaný svojím „zamestnávateľom“ t. j. – platformou.[14] Ďalej chceme poukázať na skutočnosť, že dynamika vzťahov platformových prác sa výrazne líši od tradičných foriem prác. Súvisí to najmä s tým, že predmetné vzťahy nezahŕňajú fundamentálnu dvojstrannú vertikálnu povahu pracovnoprávnych vzťahov, v ktorých vystupujú vždy dva subjekty a to zamestnanec a zamestnávateľ. V prípade platformovej práce ide o špecifickú formu ekonomicky významnej činnosti s unikátnou trojčlennou štruktúrou, zahrnujúcou okrem vyššie spomenutých tradičných aktérov aj konečných užívateľov daných platformových služieb – zákazníkov.[15] Práve z tohto dôvodu je klasický koncept vzťahu nadradenosti a podriadenosti narušený, kvôli čomu v praxi môžu vznikať nejasnosti napríklad vo vzťahu zodpovednostných vzťahov. Ďalšiu rozdielnu charakteristiku predmetnej formy neštandardnej práce tvorí vysoká flexibilita, ako aj špecifická forma odmeňovania, ktorá je spravidla založená na

[13] Vychádzame z dát získaných z analýzy, ktoré jasne demonštrujú tento trend. V uplynulom roku sme boli svedkami zaznamenania historicky najvyššieho počtu novoregistrovaných živností v Slovenskej republike. Na základe podrobného prieskumu, vykonaného ku koncu minulého roka, sa v Slovenskej republike zaregistrovalo viac ako päťstodvadsaťtritisíc fyzických osôb, aktívne vykonávajúcich podnikateľskú činnosť. Zdroj: FINREPORT SK. *Na Slovensku je po prvý raz viac ako pol milióna živnostníkov*, 2023 [cit. 09-09-2023]. Dostupné na: https://www.finreport.sk/podnikanie/na-slovensku-je-po-prvy-raz-viac-ako-pol-miliona-zivnostnikov/.

[14] RÁCZ-ANTAL, I. *A digitalizáció hatása a munkajog egyes alapintézményeire*. Budapest: Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2022, s. 204.

[15] FLORISSON, R. a MANDL, I. *Platform Work: Types and Implications for Work and Employment—Literature Review* [online]. European Foundation for the Improvement of Living and Working Conditions, 2010 [cit. 09-09-2023]. s. 57. Dostupné na: https://www.eurofound.europa.eu/sites/default/files/wpef18004.pdf.

osobitnom vyplácaní honoráru za konkrétnu realizovanú úlohu, ktorá má v podstate funkciu mzdy, avšak môže byť na základe vonkajších faktorov menená. Cena za poskytovanú službu resp. prácu je zvyčajne stanovená platformou a vytvárajúc pre subjekty platformovej práce dynamický charakter odmeňovania.

Z dôvodu vyššie uvedených rozdielov je platformová práca v súčasnom stave *de lege lata* v slovenskom pracovnom práve v aplikačnej praxi ťažko kvalifikovateľná pod konkrétne pracovnoprávne inštitúty. Samozrejme je potrebné zdôrazniť, že súčasné inštitúty pracovného práva vo vzťahu k platformovej práce ako takej nie sú nepoužiteľné, avšak len čiastočne zastrešujú charakter tejto formy práce, z čoho v praxi vznikajú mnohé negatívne dôsledky. Jedným z nich je novodobý fenomén *uberizácie* pracovnoprávnych vzťahov, ktorý je *de facto* novodobou podobou Švarcsystému, v rámci ktorého dochádza k „zamestnaniu podnikateľov" tým, že podnikateľské subjekty realizujú svoje podnikanie v spolupráci s ďalšími podnikateľmi, i keď spomínané fyzické osoby by mohli (aj mali) uskutočňovať danú činnosť v pozícií zamestnancov t. j. v pracovnoprávnom režime v zmysle Zákonníka práce.[16] *Uberizácia* je jedna z moderných foriem spomínaných praktík, kedy v aplikačnej praxi dochádza k nedovolenému zamestnávaniu jednotlivcov disponujúcich so živnostenským oprávnením, spravidla vo vzťahu k úplne alebo čiastočne digitalizovaným prácam resp. pracovným miestam. *Uberizáciu* možno zaradiť pod juresprudenciou označenou širšou kategóriou nútených živností, kedy je zamestnanec donútený zo strany svojho zamestnávateľa, aby prešiel z pracovného pomeru alebo iného pracovnoprávneho vzťahu na status živnostníka – SZČO. V mnohých prípadoch však nedochádza ani k pretransformovaniu pracovných vzťahov na iné právne vzťahy, ale už od samého začiatku, teda od vzniku záväzkového vzťahu, zmluvné strany fungujú v inom právnom režime než pracovnoprávnom. Často je tento proces iniciovaný zo strany samotných *„zamestnancov"*, ktorí sú motivovaní vykonávať závislú prácu[17] predovšetkým z dôvodu krátkodobých finančných ziskov.[18] Naopak, hlavným zámerom zamestnávateľa v tomto procese

[16] HAMUĽÁK, J. *Legal or illegal: právno-teoretické východiská a aplikačné problémy nelegálnej práce a nelegálneho zamestnávania v Slovenskej republike*. Bratislava: Wolters Kluwer, 2017, s. 42.

[17] Pozri ustanovenie § 1 ods. 2 ZP

[18] V prípade, ak fyzická osoba v roku 2022 sa rozhodla, že bude vykonávať svoju činnosť v pracovnom pomere za 1000 EUR, tak z jeho hrubej mzdy odvody predstavovali výšku

je najmä dosiahnutie zániku povinnosti poskytovať rôzne náhrady mzdy, akým je napríklad náhrada mzdy za sviatok v zmysle ustanovenia § 122 a nas. ZP, zbavenie sa zodpovednosti za škodu v prípade pracovných úrazov a chorôb z povolania a vyhnutie sa platby sociálnych odvodov za subjekty pracujúce v pracovnoprávnych vzťahoch. Chceme poukázať na skutočnosť, že pre zamestnancov *uberizácia* spravidla prináša mnohé negatívne sociálne následky ako aj stratu sociálnych istôt a benefitov vyplývajúcich z pracovného pomeru.[19] Navyše benefity, ktoré vyplývajú z takejto formy výkonu práce, akým je flexibilita a zvýšená možnosť osobného rozvoja sú častokrát len akýmisi ilúziami, ktoré pomerne rýchlo zaniknú v dôsledku prísnych zmluvných podmienok takéhoto fingovaného pracovnoprávneho vzťahu. Dobrým príkladom tejto absurdnej situácie je zakotvenie zákazu výkonu inej zárobkovej činnosti podnikateľom – SZČO, inšpirovaného priamo ustanovením § 83 ZP. V zmysle slovenského pracovného práva počas celého trvania pracovného pomeru to znamená, že aj v prípadoch čerpania dovolenky, rovnako aj počas skúšobnej a výpovednej doby, ako aj pri trvaní prekážok v práci, platí prísny zákaz vykonávania konkurenčnej činnosti zamestnanca.[20] Domnievame sa, že zakotvenie generálneho zákazu konkurencie vykonať inú zárobkovú činnosť samostatne zárobkovo činným osobám pri výkone podnikateľskej činnosti, je len ďalším jednoznačným prejavením *uberizácie* pracovnoprávnych vzťahov. Navyše, takáto limitácia SZČO v rámci obchodnoprávnych vzťahov je v rozpore so základnou koncepciou podnikania, ktorá spočíva v osobnej autonómii jednotlivca a slobode výberu z rôznych obchodných príležitostí.

134,00 EUR. Čo sa týka výšky dane, v prípade, ak u svojho zamestnávateľa si uplatňovala nárok na nezdaniteľnú časť základu dane na daňovníka, tak mesačne sa mu z hrubej mzdy zamestnávateľ strhával sumu vo výške 92,03 EUR. Takáto osoba mala **čistú mesačnú mzdu vo výške 773,97 EUR**. Na druhej strane, ak sa tá istá fyzická osoba v roku 2022 rozhodla, že bude tú istú ekonomickú činnosť vykonávať ako SZČO a sa dohodla s odberateľom (zamestnávateľom) na odmene vo výške cenný práce t. j. 1352 EUR (hrubá mzda vo výške 1000 EUR a odvody zamestnávateľa, ktoré predstavujú sumu 352 EUR). Jeho čistý mesačný príjem po splnení svojich daňových a odvodových povinnosti **bol výške 1084,91 EUR.** Pozri: JASPIS. *Odmena za prácu: vychádza lepšie živnosť alebo trvalý pracovný pomer?* [online]. [cit. 11-09-2023] Dostupné na: https://jaspis.sk/aktuality/odmena-za-pracu-zivnost-trvaly-pracovny-pomer

[19] KURIL, J, et al. *Pracovné právo*. Bratislava: Vysoká škola ekonómie a manažmentu verejnej správy, 2014, s. 17 – 18.

[20] RAK, P. Lojalita zamestnanca. Bratislavské právnické fórum 2022 In: *Bratislavské právnické fórum 2022* [elektronický dokument]*:raison d'être pracovného práva a práva sociálneho zabezpečenia na Slovensku - 100 rokov vývoja a vyhliadky do budúcnost*i 1. vyd. – Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2022, s. 122.

Samozrejme, v aplikačnej praxi nie je ojedinelou situáciou, kedy „zamestnancovi“ (teda SZČO) okrem zákazu výkonu inej zárobkovej činnosti je aj v rámci konkrétneho záväzkového vzťahu zakotvený inštitút rovnaký konkurenčnej doložky inšpirovaný ustanovením § 83a ZP.

Ďalším veľkým problémom vyplývajúcim z predmetného nežiadúceho trendu je problematika stálej dostupnosti pracujúcich subjektov pre „zamestnávateľa“. Ochrana rovnováhy medzi pracovným a súkromným životom (ang. *work-life balance*) je vo vysoko *uberizovaných* prácach, akými sú platformová práca a „práce na diaľku“ (telepráca, domácka práca a home-office) stále väčším problémom. Kultúra nepretržitej dostupnosti spolu s právom na odpojenie sú veľmi aktuálnou problematikou neštandardných resp. atypických foriem práce.[21] Tento problém je predmetom záujmu aj na úrovni najvyšších inštitúcií Európskej únie.[22] Je dôležité zdôrazniť, že na vyššie spomenutú problematiku poukázali odborníci pred viac ako desiatimi rokmi. Štúdia z roku 2011, ktorá sa zameriavala na jednotlivcov vykonávajúcich samostatnú zárobkovú činnosť v predmetnom kontexte, dôrazne poukázala na potrebu pracovať dlhé hodiny, aby si predmetní jednotlivci zabezpečili ich sociálne potreby. Z tohto hľadiska sa predpokladá, že tí, ktorí sa angažujú v podnikaní na vlastnú päsť, budú nútení ignorovať tradičné hranice, ktoré kedysi oddeľovali pracovný život od toho súkromného. Výsledkom môže byť nadmerné pracovné zaťaženie a vyhorenie, ktoré môžu nastať pomerne rýchlo.[23]

S určitými rozdielmi na úrovni právnej a sociálnej ochrany pracovníkov platformových prác v porovnaní s „klasickými zamestnancami“ v oblasti pracovného času, minimálnej mzdy a hmotného zabezpečenia, sa vyskytuje aj ďalšia problematika, ktorá býva často prehliadaná, a to nielen laikmi, ale aj odborníkmi. Konkrétne ide o otázku kontroly a monitorovania pracovníkov pôsobiacich

[21] BEZÁKOVÁ, N. Home Office a jeho právny základ v r. 2022 In: *Míľniky práva v stredoeurópskom priestore 2022* [elektronický dokument]: Zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov, 1. vyd. – Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2022, s. 274.

[22] Pozri: Uznesenie Európskeho parlamentu z 21.januára 2021 s odporúčaniami pre Komisiu, pokiaľ ide oprávo na odpojenie (2019/2181(INL)) a Uznesenia Európskeho parlamentu zo dňa 21. januára 2021 s odporúčaniami pre Komisiu, pokiaľ ide o právo na odpojenie (2019/2181(INL))

[23] FLEMING, P. The Human Capital Hoax: Work, Debt and Insecurity in the Era of Uberization. In: *Organization Studies*. Los Angeles: Sage Publications, Vyd. 38, 2017, s. 703-709.

v rámci digitálnych platformách. Trvalý monitoring pracovníkov prostredníctvom online hodnotení zo strany externých subjektov – klientov je novým aspektom, ktorý je následkom digitalizácie práce a získava stále väčší význam v kontexte neštandardných foriem práce. Spomínaný systém digitálneho hodnotenia (spravidla prebieha na diaľku resp. online) slúži ako nepretržitý nástroj na posudzovanie výkonnosti platformových pracovníkov. Mechanizmus predmetného hodnotenia tak slúži nielen na efektívne usmerňovanie pracovných procesov, ale aj na monitorovanie úrovne spokojnosti klientov a na hodnotenie kompetencií pracovníkov v porovnaní s konkurenciou. Je však dôležité si uvedomiť, že takýto systém externého (často anonymného) hodnotenia môže mať nepriaznivý vplyv na pracovné podmienky zamestnancov resp. pracovníkov platforiem. Záporné recenzie, ktoré sa často zakladajú na subjektívnych hodnoteniach a emóciách zákazníkov platforiem, môžu vážne ovplyvniť budúce pracovné príležitosti dotknutých subjektov a v niektorých prípadoch viesť k rýchlemu vylúčeniu pracovníkov z danej digitálnej platformy.[24] Samozrejme nemožno opomenúť komplexnú problematiku monitorovania pracovníkov zo strany platforiem v pozícií zamestnávateľov, ktorá napriek skutočností, že nie je novým fenoménom, avšak v kontexte digitálnych platforiem nadobudla nové rozmery.

3. Európska legislatíva – univerzálny prístup ku komplexnej problematike?

Európska komisia spoločne s odborníkmi v oblasti pracovného práva dlhodobo upozorňuje na potrebu riešiť stále pretrvávajúcu otázku správnej právnej klasifikácie pracujúcich subjektov v rámci platformovej ekonomiky. V praxi je často aplikovaná dlhodobá nesprávna kategorizácia platformových pracovníkov (ako „spolupracujúcich" resp. partnerských subjektov vykonávajúcich určitú prácu v právnom statuse podnikateľov) zo strany platforiem, aj keď realizované činnosti týchto osôb vykazujú jednoznačné znaky závislej práce, priamo posilňuje už vyššie spomenuté stále rastúce trendy *uberizácie* ako aj Švarcsystému resp. môže zvyšovať fenomén

[24] LADIVEROVÁ, E. Crowdwork – človek ako služba. In: *Míľniky práva v stredoeurópskom priestore 2022* [elektronický dokument]: Zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov. 1. vyd. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2022, s. 258.

nelegálnej práce *in genere*. Kompetentné orgány Európskej únie aktívne riešia otázku platformových pracovníkov a samotných platforiem už vyše tri roky. Tento proces bol vzhľadom na komplexitu a citlivosť tejto témy relatívne zdĺhavý aj na pomery inštitúcií EÚ. Navyše je potrebné zdôrazniť, že finalizácia a skutočná implementácia týchto nových pravidiel ešte zďaleka nie je ukončená. V roku 2019 Rada EÚ iniciovala diskusiu o nových paradigmách práce a prijala dôležité uznesenia týkajúce sa tejto problematiky. V svojom závere na danú tému Rada zdôraznila, že je nevyhnutné, aby Európska komisia podnikla kroky na preskúmanie možností, ako zabezpečiť ochranu pracovníkov digitálnych platforiem prostredníctvom vhodných legislatívnych opatrení. Spomínané preskúmanie sa zameralo na problematiku pracovných a sociálnych práv a snažila identifikovať potenciálne oblasti zraniteľnosti pracovníkov v súvislosti s neštandardnými formami práce. V snahe nájsť efektívne riešenia, ktoré by mohli byť implementované prostredníctvom smernice s cieľom zabezpečiť pracovníkom platforiem adekvátnu právnu ochranu v rapídne vyvíjajúcich pracovných podmienkach, Európska komisia predložila Európskemu parlamentu ako aj Rade EÚ na konci roku 2021 návrh týkajúci sa tejto problematike.[25]

Predmetným návrhom smernice sa zavádzajú dve fundamentálne zmeny v tejto oblasti a to:

1. Vytváranie jednotného mechanizmu pre správnu klasifikáciu subjektov pracujúcich v rámci platformovej ekonomiky. Predmetný systém by mal byť postavený na *vyvrátiteľnej domnienke pracovného pomeru (zamestnanosti)* medzi digitálnou platformu a jej pracovníkom. To znamená, že „*osoba sa považuje za pracovníka, ak sú splnené tri zo siedmich kritérií uvedených nižšie*:

I. *Digitálna pracovná platforma určuje hornú hranicu výšky odmeňovania.*
II. *Digitálna pracovná platforma vyžaduje, aby osoba dodržiavala určité pravidlá týkajúce sa vzhľadu, správania voči príjemcovi služby alebo výkonu práce.*
III. *Digitálna pracovná platforma dohliada na výkon práce, a to aj pomocou elektronických prostriedkov.*
IV. *Digitálna pracovná platforma obmedzuje slobodu zvoliť si pracovný čas alebo obdobie neprítomnosti.*

[25] RADA EÚ. *Pravidlá EÚ týkajúce sa práce pre platformy* [online]. Consilium Europa, 2023 [cit. 09-09-2023]. Dostupné na: https://www.consilium.europa.eu/sk/policies/platform-work-eu/

V. *Digitálna pracovná platforma obmedzuje slobodu prijímať alebo odmietať úlohy.*
VI. *Digitálna pracovná platforma obmedzuje slobodu využívať subdodávateľov alebo náhradníkov.*
VII. *Digitálna pracovná platforma obmedzuje možnosti vybudovať si klientsku základňu alebo vykonávať prácu pre akúkoľvek tretiu stranu.*“[26]

Samozrejme pôjde o vyvrátiteľnú prezumpciu, tým pádom digitálna platforma, ktorá v danom prípade znáša dôkazné bremeno, bude môcť v rámci konkrétneho procesu preukázať neexistenciu pracovnoprávneho vzťahu aj v prípade splnení vyššie vymenovaných podmienok.

2. Druhý zásadný prínos navrhovanej smernice sa týka automatizovaných sledovacích a rozhodovacích systémov digitálnych platforiem, ktoré po novom majú byť kontrolované kompetentnými fyzickými osobami. Týmto krokom bude platformovým pracovníkom zabezpečená garancia ľudského dohľadu, pri momentálne spravidla čisto automatizovaných procesoch, týkajúcich sa zásadných pracovných otázok. Táto zmena má poslniť transparentnosť automatizovaných úkonov digitálnych platforiem.[27] V lete tohto roku EÚ dosiahla dôležitý míľnik v procese prijímania smernice na ochranu pracovníkov pôsobiacich na digitálnych platformách. Dňa 12. júna Rada prijala svoje stanovisko k návrhu smernice Európskej komisie. Týmto krokom sa EÚ posunula bližšie k prijatiu prvého komplexného európskeho právneho predpisu, ktorý má za cieľ okrem iného chrániť právny status osôb pracujúcich v rámci platformovej ekonomiky. Samozrejme vítame kroky EÚ vzhľadom na skutočnosť, že táto zmena bola potrebná už dlhší čas. I keď analýza finálneho znenia navrhovanej smernice, ako aj efektivity jej samotného obsahu v aplikačnej praxi je priskorá, na závere tejto kapitoly sa chceme venovať otázke mechanizmu návrhovej smernice, ktorý je založený na prezumpciu zamestnávania. Myšlienka právnej domnienky existencie pracovného pomeru nie je medzi odborníkmi neznámou ideou. Toman napríklad vo vzťahu k interpretačným otázkam závislej práce navrhol, že pri výskyte určitých pochybností by platila vyvrátiteľná domnienka resp. prezumpcia v zmysle ktorej, „*vzťah medzi osobou, ktorá užíva prácu iného a osobou, ktorá ju osobne vykonáva pre túto osobu, je*

[26] Tamtiež
[27] Návrh smernice Európskeho Parlamentu a Rady o zlepšení pracovných podmienok v oblasti práce pre platformy v Bruseli 9. 12. 2021 (762 final, 2021/0414 (cod).

pracovnoprávnym vzťahom podľa Zákonníka práce...“[28] Rovnako i samotné využitie takejto vyvrátiteľnej prezumpcie nie je neobvyklým opatrením v aplikačnej praxi. V spojených štátoch amerických už bola implementovaná takáto vyvrátiteľná právna prezumpcia na vyriešenie problematiky chybného klasifikovania pracovníkov platforiem v rámci *iniciatívy AB*5.[29] Rovnako to je aj na európskom kontinente, kde momentálne je desať členských štátov Európskej únie, disponujúcich právnym poriadkom, v rámci ktorých je zakotvená nejaká forma právnej prezumpcie. Je však dôležité poukázať na skutočnosť, že spomínané právne mechanizmy týchto členských štátov majú spravidla všeobecný charakter resp. vo vybraných prípadoch sa vzťahujú na užšiu skupinu subjektov alebo na jednotlivé sektory. Navyše, žiadny z pracovnoprávnych inštitútov predmetného charakteru nebol stanovený s úmyslom riešiť problematiku nesprávnej klasifikácie v rámci platformovej ekonomiky. Hlavným dôvodom pre túto absenciu bola skutočnosť, že v období, keď boli tieto inštitúty vytvorené, nebola platformová práca ešte takým rozšíreným fenoménom.[30] V tejto inštancii však vzniká legitímna otázka, či plánovaný všeobecný mechanizmus EÚ, založený na vyvrátiteľnej právnej domnienke zamestnanosti, je efektívnym a vhodným celoplošným riešením pre túto problematiku v rámci EÚ. Kullmann zadefinovala dve hlavné negatíva tohto systému. Prvá z týchto problémov bolo identifikovaná vo výročnej správe Európskej agentúry pre bezpečnosť a ochranu zdravia pri práci z roku 2017.[31] V spomínanom dokumente bolo zdôraznené, že zákonná domnienka by mohla naraziť na ťažkosti spojené s klasifikáciou a nevedela by vo veľkej miere vyriešiť súčasné problémy platformových pracovníkov. Argumentom proti potenciálnej neefektívnosti zavedenej právnej domnienky je to, že by stále vyžadovala individuálny prístup pri klasifikácii, najmä pri riešení sporov pred kompetentnými orgánmi alebo súdmi. Súhlasíme s názorom Kullmanna, podľa ktorého tento argument nie je dostatočne

[28] BARANCOVÁ, H. et al. *Pracovné právo v európskej perspektíve*, Praha: Aleš Čenek, 2009, s. 143.

[29] PRINCE, S. J. The AB5 Experiment - Should States Adopt California's Worker Classification Law? [online] In: *American University Business Law Review*. Vyd. 43. 2022, [cit. 12-09-2023] s. 47. Dostupné na: https://ideas.dickinsonlaw.psu.edu/cgi/viewcontent.cgi?article=1330&context=fac-works

[30] KULLMANN, M. Platformisation' of Work: An EU Perspective on Introducing a Legal Presumption. In: *European Labour Law Journal*, Vyd. 13(1), 66–80. 2022, s. 76. DOI: 10.1177/20319525211063112

[31] Pozri: EU-OSHA. *Protecting Workers in the Online Platform Economy: An overview of regulatory and policy developments in the EU*. 2017, s. 5.

presvedčivý, a to z dôvodu, že kategorizácia vždy a v každom prípade vyžaduje individuálne posúdenie, či už vo vzťahu k právnej domnienke alebo bez nej. Druhým argumentom je, že v prípade splnenia konkrétnych podmienok by zo zákona platila prezumpcia, že určité subjekty sú zamestnancami. Tým pádom by zamestnávatelia – platformy museli uniesť bremeno dôkazov pri tvrdení opaku. Je dôvodné predpokladať, že nie každý prípad bude individuálne posudzovaný pred kompetentnými orgánmi.[32] Ďalším potenciálnym obmedzením zavedenia predmetného nového právneho nástroja na úrovni EÚ je, že takýto inštrument by mohol motivovať zamestnávateľov k upravovaniu metód organizácie ich pracovného procesu. Toto by mohlo viesť k novým otázkam týkajúcim sa právnej neistoty.[33] Ako sa hovorí, kde je problém, tam je aj riešenie, a je veľmi pravdepodobné, že mnohým zamestnávateľom (ako aj niektorým pracovníkom) náhla zmena v právnom statuse zamestnancov neposlúži. Je dôležité zvážiť, prečo mnohí ľudia svojvoľne radšej vykonávajú závislú prácu v pozícii SZČO, a prečo sa rozhodli pre tento právny režim, než pre tradičný pracovný pomer. Zastávame názor, že to súvisí najmä s krátkodobými finančnými výhodami tejto formy práce. Práve z tohto dôvodu by kompetentné subjekty mali pouvažovať nad vytvorením nového pracovnoprávneho inštitútu, ktorý by jednak reflektoval špecifiká tejto novodobej formy práce a ponúkal daňové a ďalšie sociálne výhody, ktoré sú spojené s podnikaním ako takým. Napriek uvedeným argumentom sme presvedčení, že zavedenie takéhoto všeobecného systému bude zabezpečovať najširšiu a najkomplexnejšiu ochranu platformových pracovníkov v rámci EÚ. Samozrejme, pri implementácii smernice môžu nastať isté odchýlky v právnej ochrane platformových pracovníkov v jednotlivých krajinách EÚ, avšak smernicou budú stanovené minimálne požiadavky s cieľom zaručiť pracovnoprávnu ochranu v oblasti platformovej ekonomiky v každej krajine EÚ. Navyše jednotnými pravidlami v oblasti pracovnoprávnej ochrany platformových pracovníkov bude posilnená právna istota *in genere*, vďaka ktorej odborové organizácie budú mať jednoduchšiu úlohu pri zastupovaní pracovníkov platforiem v rámci záležitostí týkajúcich sa kolektívneho pracovného práva, pretože identifikácia zamestnancov bude rýchlejšia a jasnejšia. Je dôležité

[32] KULLMANN, M. Platformisation' of Work: An EU Perspective on Introducing a Legal Presumption. In: *European Labour Law Journal*, Vyd. 13(1), 66–80. 2022, s. 73. DOI: 10.1177/20319525211063112

[33] Tamtiež

poukázať na skutočnosť, že vďaka jednotným pravidlám bude aj práca kompetentných orgánov (Národný Inšpektorát práce a Inšpekcie práce) uľahčená v procese identifikácie nelegálneho zamestnávania v rámci platformovej ekonomiky. Na záver by sme chceli zdôrazniť dôležitosť kombinácie správnych legislatívnych opatrení s efektívnym dohľadom, a v prípade porušenia právnych povinností, prísnych sankcií. Dozor a monitorovanie sú kľúčové pre zachovanie obsahu pracovnoprávnych noriem pre všetkých zamestnancov vrátane tých, ktoré pôsobia v čoraz väčšej platformovej ekonomike.

Záver

Práca na digitálnych platformách prináša mnoho výhod, najvýznamnejšou z nich je schopnosť efektívne využiť ponúknutú prácu s jeho aktuálnym dopytom, avšak mechanizmus a fungovanie platformovej ekonomiky prináša aj mnohé nevýhody pre platformových pracovníkov. Kombinácia vysokej súťaživosti, prísnych podmienok práce spolu s konštantou skrutíniou platforiem resp. klientov často vedie k tomu, že pracovníci platforiem prichádzajú o svoje sociálne zabezpečenie zo dňa na deň. Je dôvodné predpokladať, že s narastajúcou popularitou práce na platformách sa bude zvyšovať aj trend „*uberizácie"* pracovných vzťahov. Tento jav je predovšetkým spôsobený tým, že súčasné právne inštitúty v rámci slovenského pracovného práva nedokážu adekvátne zohľadniť špecifický charakter platformovej práce. EÚ si stanovila za cieľ zefektívniť ochranu pracovníkov platforiem pred nesprávnou právnou klasifikáciou, a to prostredníctvom zavedenia všeobecného systému založeného na prezumpcii zamestnávania. Napriek skutočnosti, že predmetným systémom by otázka nesprávnej kvalifikácie platformových pracovníkov mohla byť vyriešená , v súčasnosti na Slovensku stále chýba pracovnoprávny inštitút, ktorý by dostatočne vedel zabezpečiť komplexnú ochranu pracovníkov platforiem berúc do úvahy špecifickosť tejto formy práce. Preto je nevyhnutné, aby slovenský zákonodarca, okrem správneho zakotvenia právneho mechanizmu EÚ, aktualizoval súčasnú pracovnoprávnu legislatívu a to buď novým právnym inštitútom alebo prispôsobením súčasnej legislatívy k špecifikám platformovej práce. V súvislosti s aktualizáciou súčasnej pracovnoprávnej legislatívy, môže prichádzať do úvahy zmena definičných znakov závislej práce v zmysle ZP a to reagujúc na nových trendov a vývoju práce *in genere*. Jedným z potenciálnych návrhov *de*

lege ferenda by mohlo byť zaradenie novej pracovnej formy do existujúcej štruktúry pracovnoprávnych inštitútov, ktorá by zohľadňovala špecifický charakter platformovej práce. Pri implementácii tohto inštitútu by zákonodarca musel venovať osobitnú pozornosť charakteristickým aspektom digitálnych platforiem, akým je flexibilný pracovný čas, spôsob odmeňovania ako aj otázke zodpovednosti v kontexte špecifického trojstranného charakteru tohto typu práce. V rámci slovenského pracovného práva by mohol byť tento nový inštitút zaintegrovaný do deviatej časti ZP, ako špecifická forma dohôd o prácach vykonaných mimo pracovného pomeru.

Použitá literatúra

1. BARANCOVÁ, H. et al. *Pracovné právo v európskej perspektíve*, Praha: Aleš Čeněk, 2009, s. 143. ISBN 9788073802417
2. BEZÁKOVÁ, N. Home Office a jeho právny základ v r. 2022 In: *Míľniky práva v stredoeurópskom priestore 2022* [elektronický dokument]: Zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov, 1. vyd. – Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2022, s. 274. ISBN 978-80-7160-668-0.
3. FLORISSON, R. a MANDL, I. *Platform Work: Types and Implications for Work and Employment–Literature Review* [online]. European Foundation for the Improvement of Living and Working Conditions, 2010 [cit. 09-09-2023]. s. 57. Dostupné na: https://www.eurofound.europa.eu/sites/default/files/wpef18004.pdf.
4. FLEMING, P. The Human Capital Hoax: Work, Debt and Insecurity in the Era of Uberization. In: *Organization Studies*. Los Angeles: Sage Publications, Vyd. 38, 2017, s. 703-709. ISSN 0170
5. HAMUĽÁK, J. Legal or illegal: právno-teoretické východiská a aplikačné problémy nelegálnej práce a nelegálneho zamestnávania v Slovenskej republike. Bratislava: Wolters Kluwer, 2017, s. 42. ISBN 978-80-8168-688-7
6. ILO: *Decent work in the platform economy* [online]. Geneva:International Labour Office,2022, s. 22. [cit. 09-09-2023]. Dostupné na: https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---relconf/documents/meetingdocument/wcms_855048.pdf
7. ILO: Digital labour platforms and the future of work: Towards decent work in the online world. Geneva: ILO, 2018, s. 3. ISBN 978-92-2-031025-0

8. ILO. Non-standard employment around the world: Understanding challenges, shaping prospects. Geneva:International Labour Office,2016, s. 39. ISBN: 978-92-2-130385-5
9. KOWALIK, Z., LEWANDOWSKI, P., KACZMARCZYK, P. Job Quality Gaps between Migrant and Native Gig Workers: Evidence from Poland.In: *IZA Discussion Paper Series*, Bonn: Institute of Labor Economics,2023, No. 16216. s.10. ISSN: 2365-9793
10. KULLMANN, M. Platformisation' of Work: An EU Perspective on Introducing a Legal Presumption. In: *European Labour Law Journal*, Vyd. 13(1), 66–80. 2022, s. 76. DOI: 10.1177/20319525211063112
11. KURIL, J, et al. *Pracovné právo*. Bratislava: Vysoká škola ekonómie a manažmentu verejnej správy, 2014, s. 17 – 18. ISBN 978-80-89654-06-2
12. LADIVEROVÁ, E. Crowdwork – človek ako služba. In: *Míľniky práva v stredoeurópskom priestore 2022* [elektronický dokument]: Zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov. 1. vyd. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2022, s. 258. ISBN 978-80-7160-668-0.
13. PORUBAN, A. Skupinové zamestnávanie ako nový model práce. In*: Sdílená ekonomika sdílený právní problém?* Praha: Wolters Kluwer, 2017, s. 89. ISBN 978-80-7552-874-2.
14. PRINCE, S. J. The AB5 Experiment - Should States Adopt California's Worker Classification Law? [online] In: *American University Business Law Review.* Vyd. 43. 2022, [cit. 12-09-2023].s. 47. Dostupné na: https://ideas.dickinsonlaw.psu.edu/cgi/viewcontent.cgi?article=1330&context=fac-works
15. RADA EÚ. *Infografika – Pracovníci digitálnych platforiem v EÚ* [online]. Consilium Europa, 2023 [cit. 09-09-2023]. Dostupné na: https://www.consilium.europa.eu/sk/infographics/digital-platform-workers/
16. RADA EÚ. *Pravidlá EÚ týkajúce sa práce pre platformy* [online]. Consilium Europa, 2023 [cit. 09-09-2023]. Dostupné na: https://www.consilium.europa.eu/sk/policies/platform-work-eu/
17. RAK, P. Lojalita zamestnanca. Bratislavské právnické fórum 2022 In: *Bratislavské právnické fórum 2022* [elektronický dokument]:raison d´être pracovného práva a práva sociálneho zabezpečenia na Slovensku – 100 rokov vývoja a vyhliadky do budúcnosti 1. vyd. – Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2022, s. 122, ISBN: 978-80-7160-664-2.
18. RÁCZ-ANTAL, I. *A digitalizáció hatása a munkajog egyes alapintézményeire*. Budapest: Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2022, s. 204. ISBN 978-615-5961-83-0

Použité právne predpisy a ďalšie právne dokumenty

1. *Zákon č. 311/2001 Z. z. Zákonník práce*
2. *Zákon č. 513/1991 Zb. Obchodný zákonník*
3. Návrh smernice Európskeho Parlamentu a Rady o zlepšení pracovných podmienok v oblasti práce pre platformy v Bruseli 9. 12. 2021 (762 final, 2021/0414 (cod).

ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLII
2/2023

PROCESNÉ ASPEKTY PREKÁŽKY LITISPENDENCIE V KONTEXTE SLOVENSKEJ A MEDZINÁRODNEJ PRÁVNEJ ÚPRAVY

Bc. Vivienn Üvegesová

Univerzita Komenského v Bratislave, Právnická fakulta
Katedra občianskeho práva
uvegesova2@uniba.sk

Procesné aspekty prekážky litispendencie v kontexte slovenskej a medzinárodnej právnej úpravy

Príspevok sa zameriava na jednu z tzv. procesných podmienok, ktorá musí byť daná, aby sa o veci mohlo konať a rozhodnúť. Prekážka litispendencie má svoje významné postavenie v rámci procesných podmienok a jej vznik je podmienený uplatnením „toho istého" predmetu sporu, či mimosporovej veci na viacerých súdoch, resp. súde a inom orgáne súčasne. Zákonodarca práve v snahe eliminovať množenie sporov v tých istých veciach a v zmysle zásady *ne bis in idem* ju vníma jednoznačne ako dôvod na zastavenie konania v tých prípadoch, ak je daný predpoklad konania v tej istej veci. V súvislosti s touto prekážkou sú v doktríne civilného procesu zásadné otázky vzájomného vzťahu žaloby na plnenie a tzv. určovacej žaloby. Okrem uvedeného sa autorka v príspevku čiastočne zameriava aj na jej vyhodnotenie v kontexte právnych vzťahov s cudzím prvkom v medzinárodnom právnom priestore a pokúsi sa objasniť, či existujú v tomto zmysle spoločné kritériá pre jej existenciu a to aj s ohľadom na právne následky s ňou spojené.

Procedural aspects of lis pendens in the context of slovak and international law

This article is focused on one of the procedural conditions that has to be fulfilled in order for a case to be heard and decided by the court. The obstacle of lis pendens has an important place among the other procedural conditions and its occurrence is conditioned by the assertion of the ‘‘same‘‘subject of litigation or non- litigious matter in several courts or other authority at the same time. The legislator, in an effort to

eliminate multiple disputes in the same subject matter and in accordance with the principle of ne bis in idem, considers it as a reason to stop proceedings in about the same case. In connection with this obstacle, the doctrine of civil procedure deals with the interrelation between claims for performance and so – called declaratory claims. Besides the aforementioned, the author will also focus on its evaluation in the context of legal relations involving a foreign element in international law and they will try to clarify whether there are common criteria for its existence in this sense. Also with regard to the legal consequences associated with it.

Kľúčové slová: prekážka litispendencie, procesné podmienky, žaloba na plnenie, určovacia žaloby, medzinárodné právo procesné

Keywords: lis pendens, procedural conditions, claim for performance, declaratory claims, international procedural law

Úvod

S určitosťou možno skonštatovať, že jednotlivé procesné podmienky majú v civilnom procese značný význam. Je potrebné poukázať na skutočnosť, že žiaden právny predpis neobsahuje ich legálnu definíciu. V odborných literatúrach sú však procesné podmienky vymedzené ako isté predpoklady, ktoré musia byť naplnené na to, aby súd mohol vo veci konať a následne aj rozhodnúť a tým naplniť samotný cieľ civilného procesu.[1] Právna doktrína rozdeľuje procesné podmienky do štyroch základných skupín. Prvú skupinu tvoria *procesné podmienky viažuce sa na súd*, ktorými sú *právomoc* a *príslušnosť súdu*. Druhú skupinu tvoria *procesné podmienky viažuce sa na procesné strany*, medzi ktoré patrí *procesná subjektivita, procesná spôsobilosť a zastúpenie*. Ďalšou skupinou sú *vecné procesné podmienky*, konkrétne ide o *kvalifikované začatie konania (*či už pôjde o žalobu alebo návrh na nariadenie neodkladného alebo zabezpečovacieho opatrenia v sporovom konaní alebo o návrh v rámci mimosporového konania), *zaplatenie súdneho poplatku*. Poslednú skupinu tvoria *negatívne procesné podmienky*, konkrétne ide

[1] Napríklad LÖWY, A. in: Števček, M., Ficová, S. Baricová, J., Mesiarkinová, S., Bajánková, J., Tomašovič, M., a kol. Civilný sporový poriadok, 2 vydanie. Komentár. Praha: C. H. Beck, 2022, s. 655, ŠTEVČEK, M., Straka, R. a kol. Prednášky a texty z civilného procesu. Skriptá. 2 . vydanie. Bratislava : C. H. Beck, 2018, s. 16.

o *prekážku litispendencie* a *prekážku rei iudicatae*.[2] Na vyššie uvedené procesné podmienky súd prihliada ex offo kedykoľvek počas konania, ak zákon neustanovuje inak.[3] Procesné podmienky musia byť vždy splnené, inak by ich nedostatok zapríčinil vadu konania. Ak súd zistí nedostatok procesnej podmienky je povinný vzniknutú vadu odstrániť, a v prípade neodstrániteľných konanie zastaviť.[4]

Článok je zameraný na litispendenciu, na jednu z tzv. negatívnych procesných podmienok, označovaná aj ako prekážka začatého konania. Práve negatívne procesné podmienky sú tie, ktoré sa nesmú v konaní objaviť, pretože ak by boli dané, súd by nemohol v konaní pokračovať a rozhodnúť. V momente začatia civilného konania dochádza k založeniu prekážky litispendencie a preto nebude možné, aby o tej istej veci prebiehalo na súde iné konanie. Článok sa venuje základným kritériám pre posúdenie prekážky litispendencie. Najdôležitejším kritériom je zachovanie totožnosti veci, teda totožnosti strán a predmetu. Je však potrebné poukázať aj na okamih začatia konania a na jeho trvanie v spojitosti s prekážkou začatej veci. Okrem toho sa článok venuje aj jednotlivým procesným následkom litispendencie.

V dôsledku neustálej globalizácie problematika prekážky litispendencie presahuje aj do medzinárodného práva procesného. Na základe tohto sa v článku venujeme okrem všeobecnému vymedzeniu pojmu litispendencia, jej právnej úprave v slovenskom civilnom práve procesnom aj litispendencii upravenej normami medzinárodného práva procesného (ďalej len ako „medzinárodná litispendencia“), a to najmä s poukazom na jeden z prameňov úniovej povahy.

Cieľom článku bude poukázať na jednotlivé procesné aspekty litispendencie v slovenskom civilnom procesnom práve ako aj v slovenskom medzinárodnom práve procesnom. Práve v dôsledku odlišnej vnútroštátnej a medzinárodnej právnej úpravy spôsobuje prekážka litispendencie vznik množstva problematických a nevyriešených otázok. Aj napriek tomu, že slovenská právna úprava litispendencie je v značnej miere jednoduchá a jasná, medzinárodná litispendencia sa vyznačuje menšími nedostatkami.

---

[2] LÖWY, A. in: Števček, M., Ficová, S. Baricová, J., Mesiarkinová, S., Bajánková, J., Tomašovič, M., a kol. Civilný sporový poriadok, 2 vydanie. Komentár. Praha : C. H. Beck, 2022, s. 655.

[3] § 161 zákona č. 161/2015 Z. z. Civilný sporový poriadok (ďalej len ako „CSP“).

[4] ŠTEVČEK, M., Straka, R. a kol. Prednášky a texty z civilného procesu. Skriptá. 2 . vydanie. Bratislava : C. H. Beck, 2018, s. 17.

1. Prekážka litispendencie – prekážka začatého konania

Jednou zo základných ústavnoprávnych zásad procesného práva je nepochybne zásada *ne bis in idem,* z ktorej vyplýva nemožnosť konania a rozhodovania dva krát o tej istej veci. Práve dve negatívne procesné podmienky civilného procesu, ktorými sú *prekážka litispendencie,* označovaná aj ako *prekážka začatej veci* spolu s *prekážkou rei iudicatae* označovaná aj ako *prekážka právoplatne rozhodnutej veci* sú istým premietnutím vyššie spomínanej zásady do nášho právneho poriadku a teda aj do civilného súdneho konania. Ide o dva princípy, ktoré sú navzájom prepojené a ako to uvádza aj Pälsson, na to aby nastali účinky princípu rei iudicate nesmú v žiadnom prípade nastať účinky litispendencie.[5]

Pojem litispendencia pochádza z latinského slovného spojenia lis pendens, ktorého doslovný preklad znamená spočívajúci spor.[6] V záujme zachovania základných princípov civilného procesu je nutné zabezpečiť, aby tú istú vec neprejedávali dva súdy súčasne. V tomto prípade je potrebné podotknúť, že nemusí ísť len o vnútroštátne súdy, keďže problematika súbežných konaní má aj medzinárodný rozmer. S cieľom zabrániť vedeniu súbežných konaní právne poriadky jednotlivých štátov obsahujú právnu úpravu regulujúcu problematiku prekážky litispendencie. Výnimkou nie je ani slovenská právna úprava, v ktorej je prekážka litispendencie zakotvená v § 159 CSP, podľa ktorého *„Začatie konania bráni tomu, aby o tom istom spore prebiehalo na súde iné konanie. Ak na súde prebieha o tom istom spore iné konanie, súd zastaví konanie, ktoré sa začalo neskôr.“*[7]

Podstatou prekážky začatého konania je, že o tom istom predmete sporu a medzi tými istými subjektmi nemôže prebiehať konanie na tom istom alebo inom súde. Rozhodujúcim okamihom na posúdenie prekážky litispendencie je stav v čase začatia konania, ktoré podľa § 156 CSP nastáva *„doručením žaloby alebo návrhu na nariadenie neodkladného opatrenia alebo zabezpečovacieho opatrenia súdu.*[8] Momentom vzniku prekážky litispendencie je doručenie podania vo

[5] PÄLSSON, L. The Institute of Lis Pendens. Scandinavian Studies in Law [online]. 1970, vol. 14, s. 68. [cit. 5.8.2023]. Dostupné na: http://www.scandinavianlaw.se/pdf/14-3.pdf.

[6] REBRO, K. Latinské právnické výrazy a výroky. Bratislava : Obzor. 1986, s. 156.

[7] Je potrebné poukázať na skutočnosť, že analogicky to platí aj v prípade mimosporového konania. V článku používame pojmy ako spor a strany sporu, viažuce sa na sporové konanie, ale je potrebné podotknúť, že v prípade mimosporového konania sa totožnosť účastníkov konania a totožnosť predmetu konania posudzujú rovnako.

[8] Pozri R 97/2003.

veci samej súdu.[9] Z vyššie uvedeného teda vyplýva, že v prípade podania návrhu v takej veci, o ktorej sa už pred súdom koná, je potrebné pristúpiť k zastaveniu nového konania, ktoré začalo v momente doručenia návrhu. Prekážka litispendencie sa považuje za neodstrániteľnú vadu konania podľa § 161 ods. 2 CSP a to vo vzťahu ku konaniam, ktoré začali neskôr a jeho následkom je zastavenie konania. Pri posudzovaní splnenia tejto procesnej podmienky súd koná vždy ex offo, ak zákon neustanovuje inak.[10]

Každý jeden štát by sa mal snažiť odstrániť možný nežiadúci stav zapríčinený paralelne prebiehajúcimi konaniami o tej istej veci. O paralelne prebiehajúcich konaniach hovoríme v prípade, ak popri sebe súbežne prebieha niekoľko konaní s totožným predmetom a subjektmi konania na niekoľkých súdoch. Existuje niekoľko dôvodov prečo je nutné pristúpiť k zamedzeniu viacnásobných konaní o tej istej veci, ktoré súvisia s dodržiavaním jednotlivých princípov civilného procesu. V prípade neexistencie tejto prekážky by bolo možné, aby pred viacerými súdmi prebiehali viaceré konania o tej istej veci a výsledkom by bolo niekoľko rozhodnutí. Takéto situácie by boli v rozpore s princípom hospodárnosti konania a aj s princípom právnej istoty, čo v právnom štáte nie je v žiadnom prípade prípustné.[11] Jej zakotvenie v právnom poriadku preto môžeme hodnotiť pozitívne, ako inštitút zabezpečujúci prevenciu pred množením sporov s cieľom zabrániť vedeniu zbytočných konaní o tej istej veci a vydaniu viacerých nezlučiteľných rozhodnutí, pretože výsledkom každého konania má byť len jedno právoplatne rozhodnutie.

Paralelné konania nemožno považovať len za problematiku civilného práva procesného, ale v dôsledku globalizácie ide o problém riešený medzinárodným právom procesným. Okrem toho, že prekážka litispendencie je upravená v CSP, medzinárodná litispendencia je upravená aj normami medzinárodného práva procesného, ktoré sú unifikované či už v prameňoch úniovej povahy alebo medzinárodnej povahy.

Novelou zákona č. 97/1963 o medzinárodnom práve súkromnom a procesnom („ZMPS“) bolo do nášho právneho poriadku zavedené ustanovenie § 48a upravujúce medzinárodnú litispendeciu v konaniach

[9] LÖWY, A. in: Števček, M., Ficová, S. Baricová, J., Mesiarkinová, S., Bajánková, J., Tomašovič, M., a kol. Civilný sporový poriadok, 2 vydanie. Komentár. Praha : C. H. Beck, 2022, s. 637.

[10] Taktiež, s. 642.

[11] BENEDIK, M. Sporové konanie pre každého. Keď sa už súdu nedá vyhnúť. Bratislava. Wolters Kluwer s. r. o., 2017, s. 165.

s cudzím prvkom. Medzinárodná litispendencia má rovnaký význam ako litispendencia v civilnom práve procesnom s jediným rozdielom a to zabrániť tomu, aby došlo k vzniku paralelných konaní vo viacerých členských štátoch, resp. tretích štátoch a k vydaniu niekoľkých nezlučiteľných rozhodnutí. Medzinárodná litispendencia má svoju úpravu už od prijatia Bruselského dohovoru o právomoci a o uznávaní a výkone rozsudkov v občianskych a obchodných veciach z roku 1968. Bruselský dohovor bol časom nahradený nariadením Rady (ES) č. 44/2001 zo dňa 22.12.2000, o súdnej právomoci a o uznávaní a výkone rozsudkov v občianskych a obchodných veciach (ďalej ako „nariadenie Brusel I“) a ten následne nariadením Rady (EU) č. 1215/2012 o právomoci a uznávaní a o výkone súdnych rozhodnutí v občianskych a obchodných veciach (ďalej ako, „nariadenie Brusel Ia“), ktorý je účinný od roku 2015. Tieto predpisy upravujú situácie, kedy dochádza k vzniku kompetenčných konfliktov medzi súdmi jednotlivých členských štátov Európskej únie. Zároveň je potrebné poznamenať, že prvé dva vyššie spomenuté predpisy však neupravujú situáciu kompetenčného konfliktu medzi súdom členského štátu na jednej strane a súdom tretieho štátu na strane druhej. Ako na to poukazuje aj Burdová významnú zmenu prinieslo až nariadenie Brusel Ia, ktoré upravuje pravidlá pre vedenie konaní v tej istej veci, resp. súvisiacich konaní medzi tými istými účastníkmi konania, ktoré prebiehajú na súde členského štátu EÚ a tretieho štátu.[12]

2. Kritéria pre posúdenie litispendencie

Prekážka litispendencie vedie súd k odmietnutiu vykonávať svoju právomoc a to na základe toho, že už v tej istej veci a medzi tými istými stranami je už na inom súde vedené konanie. Na to, aby nastali účinky litispendencie je potrebné posúdiť, či sú naplnené všetky jej znaky. Pri bližšom posudzovaní charakteristických znakov litispendencie, zistíme, že dôraz sa kladie na totožnosť sporu. Musia byť kumulatívne naplnené dve kritériá, aby sme mohli hovoriť o totožnosti sporu, ktorými sú totožnosť sporových strán a totožnosť predmetu sporu.

Pri určovaní totožnosti strán konania sa nevychádza z ich procesného postavenia, teda je irelevantné, aké procesné postavenie majú v skôr začatom konaní. V jednom konaní môže byť niekto

[12] BURDOVÁ, K. Nariadenie Brusel Ia a tretie štáty. In. Regionalizmus: Stav, východiská, perspektívy : zborník vedeckých prác. - Košice : Univerzita Pavla Jozefa Šafárika, 2013. s. 31.

žalobcom, kým v druhom konaní bude tento subjekt v postavení žalovaného. Totožnosť strán sporu je daná v prípade, ak tie isté subjekty vystupujú v ďalšom konaní, bez ohľadu na ich procesné postavenie. Otázne je, či sa to týka len subjektov v postavení žalobcu a žalovaného alebo aj intervenientov. Prikláňame sa k názoru Tichého, podľa ktorého existenciu intervenientov v jednotlivých konaniach nie je možné považovať za znak totožnosti konania.[13] Najvyšší súd Slovenskej republiky vo svojom rozhodnutí uviedol, že o totožnosť strán sporu pôjde, ak v konaní vystupujú nositelia práv z toho istého právneho vzťahu v opačnom procesnom postavení. O totožnosť strán pôjde aj v prípade, ak by v konaní vystupovali právni nástupcovia účastníkov z konania, ktoré už skončilo.[14] Okrem toho súdy vo svojej rozhodovacej činnosti stanovili aj to, kedy totožnosť strán sporu nie je daná. Ide o prípady, kedy v jednom konaní vystupuje strana ako žalovaný a v inom sporovom konaní ako intervenient na strane žalovaného.[15] Totožnosť sporových strán nie je daná ani v prípade konania o splnenie dlhu medzi veriteľom a dlžníkom a konania o splnenie toho istého dlhu medzi veriteľom a ručiteľom dlžníka.[16]

Súdny dvor Európskej únie pristupuje k výkladu pojmu *tie isté subjekty* veľmi zaujímavo. Podľa neho tento pojem sa vzťahuje aj na také prípady, kde síce formálne účastníci nie sú totožní, ale ich záujmy sú natoľko totožné a prepojené, že sa považujú za jedného účastníka. V dôsledku toho, je preto vždy potrebné skúmať skutočné záujmy, ktoré sú v danom konaní zastupované. V prípade, ak totiž takéto záujmy strán nie sú zhodné, nemožno brániť stranám, aby si uplatňovali svoje nároky voči iným.[17]

Pri určovaní totožnosti sporu je smerodajným kritériom aj posudzovanie totožnosti predmetu sporu. O totožnosť predmetu sporu pôjde, ak v neskôr začatom civilnom súdnom konaní sa uplatňuje ten istý nárok, ktorý sa uplatňuje v pôvodnom konaní. Zároveň platí, že nie je možné posudzovať totožnosť nároku len podľa žalobného návrhu, ale aj podľa právneho dôvodu, teda skutkových tvrdení, o ktoré žalobca

[13] TICHÝ, Ľ. Problematika litispendence a jejích následků v nařízení Brusel I bis i ve vztahu k třetím státům. In. Právnik, ročník: 158, č. 11 /2019, s. 1023.

[14] Uznesenie Najvyššieho súdu Slovenskej republiky sp. zn. 5 Cdo 280/2010.

[15] Uznesenie Najvyššieho súdu Slovenskej republiky sp. zn. 3 Cdo 168/2008.

[16] Uznesenie Najvyššieho súdu Českej republiky sp. zn. 20 Cdo 723/2000.

[17] Vec C- 351/96 Drouot assurances SA proti Consolidated metallurgical industries (CMI industrial sites), Protea assurance a Groupement d'intérêt économique (GIE) Réunion européenne, 1998, bod. 19.

opiera svoj nárok v konaní.[18] Totožnosť predmetu konania je totožnosť nároku uplatneného z rovnakého skutkového základu či skutkového deja. Totožnosť predmetu konania je daná vtedy, keď ten istý nárok alebo stav vymedzený žalobným petitom vyplýva z rovnakých skutkových tvrdení, na základe ktorých bol uplatnený.[19] Je potrebné poznamenať, že pri žalobnom návrhu nie je podstatná jeho formulácia v jednotlivých žalobách, ale sleduje sa jeho obsahová stránka, t. j. čoho sa žalobca domáha. Prekážka litispendencie sa neuplatní, ak ide o totožnú vec v právnom zmysle, ale strany si k veci uplatňujú odlišné procesné nároky.[20]

Súdny dvor Európskej únie prispel svojou rozhodovacou činnosťou k definovaniu pojmu tá istá vec, pričom pri definovaní vychádzal z konceptu založenom na znení Bruselského dohovoru. O totožný predmet konania ide, ak konania smerujú k rovnakému výsledku (objet po francúzsky) a majú ten istý právny základ, dôvod (cause po francúzsky).[21] Podľa Súdneho dvora Európskej únie totožnosť veci je zachovaná aj v prípade, ak v jednom spore ide o pozitívny nárok strany na plnenie a v druhom o negatívnu určovaciu žalobu, v prípade, ale musí byť zachovaná tá istá vec, ktorá tvorí základ sporu.[22]

Právne relevantnou sa javí aj otázka, či je pre posúdenie totožnosti paralelného konania rozhodujúci skutkový stav na začiatku konania, ktorý je opísaný v žalobe alebo skutkové zistenia opísané v meritórnom rozhodnutí.

Môžeme konštatovať, že samotný skutkový základ nároku ako jeden zo znakov predmetu konania má, „relatívny“ charakter a môže sa v priebehu konania meniť. To jednoducho znamená, že paralelné konania, ktoré sa na začiatku sa vyznačujú totožnosťou predmetu konania, už nemusia byť totožné na konci, a práve v dôsledku toho problém prekážky litispendencie v neskoršom štádiu konania zaniká.[23] Vymedzenie pojmu „totožnosť skutku“ je nevyhnutné najmä preto, že žalobu, v ktorej je skutok dostatočne identifikovaný nemožno zamietnuť na základe nedostatočných skutkových tvrdení a tiež preto,

[18] HORA, V. Československé civilní právo procesní. I – III. Díl. Praha : Wolters Kluwer, 2010, s. 170.

[19] Uznesenie Najvyššieho súdu Slovenskej republiky sp. zn. 5 Cdo 280/2010.

[20] Uznesenie Najvyššieho súdu Českej republiky sp. zn. 26 Cdo 2659/2005.

[21] Vec C- 406/92 The owners of the cargo lately laden on board the ship „Tatry“ proti the owners of the ship „Maciej Rataj“, 1994, bod 37.

[22] Vec -144/86. Gubisch Maschinenfabrik KG v Giulio Palumbo. 1987, odsek 14.

[23] Pozri bližšie TICHÝ, Ľ. Problematika litispendence a jejích následků v nařízení Brusel I bis i ve vztahu k třetím státům. In. Právnik, ročník: 158, č. 11 /2019, s. 1021.

že dôvodom na zmenu žaloby je len také doplnenie skutkových tvrdení žalobcu, ktoré spochybňuje „totožnosť“ skutku opísaného v žalobe.[24]

Okrem totožnosti sporu ďalším kritériom pre posúdenie medzinárodnej litispendencie je časový okamih jej vzniku. Pôvodne platilo, že jednotlivé štáty mali stanovovať čas začatia konania. Problém však nastával v dôsledku odlišnej právnej úpravy v jednotlivých štátoch. Prijatím nariadenia Brusel Ia došlo istým spôsobom k zjednoteniu začatia konania. Podľa článku 32 Nariadenia Brusel Ia konanie na súde je začaté 1. v momente podania písomnosti (alebo rovnocennej písomnosti), ktorou sa konanie začína ale len za predpokladu, že žalobca urobil všetko pre to, aby sa písomnosť doručila žalovanému alebo 2. ak ide o písomnosť, ktorá sa musí doručiť pred podaním na súd, tak konanie začne v momente jej prevzatia orgánom povereným doručovaním opäť za predpokladu, že žalobca príjme kroky, aby zabezpečil podanie písomnosti na súde.[25] V oboch prípadoch sa vyžaduje, aby z procesného hľadiska žalobca realizoval ďalšie kroky. Síce ustanovenie presne nešpecifikuje lehotu, počas ktorej musí žalobca vykonať jednotlivé kroky, je možné v tomto prípade vychádzať z národných procesných noriem, prostredníctvom ktorých by sa posudzovala neprimeraná dĺžka lehoty na zrealizovanie úkonov. Ako sme na to už poukázali, na Slovensku konanie začína momentom doručenia žaloby súdu. Práve jedným z najdôležitejších procesných účinkov začatia konania je prekážka litispendencie. Z našej právnej úpravy vyplýva, že sa nevyžaduje zo strany žalobcu, aby po podaní podania, vykonal ďalšie právne úkony na to, aby bola založená prekážka.

Opätovne je potrebné poznamenať, že na to, aby došlo k vzniku litispendencie samotný žalobný petit by mal byť totožný a to v označení právnych následkov a v druhoch žaloby. Na otázku, či totožnosť druhov žalôb vôbec zakladá prekážku litispendencie neexistuje jednotný názor. Viaceré súdne rozhodnutia potvrdzujú, že konanie začaté na základe určovacej žaloby (kladnej alebo zápornej) nezakladá prekážku litispendencie pre konanie začaté na základe žaloby o plnenie. Naopak to však neplatí, pretože konanie, ktoré sa týka splnenia povinnosti je prekážkou začatého konania o určenie toho, či to právo

[24] SVOBODA, K. Totožnost skutku v civilním procesu. Právní rozhledy, 2010, č. 22, s. 815.
[25] LACKO, P. Nariadenie Brusel I. Komentár. Bratislava : Wolters Kluwer, 2016, s. 171.

alebo právny vzťah je alebo nie je.[26] Na rozdiel od rozhodovacej praxe, odborná náuka k tejto otázke pristupuje odlišne. Podľa niektorých českých autorov tým, že súd v konaní posudzuje existenciu alebo neexistenciu práva len ako istú predbežnú otázku, tak sa to nepremieta do výroku rozhodnutia ale len do odôvodnenia. V takomto prípade rozsudok nebude môcť byť z materiálnej stránky právoplatný. [27]

3. Právne následky litispendencie

Pravdepodobne jedným z najproblematickejších aspektov inštitútu litispendencie sú jednotlivé právne následky s ním spájané. Slovenská právna úprava rieši situácie paralelných konaní zastavením konania podľa § 159 CSP. Pri vnútroštátnych sporoch tento inštitút nespôsobuje problémy, keďže právna úprava obsiahnutá v CSP je jasná a nedochádza k jej zneužívaniu. V oblasti medzinárodného práva procesného sa v priebehu rokov medzinárodná litispendencia špecializovala a to s cieľom odstrániť jej možné nedostatky. Nariadenie Brusel Ia podobne ako nariadenie Brusel I a Bruselský dohovor, stanovuje dva procesné nástroje, ktorých základom je dôvera v právomoc iného štátu a ktoré sa používajú na kvalifikované vedenie konania, ktoré bolo predtým začaté na inom súde.[28] Týmito procesnými nástrojmi sú odmietnutie právomoci a prerušenie konania.

Na základe článku 29 nariadenia Brusel Ia ten súd, ktorý nezačne konať ako prvý a v tej istej veci medzi tými istými účastníkmi sa vedú konania na súdoch rôznych členských štátov je povinný aj bez návrhu prerušiť konanie, až do momentu pokým sa nepotvrdí právomoc súdu, ktorý začal konať ako prvý a to bez toho, aby bol dotknutý článok 31 ods. 2 nariadenia Brusela Ia. Článok 29 nariadenia Brusel Ia, so sebou prinieslo niekoľko problémov, pretože častokrát dochádzalo k jeho zneužívaniu jednotlivými procesnými stranami. Dochádzalo k situáciám kedy, niektorá zo sporových strán podala na súd v danom štáte negatívnu určovaciu žalobu aj keď vedela, že ten konkrétny súd nemá v danej veci právomoc a to predtým, než druhá strana stihla podať žalobu na plnenie na súde, ktorý právomoc má za účelom časového

[26] Pozri rozsudok Najvyššieho súdu Slovenskej republiky sp. zn. 3Cdo/100/1, uznesenie Najvyššieho súdu Českej republiky sp. zn. 20Cdo 2931/99, uznesenie Krajského súdu v Bratislave sp. zn. 14 Co/140/2001.

[27] DAVID,L. a kol. Občanský soudní řád. Komentář. I. díl. Praha: Wolters Kluwer, 2009, s. 727.

[28] TICHÝ, Ľ. Problematika litispendence a jejích následků v nařízení Brusel I bis i ve vztahu k třetím státům. In. Právnik, ročník: 158, č. 11 /2019, s. 1026.

predlžovania sporu. V takom prípade musel súd, na ktorom bola neskôr podaná žaloba konanie prerušiť a čakať, kým prvý súd nerozhodne o tom, že právomoc mu neprislúcha. Časové predlžovanie sporu slúžilo na získanie určitých výhod v konaní daným subjektom, či už možnosť pre zaobstaranie dôkazov, svedkov alebo naopak možnosť získať čas na odstránenie vecí, svedčiacich v ich neprospech. Za účelom zabránenia takýchto situácií bolo prijaté ustanovenie čl. 31ods. 2. Podľa tohto článku, v prípade, ak začne konať súd členského štátu, ktorému prislúcha výlučná právomoc na základe dohody uvedenej v článku 25 nariadenia Brusel Ia, akýkoľvek súd iného členského štátu je povinný prerušiť konanie dovtedy, pokým súd, ktorý koná na základe dohody nevyhlási, že nemá právomoc podľa tejto dohody.

Na to, aby súd, pred ktorým začalo konanie neskôr mohol prerušiť konanie musí byť podľa článku 29 ods. 2 nariadenia Brusel Ia bezodkladne informovaný iným súdom o inom prebiehajúcom konaní, ktoré začalo skôr. Pre zabezpečenie právnej istoty a dodržanie zásady rýchlosti a hospodárnosti konania by bolo vhodné, ak by zákonodarca v tomto ustanovení bližšie stanovil lehotu, v rámci ktorej by sa mala poskytnúť informácia danému súdu a aj lehotu na ďalšie procesné rozhodnutia, Ako na to poukazuje aj Tichý v nariadení Brusel Ia neexistujú žiadne špecificky stanovené lehoty na rozhodovanie súdov, a teda ani žiadne sankcie za oneskorené splnenie týchto povinností. Poukazuje na to, že pojem „bezodkladne“ v článku 29 ods. 2 nariadenia Brusel Ia sa má vykladať v tom zmysle, že súd by mal rozhodnúť o svojej právomoci do šiestich mesiacov od začatia konania.[29]

V praxi k prerušeniu konania dochádza na základe návrhu účastníkov konania, čo nie je samozrejme pravidlom a súd môže komunikovať s inými súdmi aj ex offo z vlastnej iniciatívy alebo z iniciatívy iných subjektov než účastníkov konania. Pre zefektívnenie komunikácie a zabezpečenie väčšej súčinnosti medzi jednotlivými súdmi by bolo vhodné zaviesť povinnú evidenciu jednotlivých konaní začatých v medzinárodnom priestore a to prostredníctvom verejného registra. V súčasnosti elektronická komunikácia už nie je žiadnym problémom a preto vytvorenie jednotného registra, v ktorom by boli vedené všetky prebiehajúce konania, by bol veľkým pokrokom v oblasti súdnictva.

Podľa článku 29 ods. 3 nariadenia Brusel Ia súd, ktorý začal konať neskôr svoju právomoc odmietne a to, či už formou zamietnutia alebo

[29] Tamtiež.

odmietnutia žaloby. Takýmto procesným rozhodnutím súd vyjadruje svoje presvedčenie, že na inom súde prebieha konanie, ktorému dáva prednosť a pred ním konanie definitívne končí. Zavedením tohto ustanovenia sa sledovalo zamedzenie zdržovacích taktík, ku ktorým častokrát dochádzalo zo strany účastníkov konania. Je potrebné podotknúť, že ten istý procesný postup platí aj v prípade uplatnenia článku 31 nariadenia Brusel Ia, ktorý v odseku 3 uvádza, že ak súd, ktorý bol zvolený dohodou strán potvrdí svoju právomoc, súd iného členského štátu je povinný odmietnuť vykonávať svoju právomoc v prospech tohto súdu. Je potrebné zdôrazniť fakt, že jedine súd, pred ktorým skôr začalo konanie má právomoc rozhodnúť o svojej právomoci. Ak o nej rozhodne, toto rozhodnutie súdu je záväzné a súd, ktorý začal konať neskôr ju nemôže preskúmavať. Rovnako sa to uplatní aj v prípade, ak by súd, ktorý začal konať neskôr mal pochybnosti o právomoci, poprípade by bol presvedčený, že na strane prvého súdu je nedostatok právomoci.[30]

Jedným z nedostatkov nariadenia Brusel Ia je neexistencia ustanovenia, ktorý by stanovoval určitú sankciu za porušenie ustanovenia týkajúcej sa výlučnej právomoci. To znamená, že ak vo veci rozhodol iný súd než ten, ktorý by mal na základe dohody o voľbe právomoci, rozhodnutie takéhoto súdu by bolo možné uznať a vykonať v iných členských štátoch. Takáto situácia však vedie k narúšaniu jedného zo základných princípov civilného konania, ktorým je princíp právnej istoty. Preto je potrebné, aby zákonodarca *de lege ferenda* pristúpil k upresneniu postupu uplatňovania článku 31 nariadenia Brusel Ia.

Okrem totožných konaní nariadenie Brusel Ia obsahuje aj právnu úpravu týkajúcu sa súvisiacich konaní. O súvisiace konania ide, „*ak sú navzájom tak úzko spojené, že je vhodné prerokovať a rozhodnúť ich spoločne, a tak sa vyhnúť riziku nezlučiteľných rozsudkov vydaných v samostatných konaniach*.“[31] Na rozdiel od totožných konaní v prípade ak sa na súdoch rôznych členských štátov vedú súvisiace konania, tak súd, ktorý začal konať neskôr môže prerušiť konanie. To znamená, že prerušenie konania podľa článku 30 ods. 1 nariadenia Brusel Ia je fakultatívne. Zaujímavou otázkou sa javí to, za akých okolností by sa malo pristúpiť k prerušeniu konania a na čo by mali súdy pri

[30] Pozri bližšie vec C-351/89 Overseas Union Insurance Ltd a Deutsche Ruck Uk Reinsurance Ltd a Pine Top Insurance Company Ltd proti New Hampshire Insurance Company, 1991, odsek 22,26.

[31] Pozri bližšie článok 31 ods. 3 nariadenia Brusel Ia.

rozhodovaní brať ohľad. V prípade nejakých pochybností by súdy mali konanie prerušiť. Pri prerušení konania by sa malo prihliadať v prvom rade na ako konania spolu súvisia a riziko navzájom nezlučiteľných rozhodnutí. Rovnako dôležitá je aj samotná fáza, v ktorej jednotlivé konania sú a blízkosť konania vo vzťahu k predmetu sporu.[32]

Záver

Prekážka litispendencie je podľa právnej náuky považovaná za jednu z tzv. negatívnych procesných podmienok, ktorá vylučuje možnosť súdu, aby vo veci mohol konať a autoritatívne rozhodnúť. Úvod aj prvá kapitola článku boli primárne venované všeobecnému vymedzeniu pojmu litispendencia, jej významu a právnej úprave, či už na národnej alebo medzinárodnej úrovni. S jednoznačnosťou možno skonštatovať, že slovenská právna úprava litispendencie je v značnej miere jednoduchá a neprináša problémy na rozdiel od medzinárodnej právnej úpravy.

Prekážku litispendencie možno považovať za jeden zo spôsobov riešenia paralelných súdnych konaní, ktorý je typický hlavne pre kontinentálny systém. Právna úprava litispendencie má význam predovšetkým v tom, že vďaka nej je možné predísť vzniku nezlučiteľných súdnych rozhodnutí, ktoré medzi sebou vytvárajú konflikt a ďalej taktiež podporuje hospodárnosť súdneho konania.

Pre bližšie pochopenie litispendencie bolo potrebné charakterizovať jej hlavné znaky, ktoré sú spoločné pre jednotlivé právne úpravy. Druhá kapitola článku sa venuje jednotlivým kritériám pre posúdenie litispendencie. Najdôležitejšími kritériami pre jej posúdenie je zachovanie totožnosti veci, t. j. totožnosti predmetu a totožnosti subjektov. Podmienka totožnosti subjektov je naplnená, ak tie isté subjekty vystupujú v ďalšom konaní, bez ohľadu na ich procesné postavenie a podľa názoru Súdneho dvora Európskej únie je potrebné posudzovať aj spoločné záujmy. O totožnosť predmetu sporu ide, ak v neskôr začatom civilnom súdnom konaní sa uplatňuje ten istý nárok, ktorý sa uplatňuje v pôvodnom konaní, ale nárok sa neposudzuje len podľa žalobného návrhu, ale aj podľa skutkových tvrdení, o ktoré žalobca opiera svoj nárok v konaní. Napokon pri posudzovaní splnenia podmienok medzinárodnej litispendencie je rozhodujúce aj určenie

[32] Návrh generálneho advokáta zo 16. septembra 1993 vo veci C-129/92, Owens Bank Ltd proti Fulvio Bracco a Bracco Industria Chimica SpA, 1994, bod 76.

časového okamihu začatia konania. Vďaka článku 32 Nariadenia Brusel Ia je už okamih začatia konania jasnejší, pretože konanie môže začať v momente podania písomnosti alebo prevzatím písomnosti príslušným orgánom pre doručovanie, ak sa písomnosť najprv doručuje súdu, za predpokladu, že žalobca zrealizuje ďalšie kroky.

Posledná kapitola článku bola zameraná na jednotlivé právne následky medzinárodnej litispendencie v nariadení Brusel Ia. Jedným z hlavných následkov je prerušenie konania a to aj bez návrhu zo strany súdu, ktorý nezačne konať ako prvý a už tej istej veci medzi tými istými účastníkmi sa vedie konanie na súdoch rôznych členských štátov až do momentu pokým sa nepotvrdí právomoc súdu, ktorý začal konať ako prvý. Takáto právna úprava si však z dôvodu zneužívania jednotlivými subjektmi vyžiadala zmenu. Práve za účelom zabránenia takýchto situácií bolo prijaté ustanovenie, ktoré ustanovilo, že v prípade v prípade, ak začne konať súd členského štátu, ktorému prislúcha výlučná právomoc, akýkoľvek súd iného členského štátu je povinný prerušiť konanie dovtedy, pokým súd, ktorý koná na základe dohody nevyhlási, že nemá právomoc podľa tejto dohody. Súd na to, aby prerušil konanie musí byť bezodkladne informovaný o prebiehajúcom konaní. Z nášho pohľadu by *de lege ferenda* mal zákonodarca pre zabezpečenie právnej istoty a dodržanie zásady rýchlosti a hospodárnosti konania stanoviť lehotu, v rámci ktorej by sa mala poskytnúť informácia danému súdu a aj lehotu na ďalšie procesné rozhodnutia.

Pri komparácií sme dospeli k niektorým nedostatkom, ktoré z nášho pohľadu potrebujú výraznejšiu zmenu. Z nášho pohľadu pre zefektívnenie komunikácie a zabezpečenie väčšej súčinnosti medzi jednotlivými súdmi by bolo vhodné zaviesť povinnú evidenciu jednotlivých konaní začatých v medzinárodnom priestore a to prostredníctvom verejného registra dostupného pre všetky súdy. Súdy by sa touto cestou rýchlejšie dozvedeli o prebiehajúcich konaniach, keďže v súčasnosti elektronická komunikácia je základom fungovania celého sveta. Vytvorenie jednotného registra de, v ktorom by boli vedené všetky prebiehajúce konania, by bol veľkým pokrokom v oblasti súdnictva.

Za nedostatok nariadenia Brusel Ia považujeme aj neexistenciu ustanovenia, ktoré by stanovovalo určitú sankciu za porušenie ustanovenia týkajúceho sa výlučnej právomoci. Čo v prípade, ak v danej veci rozhodne iný súd než ten, ktorý by mal na základe výlučnej právomoci založenou dohodou strán o voľbe právomoci podľa článku

25 nariadenia Brusel Ia. Bude takéto rozhodnutie súdu naozaj možné uznať a vykonať v iných členských štátoch? Z nášho pohľadu takáto nedostatočná právna úprava vedie k narúšaniu jedného zo základných princípov civilného konania, ktorým je princíp právnej istoty. Preto je potrebné, aby zákonodarca *de lege ferenda* pristúpil k upresneniu takýchto situácií.

Zoznam použitej literatúry

1. BENEDIK, M. Sporové konanie pre každého. Keď sa už súdu nedá vyhnúť. Bratislava. Wolters Kluwer s. r. o., 2017.
2. DAVID, L. a kol. Občanský soudní řád. Komentář. I. díl. Praha: Wolters Kluwer, 2009.
3. HORA, V. Československé civilní právo procesní. I. – III. díl. Praha : Wolters Kluwer, 2010.
4. LACKO, P. Nariadenie Brusel I. Komentár. Bratislava : Wolters Kluwer, 2016.
5. LÖWY, A. In: Števček, M., Ficová, S. Baricová, J., Mesiarkinová, S., Bajánková, J., Tomašovič, M., a kol. Civilný sporový poriadok, 2. vydanie. Komentár. Praha : C. H. Beck, 2022.
6. ŠTEVČEK, M., Straka, R. a kol. Prednášky a texty z civilného procesu. Skriptá. 2. vydanie. Bratislava : C. H. Beck, 2018.

Elektronické zdroje

7. BURDOVÁ, K. Nariadenie Brusel Ia a tretie štáty. In. Regionalizmus: Stav, východiská, perspektívy: zborník vedeckých prác. - Košice : Univerzita Pavla Jozefa Šafárika, 2013.
8. PÄLSSON, L. The Institute of Lis Pendens. Scandinavian Studies in Law [online]. 1970, vol. 14, s. 68. [cit. 5.8.2023]. Dostupné na: http://www.scandinavianlaw.se/pdf/14-3.pdf
9. REBRO, K. Latinské právnické výrazy a výroky. Bratislava : Obzor. 1986.
10. SVOBODA, K. Totožnost skutku v civilním procesu. Právní rozhledy, 2010, č. 22.
11. TICHÝ, Ľ. Problematika litispendence a jejích následků v nařízení Brusel I bis i ve vztahu k třetím státům. In. Právnik, ročník: 158, č. 11/2019.

Judikatúra

12. R 97/2003
13. Rozsudok Najvyššieho súdu Slovenskej republiky sp. zn. 3Cdo/100/01,
14. Uznesenie Najvyššieho súdu Slovenskej republiky sp. zn. 3 Cdo 168/2008.
15. Uznesenie Najvyššieho súdu Slovenskej republiky sp. zn. 5 Cdo 280/2010.
16. Uznesenie Najvyššieho súdu Českej republiky sp. zn. 20 Cdo 723/2000.
17. Uznesenie Najvyššieho súdu Českej republiky sp. zn. 26 Cdo 2659/2005.
18. Uznesenie Najvyššieho súdu Českej republiky sp. zn. 20 Cdo 2931/99.
19. Uznesenie Krajského súdu v Bratislave sp. zn. 14 Co/140/2001.
20. Vec C- 351/96 Drouot assurances SA proti Consolidated metallurgical industries (CMI industrial sites), Protea assurance a Groupement d'intérêt économique (GIE) Réunion européenne, 1998, bod. 19.
21. Vec C- 406/92 The owners of the cargo lately laden on board the ship „Tatry" proti the owners of the ship „Maciej Rataj", 1994, bod 37.
22. Vec -144/86. Gubisch Maschinenfabrik KG v Giulio Palumbo. 1987, odsek 14.
23. Vec C-351/89 Overseas Union Insurance Ltd a Deutsche Ruck Uk Reinsurance Ltd a Pine Top Insurance Company Ltd proti New Hampshire Insurance Company, 1991, odsek 22,26.
24. Návrh generálneho advokáta zo 16. septembra 1993 vo veci C-129/92, Owens Bank Ltd proti Fulvio Bracco a Bracco Industria Chimica SpA, 1994, bod 76.

ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLII
2/2023

METODIKA VYŠETŘOVÁNÍ KYBERGROOMINGU[1]

Mgr. Daniel Oborák

Univerzita Karlova Praha, Právnická fakulta
Katedra trestního práva
daniel.oborak@prf.cuni.cz

Metodika vyšetřování kybergroomingu

Článek se zabývá kybergroomingem, novým typem kriminálního jednání spočívajícím v cíleném navazování vztahu útočníka s dítětem za účelem jejího sexuálního zneužití, ke kterému dochází prostřednictvím kyberprostoru, a to konkrétně optikou kriminalistické teorie a vyšetřovací praxe. Autor si v článku klade za cíl vytvořit jednotnou a komplexní metodiku vyšetřování tohoto druhu kriminality, která bude reflektovat duální povahu této trestné činnosti, tedy její kybernetické i mravnostní aspekty, včetně veškerých specifik a zvláštností, které vyšetřování kybergroomingu doprovázejí. Článek vychází nejen z kriminalisticko-teoretického základu daného problému obsaženého ve vědeckých monografiích a odborných článcích, ale reflektuje rovněž každodenní praxi vyšetřovatelů specializovaných na tuto problematiku. Článek obsahuje základní kriminalistickou charakteristiku kybergroomingu, vymezuje typické stopy, které při páchání tohoto typu kriminality vznikají, jakož i specifika předmětu vyšetřování, tedy přehled nejdůležitějších informací o činu a o jeho pachateli, jejichž získání by mělo být z hlediska objasnění věci hlavním cílem orgánu činného v trestním řízení. Zmíněny jsou rovněž specifika podnětů k vyšetřování, která jsou ovlivněna zejména skutečností, že dítě jakožto typická oběť kybergroomingu zpravidla nebude sama oznamovatelem trestného činu. Jádro článku tkví zejména v představení specifik počátečních a následných úkonů při vyšetřování kybergroomingu, kde se zabývá zejména problematikou volatilní povahy digitálních stop, jejichž správné zajištění je klíčem k úspěchu ve vyšetřování kybergroomingu. Závěrem je autorem zdůrazněn

[1] Tento text byl zpracován v rámci projektu studentského vědeckého výzkumu „Trestní řád de lege lata i de lege ferenda v ústavněprávních souvislostech“ realizovaného v roce 2023 na Právnické fakultě Univerzity Karlovy, SVV 260 620/2023.

význam zapojení veřejnosti při potírání kybergroomingu, zejména co se týče primární prevence cílené na děti.

The Methodology of Cybergrooming Investigation

This paper deals with cybergrooming, a new type of criminal behavior described as targeted establishment of a relationship between an attacker and a child for the purpose of his/her sexual abuse, which takes place through cyberspace, which is examined specifically through the lens of forensic science and investigative practice. The article aims to create a unified and comprehensive methodology for the purpose of investigating this type of crime, which shall reflect the dual nature of this criminal activity, its cybercrime and sexcrime aspects, including all the specifics that accompany the investigation of cybergrooming. The article is based not only on the basis of forensic theory contained in scientific monographs and articles, but also reflects the everyday practice of investigators specialized in this issue. The paper contains the basic forensic characteristics of cybergrooming, it also defines the typical clues that form when the crime happens, as well as the specifics of the subject of the investigation, i.e. an overview of the most important information about the crime and its perpetrator, the acquisition of which should be the main goal of the investigators for the purpose of solving the actual crime. The specifics of the incentives for the investigation are also mentioned, which are influenced in particular by the fact that a child, as a typical victim of cybergrooming, will usually not report the crime himself. The most important part of the entire work lies mainly in the presentation of the specifics of the initial and subsequent actions during the investigation of cybergrooming, where the work mainly deals with the issue of the volatile nature of digital clues, which should be secured correctly for the purpose of achieving succes in the investigation of cybergrooming. In conclusion, the author emphasizes the importance of public involvement in combating cybergrooming, especially with regard to primary prevention aimed at children.

Klíčová slova: kybergrooming, metodika vyšetřování, kybernetická kriminalita

Key words: cybergrooming, investigation methodology, cybercrime

Úvod

Vyšetřování mravnostních trestných činů páchaných na dětech bylo odjakživa z hlediska kriminalistiky neobvykle obtížnou disciplínou vyžadující specifickou odbornost a zvláštní kriminalistické postupy.

Její speciální povaha vyvěrá zejména z požadavku na citlivý přístup orgánů činných v trestním řízení k obětem těchto trestných činů. Požadavek na ohleduplnost k dětským obětem se projevuje zejména při stěžejním okamžiku trestního řízení, kterým je výslech oběti. Vzhledem ke skutečnosti, že zásadním požadavkem na vedení trestního řízení je co největší minimalizace sekundární viktimizace dětské oběti, každé opakování výslechu v jednotlivých fázích trestního řízení či pouhé doplnění předchozího výslechu z důvodu zjištění nových skutečností je nežádoucí. Je tak zcela zásadní a klíčové, aby výslech oběti a vytěžení jejího nejbližšího okolí byly prováděny na základě předepsaných postupů speciálně vyškolenými pracovníky, a to tak, aby negativní efekt trestního řízení na oběť trestného činu byl co možná nejvíce redukován.

Kybergrooming, jakožto způsob navazování kontaktů s dětmi prostřednictvím kyberprostoru za účelem jejich sexuálního zneužití, je z hlediska požadavků na erudovanost orgánů činných v trestním řízení a na preciznost jejich postupu v rámci trestního řízení oblastí ještě problematičtější, a to vzhledem ke skutečnosti, že u kybergroomingu se specifika mravnostních trestných činů páchaných na dětech kombinují se specifiky kriminality páchané v kyberprostoru.

Kriminalita páchaná v kyberprostoru představuje v současné době jednu ze zásadních výzev kriminalistiky a forenzních věd, a to především vzhledem ke specifické povaze digitálních stop, které bývají zpravidla centrem dokazování těchto trestných činů, a ke zvláštnostem způsobů jejich zajišťování. K řádnému zajištění digitální stopy a k jejímu následnému vyhodnocení je potřeba nejen speciálně vyškolených pracovníků a zvláštních metodických postupů, ale rovněž moderního softwaru a technického vybavení. Stejně tak je zapotřebí specialistů s vysokou úrovní odbornosti v roli znalců oboru Informační a komunikační technologie. I přes relativně dobrou technickou i personální vybavenost specializovaných útvarů Policie České republiky je však kybernetická kriminalita z hlediska objasněnosti na samém chvostu statistických přehledů kriminality.

Ambicí tohoto článku je vytvoření metodiky vyšetřování kybergroomingu zahrnující veškeré složky kriminalistické metodiky, včetně kriminalistické charakteristiky, typických stop, podnětu i předmětu vyšetřování a přehledu jednotlivých úkonů činěných v rámci vyšetřování této trestné činnosti. Metodika si klade za cíl v dostatečné míře reflektovat duální povahu kybergroomingu, který si právě z důvodu tohoto svého specifika zaslouží vlastní přehled

kriminalistických metod a policejní praxe. Cílem autora tak není pouze akademicko-teoretický pohled na kriminalistickou praxi orgánů činných v trestním řízení, ale je jím rovněž snaha o vytvoření jakési praktické příručky pro správné pochopení a kriminalistické „uchopení" tohoto aktuálního a mimořádně společensky škodlivého fenoménu.

1. Kriminalistická charakteristika kybergroomingu

Pojmem **kybergrooming** rozumíme cílené navazování blízkého vztahu útočníka s obětí, kterou je zpravidla dítě, za účelem jejího pozdějšího sexuálního zneužití, přičemž k navazování a rozvíjení tohoto kontaktu dochází prostřednictvím kyberprostoru, převážně pak v prostředí sociálních sítí.

Útočník s dítětem navazuje přátelský až intimní vztah a v průběhu času posiluje v dítěti pocit důvěry. Chování útočníka má za cíl vyvolat v oběti falešnou důvěru a přimět ji k osobní schůzce.[2] Kontakt útočníka s dítětem může být udržován po dlouhou dobu, může trvat měsíce i roky, než útočník iniciuje osobní schůzku s dítětem. V některých případech komunikují útočníci s dítětem pod vlastní identitou, často však využívají identit fiktivních, a to k vlastní ochraně či k posílení důvěry dítěte. Mnohdy se vydává za osobu věkově blízkou své oběti, přičemž se při samotném osobním setkání může v takovém případech vydávat za rodiče svého mladšího alter-ega, který má setkání zprostředkovat a oběť k fiktivnímu „příteli z internetu" dopravit.[3] Útočníci s homosexuálními sklony se pak často vydávají za osoby opačného pohlaví.

Ve chvíli, kdy dítě odmítá vyhovět návrhům útočníka, které mohou zahrnovat on-line sexuální aktivity či osobní setkání, obvykle dochází k obratu ve způsobu komunikace.[4] Útočník poté dítě citově vydírá či mu dokonce vyhrožuje zneužitím informací, které mu dítě dříve poskytlo, zpravidla zveřejněním intimních fotografií a videí na veřejně přístupných sítích, jejich zasláním rodičům, kamarádům či škole. Vzhledem k blízkému vztahu útočníka a oběti však dostatečnou

[2] KOPECKÝ, K. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: Univerzita Palackého v Olomouci. 2015.

[3] Tamtéž s. 39

[4] Tamtéž s. 39.

hrozbou pro dítě může být již pohrůžka ukončením vzájemné komunikace útočníkem.[5]

Samotné osobní setkání útočníka s obětí je obvykle nejkritičtějším momentem celého procesu kybergroomingu. Zatímco v kyberprostoru je manipulace útočníka limitována specifiky zprostředkované komunikace a samotnou povahou kyberprostoru (v kyberprostoru se například do jisté míry stírá společenský statusový rozdíl mezi dospělou osobou a dítětem[6]), při bezprostředním kontaktu útočníka s dítětem bývá útočníkovo psychologické působení na dítě mnohem efektivnější. Při osobním setkání pak může útočník dítě pohlavně zneužít či využít k výrobě dětské pornografie.[7]

V roce 2011 byla přijata Směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV („směrnice 2011/93/EU“). Směrnice mimo jiné reagovala na rostoucí hrozbu kybergroomingu a v čl. 6 stanovila požadavek na zajištění trestnosti navazování kontaktu s dětmi k sexuálním účelům členskými státy.

Český zákonodárce reagoval na přijetí směrnice 2011/93/EU novelizací trestního zákoníku zákonem č. 141/2014 Sb. s účinností od 1. 8. 2014, kterou bylo do Hlavy III. zvláštní části trestního zákoníku vloženo nové ustanovení § 193b upravující skutkovou podstatu trestného činu navazování nedovolených kontaktů s dítětem.

Trestný čin navazování nedovolených kontaktů s dítětem je v českém právním řádu koncipován jako předčasně dokonaný trestný čin. Materiálně se jedná o přípravu k trestnému činu pohlavního zneužití, výroby a jiného nakládání s dětskou pornografií, zneužití dítěte k výrobě dětské pornografie, svádění k pohlavnímu styku a k jiným sexuálně motivovaným trestným činům. K jeho dokonání postačí již samotné pozvání dítěte na schůzku. Pro naplnění skutkové podstaty trestného činu navazování nedovolených kontaktů s dítětem tak není třeba dalších kroků ze strany útočníka, jak stanovuje evropská úprava. Úmysl pachatele však již v době pozvání musí směřovat ke

[5] KUDRLOVÁ, K. *Kriminalita spojená s využíváním nových médií dětmi*. Praha, 2019. Disertační práce. Katedra trestního práva. Právnická fakulta Univerzity Karlovy. Vedoucí práce doc. JUDr. Bc. Tomáš Gřivna, Ph.D. s. 141.

[6] KOPECKÝ, K. Rizikové formy chování českých a slovenských dětí v prostředí internetu. s. 24.

[7] VLACH, J., KUDRLOVÁ, K., PALOUŠOVÁ V. *Kyberkriminalita v kriminologické perspektivě*. Praha: Institut pro kriminologii a sociální prevenci, 2020.

spáchání sexuálně motivovaného trestného činu. Dítětem zákon v tomto ustanovení rozumí osobu mladší patnácti let věku. Navrhovatelem setkání přitom musí být sám pachatel, nikoliv dítě.

Trestný čin navazování nedovolených kontaktů s dítětem podle ustanovení § 193b trestního zákoníku nelze zcela ztotožňovat s kybergroomingem. Ve shodě s Krupičkou lze uvést, že tato skutková podstata kriminalizuje až závěrečnou fázi kybergroomingu, tedy samotný návrh osobní schůzky ve skutečném světě učiněný útočníkem.[8] Kybergrooming však může být trestný rovněž jako trestný čin výroby a jiného nakládání s dětskou pornografií podle § 192 trestního zákoníku, zneužití dítěte k výrobě pornografie podle § 193 trestního zákoníku či jako trestný čin sexuálního nátlaku podle § 186 trestního zákoníku, a to v závislosti na konkrétních skutkových okolnostech případu.[9] Komunikace s dítětem za účelem jeho pozdějšího znásilnění může být rovněž v závislosti na konkrétních skutkových okolnostech kvalifikována jako příprava zvlášť závažného zločinu znásilnění dle § 185 odst. 1, odst. 2 písm. b) ve spojení s § 20 odst. 1 trestního zákoníku v případě mladistvého, či § 185 odst. 1, odst. 3 písm. a) ve spojení s § 20 odst. 1 trestního zákoníku v případě dítěte mladšího patnácti let, i když doposud nemuselo dojít k nabídce osobní schůzky.

Ačkoliv psychologické působení na osobu za účelem jejího zneužití může být zaměřeno i na dospělé osoby a stále bude takové jednání spadat do definice kybergroomingu, tato metodika se těmito případy záměrně nezabývá. Hlavním důvodem je skutečnost, že nejde o typický způsob páchání kybergroomingu, a vyšetřování tak bude probíhat zásadním způsobem rozdílně. Tato metodika zároveň nebude podrobněji rozebírat postupy orgánů činných v trestním řízení v případě dokonaného znásilnění či pohlavního zneužití oběti na osobní schůzce oběti a útočníka, jelikož vyšetřování těchto skutečností je předmětem metodiky vyšetřování znásilnění či mravnostní kriminality v obecném slova smyslu.

[8] KRUPIČKA, J. Kybergrooming – zrcadlo společnosti? In: GŘIVNA, T., RICHTER, M., ŠIMÁNOVÁ, H. (eds.). *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022, s. 356.

[9] Tamtéž s. 357.

2. Typické stopy

Kriminalistickou stopou rozumíme každou změnu v materiálním prostředí či ve vědomí člověka, která je v příčinné nebo jiné souvislosti s kriminalisticky relevantní událostí, existuje nejméně od svého vzniku do zajištění a je vyhodnotitelná současnými kriminalistickými metodami a prostředky.[10]

Kriminalistické stopy tradičně dělíme na **stopy materiální** a **stopy paměťové**.[11] Zvláštním druhem kriminalistických stop, které nabývají na významu zejména v posledních desetiletích, jsou pak **stopy digitální**. Digitální stopy lze definovat jako jakákoliv data či informace přenesená, vytvořená, uložená či modifikovaná za použití počítačového systému.[12] Ačkoliv jsou digitální stopy některými autory řazeny mezi stopy materiální[13], svou nestálostí a dynamickou povahou se blíží stopám paměťovým, přičemž jejich nositelem je namísto paměti člověka paměťové médium počítačového systému či jiné technické zařízení, které je k ukládání informací tohoto typu určeno. Digitální stopy jsou ze své podstaty stopami latentními, ke zviditelnění kriminalisticky významných informací je tak třeba použít dodatečných technických prostředků a činností.[14] Problematickým aspektem zajišťování digitálních stop je rovněž skutečnost, že nelze předem zcela bezpečně určit, zda se na konkrétním nosiči informací či v počítačovém systému kriminalistické stopy nacházejí, respektive jaký je jejich rozsah.[15] Před zajištěním počítačového systému či nosiče informací je tak třeba udělat alespoň základní předběžnou analýzu za účelem zjištění, zda daný nosič kriminalisticky významné informace vůbec obsahuje.[16]

Z hlediska vyšetřování kybergroomingu budou v centru zájmu orgánů činných v trestním řízení zejména právě stopy digitální, jejichž nositeli budou zejména konverzace na sociálních sítích, uživatelské účty oběti i pachatele, e-mailové zprávy, chaty, fotografie v digitální

[10] MUSIL, J., KONRÁD, Z., SUCHÁNEK, J. *Kriminalistika. 2., přepracované a doplněné vydání*. Praha: C. H. Beck, 2004. s. 78.

[11] PORADA, V., STRAUS, J. *Kriminalistické stopy: teorie, metodologie, praxe*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012. s. 61.

[12] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s. 403.

[13] Tamtéž s. 404.

[14] STRAUS, J., PORADA, V. *Teorie, metody a metodologie kriminalistiky*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. s. 358.

[15] Tamtéž s. 358.

[16] Tamtéž s. 358.

podobě či videa. Digitálními stopami však budou také data o těchto datech (tzv. metadata), přihlašovací logy, záznamy o poloze zařízení, logy IP adres a jiné záznamy o provozu telekomunikačních zařízení.

Druhým stěžejním typem kriminalistických stop budou stopy paměťové, kterými rozumíme vzpomínky v paměti zainteresovaných osob. Těmito osobami mohou být kromě pachatele a oběti také jiné osoby, kterým se oběť svěřila, tedy například přátelé oběti, její rodiče či učitelé a vychovatelé.

Co se týče vzniku materiálních stop, tyto nabývají při vyšetřování kybergroomingu na významu v případě realizace osobního setkání pachatele a oběti. V případě dokonaného sexuálního zneužití či znásilnění oběti pak zajištění materiálních stop bude jedním z prvotních a nedokladných úkonů.

3. Zvláštnosti předmětu vyšetřování

Základní předmět vyšetřování je v obecné rovině dán ustanovením § 89 odst. 1 trestního řádu. Rozumíme jím odpovědi na otázky, zda se stal skutek, v němž je spatřován trestný čin a zda tento skutek spáchal obviněný, případně z jakých pohnutek. Dále jsou jím podstatné okolnosti mající vliv na posouzení povahy a závažnosti činu, podstatné okolnosti k posouzení osobních rodinných, majetkových a jiných poměrů obviněného a podstatné okolnosti umožňující stanovení následku, výše škody či bezdůvodného obohacení. V neposlední řadě jsou jím okolnosti, které vedly k trestné činnosti nebo které spáchání trestného činu umožnily.

Jednotlivé zvláštní aspekty předmětu vyšetřování kybergroomingu lze rozdělit do následujících kategorií:

1. informace o útoku;
2. informace o počítačovém systému;
3. informace o datech;
4. informace o pachateli;
5. případná mnohost útoků.[17]

Informacemi o útoku rozumíme informace o metodách a formě navazování kontaktů mezi pachatelem a dítětem, o samotné povaze útoku (tedy zda šlo pouze o komunikaci v rámci kyberprostoru, či zda došlo k osobnímu setkání, při kterém pachatel dítě přiměl k pohlavnímu

[17] Kategorizace zvláštních aspektů předmětu vyšetřování bude obdobná, jako je tomu v případě obecné kybernetické kriminality. Srov.: KOLOUCH, J. *CyberCrime*, s. 406 – 407.

styku či jej zneužil k výrobě pornografie), případně také o následku způsobeném jednáním pachatele. Vyšetřování se bude zaměřovat zejména na obsahovou stránku komunikace mezi pachatelem a obětí kybergroomingu. V případě vyšetřování kybergroomingu je třeba posuzovat povahu zvolených slovních formulací a sdělovaných skutečností, jelikož podle povahy a způsobu komunikace mezi pachatelem a obětí je posuzován úmysl pachatele přimět dítě k sexuálním praktikám a intenzita praktik, ke kterým útok směřoval.[18]

Pro naplnění znaků skutkové podstaty trestného činu navazování nedovolených kontaktů s dítětem je rovněž důležité posouzení, zda to byl právě pachatel, kdo případnou osobní schůzku mezi ním a dítětem inicioval.

Informacemi o počítačovém systému rozumíme především informaci o tom, z jakého koncového přípojného bodu telekomunikační sítě byl útok prováděn, tedy z jakého počítačového systému k útokům docházelo, prostřednictvím čehož je možné zjistit, kdo je uživatelem profilu na sociální síti, ze kterého byl útok prováděn. Předmětem vyšetřování tak bude zejména zjištění IP adresy, ze které se útočník ke svému profilu na sociální síti jako koncový uživatel připojoval.

Informacemi o datech rozumíme zejména informace o tom, zda nebylo s daty manipulováno, tedy zda nedošlo k pozměnění komunikace mezi pachatelem a obětí, či k úpravě případných fotografií či videí, které obsahují kriminalistické stopy. Orgány činné v trestním řízení musejí v rámci vyšetřování zkoumat, zda nebyla porušena integrita těch dat, která mohou sloužit jako důkaz v trestním řízení. U každé digitální stopy je nutné zkoumat její pravost. Jak zdůrazňuje Smejkal, u digitálních stop nelze bez dalšího presumovat, že jsou pravé, jen proto, že vzešly z počítače.[19] Pravost informací získaných z digitálních stop je tak třeba v průběhu řízení ověřovat.

Co se týče **osoby pachatele**, stěžejním dílčím předmětem vyšetřování bude prokázání skutečnosti, zda pachatel věděl, že jeho jednání směřuje vůči dítěti mladšímu věku patnácti let. Dovodit skutečnost, že pachatel věděl, že se jedná o osobu mladší patnácti let, lze prostřednictvím analýzy komunikace s obětí, kdy oběť běžně útočníkovi svůj věk sama sdělí. Skutečnost, že pachatel musel znát

[18] Usnesení Nejvyššího soudu ze dne 25.11.2020 sp. zn. 8 Tdo 1041/2020.

[19] SMEJKAL, V. *Kybernetická kriminalita. 2. rozšířené a aktualizované vydání*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. s. 714.

informaci o věku oběti lze však také prokázat již ze samotného profilu oběti, kde je věk uživatele zpravidla uveden.[20]

Předmětem vyšetřování bude rovněž tzv. druhý úmysl pachatele, tedy úmysl směřující ke spáchání jiného sexuálně motivovaného trestného činu. V tomto ohledu je klíčové posouzení povahy sexuálně motivovaných narážek, které jsou součástí komunikace mezi pachatelem a obětí kybergroomingu.[21] Pro prokázání zavinění, které je v případě trestného činu navazování nedovolených kontaktů s dítětem vyžadováno ve formě úmyslu, je nutné analyzovat obsahovou stránku komunikace mezi pachatelem a obětí kybergroomingu, přičemž v tomto ohledu bude zásadní povaha sexuálně motivovaných narážek. Dále je třeba posoudit, jaká je role pachatele v rámci sexuálně laděné komunikace, zda je v této komunikaci dominantním prvkem, či zda je prvkem pasivním.

K osobě pachatele je v rámci vyšetřování třeba dále zkoumat, zda se jednalo o osobu se sexuální deviací, či zda se jednalo o sexuálně zdravou. Je nutné zdůraznit, že pro naplnění skutkové podstaty trestného činu navazování nedovolených kontaktů s dítětem není zapotřebí, aby pachatel byl osobou s pedofilní, hebefilní, efebofilní[22] či jinou sexuální deviací. Zkoumání duševního stavu útočníka, zejména za účelem zjištění jeho případných sexuálních odchylek a preferencí, má význam především co do určení druhu a výše trestu, případně pro účely posouzení, zda je v daném případě namístě uložení ochranného opatření. Posouzení sexuální deviace a jejího vlivu na jednání pachatele je rovněž zásadní pro určení, zda v daném případě nebyly vymizelé ovládací a rozpoznávací schopnosti pachatele, tedy zda byla osoba v době spáchání trestného činu příčetná, či zda nedošlo v důsledku sexuální deviace alespoň k jejich podstatnému snížení, tedy zda se v tomto případě nejednalo o zmenšenou příčetnost ve smyslu ustanovení § 27 trestního zákoníku. Zodpovězení těchto otázek bude předmětem vyšetření duševního stavu obviněného znalcem z oboru sexuologie ve smyslu ustanovení § 116 trestního řádu.

Co se týče šetření k **mnohosti útoků** kybergroomera, jediný útočník bude obvykle komunikovat s větším počtem potenciálních obětí, aby zvýšil svou šanci na úspěšné vylákání pornografického obsahu či na

[20] Prokázat útočníkovu znalost věku oběti lze například také tehdy, když útočník na facebookovém profilu oběti dá *„to se mi líbí“* u narozeninové fotografie, u které je uveden věk oslavence.

[21] Usnesení Nejvyššího soudu ze dne 25.11.2020 sp. zn. 8 Tdo 1041/2020. Bod 51.

[22] Hebefilií rozumíme sexuální deviaci spočívající v sexuální náklonnosti vůči dospívajícím dívkám, efebofilií naopak rozumíme sexuální náklonnost vůči dospívajícím chlapcům.

zneužití dítěte. Nebývá výjimkou, že jeden útočník zakládá více profilů pod různými identitami, a to i v rámci jediné sociální sítě či seznamky. V rámci vyšetřování je tak zapotřebí provázat jednotlivé účty a *aliasy* založené a využívané jediným útočníkem s touto konkrétní osobou, resp. zpravidla také s jedním počítačovým systémem, ze kterého útoky činěné prostřednictvím většího počtu účtů směřovaly, a to prostřednictvím identifikace shodných markantů technického (IP adresy) i netechnického (jméno, přezdívka, modus operandi) charakteru.

4. Zvláštnosti podnětů vyšetřování

Kybergrooming probíhá většinou skrytě a bez vědomí orgánů činných v trestním řízení, stejně tak bez vědomí rodičů, učitelů a dalších dospělých osob, které by bylo možné z hlediska kriminologie označit za tzv. schopné strážce[23]. Tam, kde by v případě groomingu ve skutečném světě pachateli hrozilo odhalení již samotnou přítomností jiných dospělých osob (např. na dětských hřištích, v okolí škol, ale rovněž také na dětských táborech či v zájmových kroužcích), se v případě kybergroomingu může útočník skrýt pod anonymním pláštěm kyberprostoru. Ze samotné anonymní povahy kyberprostoru a z jeho domnělé oddělenosti od skutečného světa vyplývá jeden ze zásadních kriminologických aspektů kybergroomingu, kterým je jeho relativně vysoká latence.

Oproti jiným typům kybernetické kriminality vysokou latentnost tohoto fenoménu podporuje rovněž skutečnost, že se dětské oběti kybergroomingu bojí rodičům či jiným dospělým osobám sdělit, že se stalo obětí internetového útočníka. Dětské oběti kybergroomingu, obzvláště ty mladší, se zpravidla domnívají, že ony samy se dopustily něčeho zakázaného a že budou potrestány, a to například rodičovským zákazem nebo omezením užívání internetu či sociálních sítí. Z těchto důvodů bývá samo dítě oznamovatelem jen v ojedinělých případech. Trestní oznámení zpravidla podává rodič dítěte, pedagog či jiná dospělá osoba. Pokud dochází k oznámení samotným dítětem, takové oznámení bývá učiněno na popud právě těchto osob. Z toho může vyplývat

[23] Z anglického termínu „capable guardians“. Jedná se o osoby, které svou pouhou přítomností odrazují potenciální útočníky od spáchání trestného činu. Jde o součást teorie rutinní činnosti Cohena a Felsona, srov.: COHEN, L. E., FELSON, M. *Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review* [online]. 1979, 44 (4) [cit. 2023-04-15]. Dostupné z: doi:10.2307/2094589.

prvotní neochota či zdrženlivost oběti kybergroomingu spolupracovat s orgány činnými v trestním řízení na odhalení a dopadení pachatele. V tomto ohledu je nutné si uvědomit, že oběť kybergroomingu nemusí pociťovat zájem rodičů a okolí (potažmo zájem orgánů činných v trestním řízení) na vyšetření věci a na dopadení a potrestání pachatele jako zájem vlastní. Jak již bylo výše uvedeno, kybergrooming spočívá v navázání přátelského až intimního vztahu s dítětem, který nemusí být následným sexuálně motivovaným nátlakem na dítě zcela přetrhán. Motivací dítěte nespolupracovat s policií tak může kromě studu a strachu z potrestání jeho samotného pramenit rovněž ze snahy útočníkovi pomoci.

Při absenci osob, které by kybergrooming oznamovaly, se nabízí řešení v podobě vyhledávání trestné činnosti samotnými orgány činnými v trestním řízení, tedy zjišťování informací o trestných činech na základě vlastní operativně pátrací činnosti útvarů Policie České republiky. V kontextu nedávných projektů, které měly za cíl informovat veřejnost o hrozbách internetového predátorství za pomocí vytvoření falešných profilů dětí, jakými byly dokumentární film autorů Víta Klusáka a Barbory Chalupové s názvem *V Síti* či pořad *Černota* internetové televize *stream.cz*, by bylo možné uvažovat o vyhledávání a „chytání" kybergroomerů za pomoci falešných dětských profilů vytvářených a spravovaných přímo příslušníky Policie České republiky. Dle Krupičky však takové postupy mohou hraničit s řízenou policejní provokací a jsou nepřípustné bez podezření na konkrétní osobu.[24] Dle názoru autora článku však může být případná institucionalizace vyhledávání profilů kybergroomerů „policejními agenty" při současném šetření ústavně zaručených práv a svobod dotčených osob v souladu s principy českého trestního práva procesního a mohlo by jít o vhodný návrh *de lege ferenda*.[25]

Orgány činné v trestním řízení se o existenci profilů útočníků na sociálních sítích a o dalším závadném obsahu spojeném se zneužíváním dětí včetně dětské pornografie dozvídají rovněž prostřednictvím tzv. **reportů** v rámci projektu *CyberTipline* americké neziskové organizace

[24] KRUPIČKA, J. Kybergrooming – zrcadlo společnosti?, s. 352.

[25] Příkladem ze zahraničí může být operativně pátrací činnost britské policie v kyberprostoru, tzv. **covert sting operations**, kdy policie právě na výše uvedeném principu „loví" kybergroomery. Tato činnost má přísně stanovené mantinely, kdy nesmí ze strany policejního orgánu docházet k žádné formě iniciace komunikace s útočníkem, policejní orgán musí být v této komunikaci zdrženlivý a nesmí sám iniciovat osobní schůzku. Zdroj: Online grooming and UK law. Childnet International [online]. [cit. 2023-04-17]. Dostupné z: https://www.childnet.com/wp-content/uploads/2014/08/online-grooming.pdf.

National Center for Missing & Exploited Children („NCMEC“). Provozovatelé sociálních sítí a dalších internetových služeb poskytují společnosti NCMEC informace o závadném obsahu, který na svých sítích detekují. Na základě těchto dat jsou vypracovávány reporty, které jsou prostřednictvím institucí mezinárodní justiční a policejní spolupráce přeposílány orgánům činným v trestním řízení států, na jejichž území se útočník dle zjištěné IP adresy nachází.[26] Tyto reporty jsou v případě České republiky zasílané prostřednictvím EUROPOLu Úřadu Služby kriminální policie a vyšetřování Policejního prezidia Policie České republiky. Obsahem těchto reportů jsou především soubory či záznamy komunikace, které byly vyhodnoceny jako závadné, společně s časovými značkami, údaji o profilu útočníka, IP adresami jednotlivých přihlášení, časů podezřelých aktivit a dalších informací, na základě kterých lze provést jednoznačnou identifikaci zařízení, ze kterého byl útok proveden, potažmo i samotného pachatele.[27]

Vyloučeno není ani oznámení učiněné právnickou osobou, zpravidla bude takovou osobou provozovatel sociálních sítí či jiných služeb v rámci kyberprostoru, či ISP[28]. Oznamovatelem může být v případě kybergroomingu rovněž škola či jiná výchovně vzdělávací instituce, podobně jako je tomu rovněž u jiných druhů mravnostní kriminality páchané na dětech.[29]

5. Typické vyšetřovací situace

Vyšetřovací situací rozumíme stav, v němž se nalézá vyšetřování v určitém momentu, v němž se rozhoduje o dalším postupu ve vyšetřování.[30] Tento stav je determinován mnoha proměnnými, z nichž je z hlediska typizace vyšetřovacích situací nejpodstatnější **stupeň informační určitosti**, tedy kvalita a kvantita informací, které jsou

[26] CyberTipline Reports [online]. NCMEC [cit. 2023-04-15]. Dostupné z: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata#reports.

[27] Některé případy dopadení pachatele na základě mezinárodní spolupráce s NCMEC byly v České republice medializovány. Příkladem je případ zneužívání sedmileté dívky otcem, který si styk nahrával na mobilní telefon. Zdroj: Muž měl zneužívat malou holčičku. Policie ČR [online]. [cit. 2023-04-15]. Dostupné z: https://www.policie.cz/clanek/muz-mel-zneuzivat-malou-holcicku.aspx.

[28] *Internet service provider* (zkr.), v překladu (z angl.) poskytovatel internetového připojení.

[29] CHMELÍK, J. *Rukověť kriminalistiky*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. s. 339.

[30] PORADA, V. Kriminalistické stopy: teorie, metodologie, praxe, s. 838.

obsahem souboru poznatků o trestném činu a o jeho pachateli, jež má v daný moment orgán činný v trestním řízení k dispozici.[31] Dalšími faktory mohou být podmínky materiální, organizační i personální, které se budou lišit například podle materiální vybavenosti vyšetřujícího útvaru, podle osobnosti vyšetřovatele, jakož i podle okolností, jenž ze strany orgánu činného v trestním řízení ovlivnit nelze, jako je počasí či politicko-společenská situace. Vyšetřovací situaci v případě kybergroomingu ovlivňuje také úroveň rizikového chování dětí na internetu či celková kybernetická gramotnost ve společnosti.[32] Aktuální vyšetřovací situace determinuje, jaké vyšetřovací verze budou vytyčeny, které úkony budou provedeny jako prvotní a jak bude probíhat následná etapa vyšetřování.

Typickou počáteční vyšetřovací situací v případě kybergroomingu bude situace, v níž orgány činné v trestním řízení zjistí skutečnosti nasvědčující tomu, že se stal skutek, v němž je spatřován trestný čin, v hrubých rysech pak mohou znát i skutečnosti objasňující způsob spáchání předmětného trestného činu, které mohou být obsahem již samotného trestního oznámení, přijatého reportu NCMEC či oznámení jiného subjektu.

Počáteční vyšetřovací situace kybergroomingu se pak budou lišit podle toho, zda již od počátku vyšetřování známe totožnost útočníka (jinými slovy zda vystupuje pod svým skutečným jménem – v ideálním případě se současným uvedením datumu narození), či zda vystupuje toliko pod přezdívkou či zda používá falešnou identitu.[33] Ztotožnění útočníka podle informací vyplývajících z profilu na sociálních sítích je možné na základě jednoduché prověrky učinit také v případech, kdy není uvedeno přímo jeho jméno a datum narození, ale je uvedena jeho e-mailová adresa či telefonní číslo.[34]

---

[31] Tamtéž, s. 838.

[32] HEJDUK, M. Kriminalistické aspekty odhalování, prověřování a vyšetřování počítačové mravnostní kriminality. *Bezpečnostní teorie a praxe*. Praha: Policejní akademie. 2021 (1). [cit. 2023-04-15]. Dostupné z: https://veda.polac.cz/wp-content/uploads/2021/04/Kriminalisticke-aspekty-odhalovani-proverovani-a-vysetrovani-pocitacove-mravnostni-kriminality.pdf. s.71.

[33] Srov. typické počáteční situace v případě obecné kybernetické kriminality: PORADA, V. Kriminalistické stopy: teorie, metodologie, praxe, s. 967 – 969.

[34] A to prověrkou uvedených údajů v policejních informačních systémech jako jsou IS Telefony či Centrální databáze objektů, ve které můžeme rovněž zjistit případné provázání s jinými již dříve šetřenými incidenty.

6. Typické vyšetřovací verze

Vyšetřovacími verzemi v kriminalistice rozumíme jeden z druhů tzv. kriminalistických verzí, mezi které dále řadíme operativně-pátrací verze a soudní verze.[35] Kriminalistickými verzemi rozumíme metodu kriminalistické praxe spočívající ve vyvození a prověrce všech dosud opodstatněných domněnek o příčinách a formách spojení všech jevů kriminalisticky významné události jako reálně možných objasnění doposud zjištěných skutečností. Cílem kriminalistických verzí je prověrka doposud zjištěných skutečností a získání znalosti o nových skutečnostech, přičemž kriminalistické verze jsou potřebné pro zaměření dalšího průběhu vyšetřování.[36]

V případě trestněprávního postihu kybergroomingu je středobodem vyšetřování objasnění skutečností prokazujících či vyvracejících naplnění znaku subjektivní stránky trestného činu ve formě úmyslu. Vytyčené vyšetřovací verze se tak budou alespoň zpočátku primárně zaobírat existencí či neexistencí úmyslu pachatele dítě prostřednictvím kybergroomingu zneužít. Typické vyšetřovací verze mohou být v případě, že je skutek kvalifikován jako navazování nedovolených kontaktů s dítětem podle ustanovení § 193b trestního zákoníku, s ohledem na výše uvedené vytyčeny takto:

1. osoba vylákala dítě k osobní schůzce s úmyslem jejího pozdějšího sexuálního zneužití či výroby pornografického materiálu, přičemž věděla, že se jedná o dítě ve věku mladším patnácti let;
2. osoba nabídla dítěti osobní schůzku bez úmyslu jejího pozdějšího sexuálního zneužití či výroby pornografického materiálu;
3. osoba nabídla dítěti osobní schůzku za účelem sexu či výroby pornografického materiálu, avšak zároveň se domnívala, že se jedná o osobu starší patnácti let.

7. Specifika počátečních úkonů

Bezprostředně poté, co se orgán činný v trestním řízení dozví o skutečnostech důvodně nasvědčujících tomu, že došlo ke spáchání trestného činu, je zapotřebí učinit neodkladné úkony, kterými se rozumí

[35] KONRÁD, Z., PORADA, V., STRAUS, J., SUCHÁNEK, J. Kriminalistika: kriminalistická taktika a metodiky vyšetřování. 2. rozšířené vydání, s. 21.

[36] Tamtéž, s. 20.

ty úkony, jejichž včasné neprovedení by mohlo zmařit účel trestního řízení.

V případě kybergroomingu se u vymezení počátečních úkonů projevuje zejména jeho kybernetická podstata, proto bude v plánu vyšetřování předním příčkám vévodit zajištění kriminalisticky relevantních dat, primárně tedy zajištění komunikace mezi pachatelem a obětí. Zásadní je rovněž zjištění IP adresy počítačového systému, ze kterého se útočník ke svému profilu přihlašoval, a to včetně data a času připojení prostřednictvím této adresy k dané sítí.

Klíčové je v tomto ohledu včasné zajištění **přihlašovacích logů** k účtu útočníka obsahujících IP adresy, které si lze vyžádat od provozovatele dané sociální sítě či jiné služby. Za součinnosti s poskytovateli internetového připojení (ISP), kteří po dobu šesti měsíců uchovávají informace o počítačových systémech včetně IP adres, času a délky používané služby, lze pak pomocí přihlašovacích logů k danému účtu určit koncový přípojný bod, tedy počítačový systém, ze kterého byl útok veden.[37]

Počátečním úkonem ve věci je rovněž **ohledání uživatelského účtu útočníka a uživatelského účtu oběti** na předmětné sociální síti či jiné službě. Ohledání uživatelského účtu orgány činíme za účelem prvotního zajištění kriminalistických stop nacházejících se přímo na profilu uživatele sociální sítě či jiné služby, než dojde ke zmrazení a poskytnutí těchto dat provozovatelem služby. Vyšetřovatel pořizuje prostřednictvím printscreenů obrazovky záznamy o veřejně dostupných informacích k předmětnému účtu, kterými mohou být jméno či *nick* účtu, přiložená fotografie, seznam přátel, zveřejněné statusy, webovou adresu účtu a další data. Součástí ohledání by mělo být zajištění tzv. **jednoznačného identifikátoru účtu**, tedy unikátního nezměnitelného kódu účtu, který každý jednotlivý účet v rámci předmětné sítě odlišuje od ostatních účtů, přičemž se takový kód nemění nehledě na případné změny jména, nicku, profilové fotografie či dalších údajů. Ohledání uživatelského účtu se řídí ustanovením § 113 trestního řádu a je třeba o něm vyhotovit protokol. Stejným způsobem lze učinit prvotní ohledání komunikace mezi útočníkem a dítětem při přijetí trestního oznámení.

Pro řádné zajištění komunikace mezi pachatelem a obětí je však třeba co nejrychleji zajistit data nacházející se na serverech třetích osob, zpravidla provozovatelů sociálních sítí a dalších internetových služeb,

[37] HEJDUK, M. Kriminalistické aspekty odhalování, prověřování a vyšetřování počítačové mravnostní kriminality, s. 73 – 74.

a to tak, aby nedošlo k jejich odstranění či pozměnění útočníkem v důsledku jeho obavy z trestního stíhání. Z důvodu požadavku na zachování dat v nezměněné podobě před jejich zajištěním je třeba využít institutu příkazu k uchování dat, tzv. **data freezing** či **data preservation**, ve smyslu ustanovení § 7b odst. 1 trestního řádu. V případě žádosti českých orgánů činných v trestním řízení o uchování dat nacházejících se v datových centrech umístěných na území jiných států, což se týká většiny „velkých" provozovatelů internetových služeb, lze pak postupovat urychleně dle ustanovení § 65a odst. 1 zákona č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, ve znění pozdějších předpisů, u něhož dochází k žádost o uchování dat českými orgány cestou přímé komunikace mezi Národní centrálou proti terorismu, extremismu a kybernetické kriminalitě Policie České republiky, která pro Českou republiku plní funkci kontaktního místa podle mezinárodní smlouvy, a příslušným zahraničním útvarem.

Takto uchovaná data si posléze orgán činný v trestním řízení vyžádá od provozovatelů služeb prostřednictvím příslušných zajišťovacích institutů trestního práva procesního, a to s ohledem na povahu zajišťovaných dat buď prostřednictvím ustanovení § 158d odst. 3 trestního řádu v případě, že se jedná o samotnou obsahovou stránku komunikace, nebo prostřednictvím postupu dle ustanovení § 88a trestního řádu pro případ, že se jedná o údaje o telekomunikačním provozu.

V případě, že je již od počátku známa osoba, která útoky prováděla, resp. je znám počítačový systém, z nějž byly útoky prováděny, je zapotřebí neodkladně provést **ohledání místa činu**, respektive **domovní prohlídku** případně **prohlídku prostor nesloužících k bydlení**[38] a zajistit veškeré nalezené hmotné nosiče dat a samotný počítačový systém, ze kterého byly útoky prováděny, a provést jejich ohledání. Při těchto úkonech by měla být zajištěna přítomnost experta z oboru výpočetní techniky, který navrhuje rozsah zajištění pro potřeby počítačové expertízy a zajišťuje podrobné zadokumentování situace, zejména stavu techniky v době zahájení úkonu, dále informace o tom, zda je či není technika v provozu a zda je připojena k síti elektronické komunikace.[39] V případě přítomnosti většího počtu počítačových

[38] Případně **osobní prohlídku** za účelem zajištění mobilního telefonu či jiného přenosného zařízení či nosiče, kterou má osoba u sebe.

[39] KONRÁD, Z., PORADA, V., STRAUS, J., SUCHÁNEK, J. Kriminalistika: kriminalistická taktika a metodiky vyšetřování. 2. rozšířené vydání, s. 348 – 349.

systémů je třeba se soustředit rovněž na připojení jednotlivých počítačových systémů k internetové síti, a to co do zjištění způsobu připojení u jednotlivých systémů a co do identifikace jednotlivých ISP poskytujících připojení, případně je třeba určit a zaznamenat topologii lokální sítě a propojení počítačových systémů mezi sebou (např. v případě vedení útoků skrze firemní počítač).[40]

8. Specifika následných úkonů

Klíčovým momentem celého vyšetřování je **výslech oběti trestného činu – dítěte**. V tomto bodě vyšetřování se nejintenzivněji projeví povaha kybergroomingu jakožto trestného činu mravnostního, z čehož vyplývá požadavek na vysoce profesionální práci s obětí, a to z důvodu obzvláště vysokého rizika její sekundární viktimizace.

Výslech dítěte jakožto oběti trestného činu by měla vždy vykonávat osoba, která je v této oblasti vyškoleným specialistou. Výjimkou mohou být situace, kdy nelze takovou osobu zajistit a kdy by pozdější provedení úkonu mohlo zmařit účel trestního řízení. I v takovém případě je však vždy třeba dbát o to, aby nebylo dítě výslechem traumatizováno a aby bylo co nejvíce redukováno riziko vzniku sekundární viktimizace dítěte. Je-li to pro dítě výhodné, měl by být výslech dítěte prováděn ve speciální výslechové místnosti.[41]

Klást otázky dítěti jinými osobami je v souladu s ustanovením § 102 odst. 3 trestního řádu možné pouze prostřednictvím vyslýchajícího. Vzhledem k povaze kybergroomingu pak bude u výslechu dětí mladších patnácti let obvykle přítomen orgán sociálně-právní ochrany dětí nebo osoba mající zkušenosti s výchovou mládeže. Vhodná je rovněž přítomnost dětského psychologa. Rovněž lze zmínit, že výslech dětí mladších patnácti let by měl být prováděn v dopoledních hodinách.

Specifický přístup k dětské oběti mravnostního trestného činu by se měl projevovat ve všech stadiích výslechu. Již před začátkem

[40] KOLOUCH, J. CyberCrime, s. 427 – 428.

[41] Speciální výslechová místnost je přizpůsobena dětem tak, aby co možná nejvíce navozovala pocit bezpečí a pohody. Nezbytnou součástí vybavení jsou demonstrační pomůcky – panenky **Jája, Pája, maminka, tatínek, babička a děda**, na kterých dítě může popsat zneužití méně traumatizujícím způsobem. Zdroj: Standard vybavení speciální výslechové místnosti pro dětského účastníka trestního řízení [online]. Policie ČR [cit. 2023-04-17]. Dostupné z: https://www.mvcr.cz/clanek/standard-vybaveni-specialni-vyslechove-mistnosti-pro-detskeho-ucastnika-trestniho-rizeni.aspx.

samotného výslechu je důležité vhodným způsobem navázat kontakt s dítětem, při kterém je zásadní získat jeho důvěru.[42]

V úvodní fázi výslechu je třeba dítě poučit, a to přiměřeně jeho věku. Účelem poučení dítěte není pouze dodržení zákonných požadavků výslechu a šetření práv vyslýchané osoby, ale také seznámení dítěte s tím, co se konkrétně bude dít a jak bude rozhovor probíhat, čímž by měla vyslýchající osoba dítě do jisté míry uklidnit.

Je třeba zdůraznit, že traumatizující povaha kybergroomingu může mít významný vliv na kvalitu výpovědi dítěte, které se stalo obětí tohoto typu jednání. Dle Čírtkové mohou výpověď dítěte, které se stalo obětí mravnostní kriminality, negativně ovlivňovat některé obranné mechanismy jeho psychiky, jako je:

- *vytěsnění* – určité traumatizující komponenty děje mohou být vytěsněny, jelikož vzpomínky na tyto děje mohou psychiku dítěte silně destabilizovat;
- *popření* – dítě se brání akceptovat realitu tím, že ji zcela popře;
- *disociace* – vzpomínky na traumatizaci nejsou integrovány do celkového vnitřní života oběti, ač nejsou vytěsněny (v mysli dítěte dochází k odštěpení „dobré stránky“ a „zlé stránky“ pachatele, jako by šlo o dvě odlišné osoby);
- *idealizace – devalvace* – možná je také idealizace pachatele dítětem jdoucí ruku v ruce s devalvací sebe sama či svého okolí (například rodičů), a to za účelem iluzorního vyhnutí se konfliktu s blízkou osobou, kterou pro dítě kybergroomer představuje;
- *identifikace s agresorem* – je rovněž možná vnitřní akceptace pachatele dítětem a jeho identifikace s ním.[43]

Znalost uvedených obranných mechanismů ega dítěte, a to za současné schopnosti identifikovat vzpomínkové mezery v paměti vyslýchaného, je klíčová pro korektní vedení výslechu ze strany orgánu činného v trestním řízení i pro posuzování věrohodnosti výpovědi dítěte – oběti.[44] Vyslýchající musí počítat rovněž se zvýšenou sugestibilitou dítěte, tedy větší náchylností dítěte „vyhovět“ vyslýchajícímu kladnými odpověďmi na otázky.

Významným následným úkonem vyšetřování je analýza zajištěných digitálních stop, jež mohou být nositeli důkazů v trestním řízení, které se provádí za pomocí znaleckého zkoumání stop – **digitální forenzní**

[42] ČÍRTKOVÁ, L. *Forenzní psychologie. 3., upr. vyd*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. s. 179.

[43] Tamtéž, s. 178 – 179.

[44] ČÍRTKOVÁ, L. Forenzní psychologie. 3., upr. vyd., s. 179.

analýzy. Pro práci s digitálními stopami je klíčové, aby bylo v okamžiku jejich použití jako důkazu možné prokázat, že v průběhu řízení nedošlo k jejich modifikaci. Základní zásadou zajišťování digitálních stop je proto **zásada zachování integrity digitální stopy**. Při práci s digitálními stopami, od jejich zajištění, přes jejich analýzu až do ukončení znaleckého zkoumání a následné předložení stopy jako důkazu před soudem, je třeba dodržovat určité principy, které k naplnění této zásady vedou.[45] Předně je třeba pracovat – pokud je to v dané situaci možné – s tzv. **duplikátem digitální stopy**, kterým se rozumí přesná bitová kopie datového nosiče, tedy přesná digitální reprodukce všech datových objektů obsažených na originálním fyzickém nosiči dat přenesená na nosič dat stejného typu. Oproti tomu běžná **kopie digitální stopy**, u které nedochází k přenosu dat na stejný typ média, nemusí obsahovat veškeré informace originálního nosiče, její průkazní a technická hodnota tak bude nižší.[46] S pouhou kopií dat se budeme muset spokojit v případě, že nemáme přístup k fyzickému nosiči. Pro zajištění integrity digitální stopy je třeba dále provést autentizaci duplikátu digitální stopy prostřednictvím kontrolního součtu, tzv. ***hashe***.[47] Ověřování *hashe* by mělo být prováděno průběžně, a to zejména, pokud nedochází k analýze dat bezprostředně po jejich zajištění.[48]

Smejkal k tomuto uvádí, že pořízení bitových kopií a jejich následné *hashování* přichází v úvahu v případě analýzy „neživých" zařízení, kterými se rozumí statické datové nosiče. V současné době se však stále častěji objevuje potřeba zajišťovat tzv. dynamická paměťová zařízení, u kterých by odpojení či vypnutí mohlo vést k nenávratné ztrátě relevantních dat, nebo takové odpojení není vzhledem k povaze systému vůbec možné. Při zajišťování dat z těchto systémů pak nutně dochází k určitému zásahu do samotného předmětu zkoumání, vzhledem ke skutečnosti, že pro uchování dat či pro analýzu běžícího systému je třeba spustit program, který do integrity datového nosiče či systému vždy do jisté míry zasáhne, jinými slovy provede změnu

[45] SMEJKAL, V. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání, s. 700.

[46] PORADA, V. *Dokazování obsahu elektronických dokumentů*. Košická bezpečnostná revue. Košice, 2012, 2012 (2), 104 - 108. s. 105.

[47] Jedná se o proces, při kterém je soubor dat převeden na základě určité matematické funkce do relativně malého čísla, přičemž opětovným použitím stejného algoritmu lze porovnáním výsledných čísel zjistit, zda došlo ke změně v původním souboru dat.

[48] AMIRIDU, R. *Zajištění integrity elektronického důkazu*. Brno, 2021. Diplomová práce. Masarykova Univerzita. Vedoucí práce JUDr. Mgr. Jakub Harašta, Ph.D.

v takovém systému.[49] Zajišťování a vyhodnocování stop v dynamickém prostředí se označuje jako ***Live Forensics***, resp. ***Live Data Acquistition***.[50] Integrita digitálních stop tak v těchto případech nemůže být zajištěna zcela do důsledku.

Obsahem samotné digitální forenzní analýzy jsou aktivity směřující k analýze všech procesů, které vznikly v průběhu kriminalisticky relevantní události, a to tak, aby mohlo být na základě výsledků analýzy zodpovězeno na základní kriminalistické otázky **Kdo? Co? Kde? Kdy? Jak? Proč?**. Výsledkem digitální forenzní analýzy je pak znalecký posudek. [51]

Významným následným úkonem vyšetřování kybergroomingu je, jak již bylo uvedeno dříve, **znalecké zkoumání duševního stavu útočníka**, a to především co do potvrzení či vyvrácení hypotézy o sexuální deviaci pachatele a jejím případném vlivu na spáchání trestného činu. Ustanovení § 116 odst. 1 trestního řádu stanovuje požadavek, aby k vyšetření duševního stavu obviněného byl přibrán znalec z oboru psychiatrie. Přibrání jediného znalce v oboru sexuologie bude v takovém případě vzhledem k požadavku vyjádřeném ustanovením § 116 odst. 1 trestního řádu možné toliko v případě, že se bude zároveň jednat o znalce se specializací v oboru psychiatrie, v jiném případě bude ke znalci v oboru sexuologie nutné přibrat znalce v oboru psychiatrie.[52]

Samotné sexuologické vyšetření zahrnuje anamnestické vyšetření pachatele, zpracování informací ze spisu a *penilní pletysmografii* („PPG“).[53] Při PPG vyšetření se u vyšetřované osoby za pomoci falometru (jinak také pletysmografu) měří prokrvení penisu či pochvy či jiné fyziologické odezvy při promítání obrázků sexuálně deviantní i nedeviantní povahy. Dle Procházky pak zpravidla znalec dospěje k jednomu ze tří typů forenzně sexuologických závěrů:

[49] SMEJKAL, V. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání, s. 699.

[50] K rozdílnosti zajišťování kopií „živých“ a „neživých“ zařízení viz KOLHE, M, AHIRAO, P. Live Vs Dead Computer Forensic Image Acquisition. *International Journal of Computer Science and Information Technologies*. 2017, 8 (3), s. 455-457.

[51] PORADA, V. Kriminalistika: technické, forenzní a kybernetické aspekty. 2. aktualizované a rozšířené vydání, s. 720.

[52] ŠÁMAL, P. § 116 [Vyšetření obviněného]. In: ŠÁMAL, P. *Trestní řád: komentář. 7., dopl. a přeprac. vyd*. V Praze: C.H. Beck, 2013. Velké komentáře. s. 1648–1649.

[53] PROCHÁZKA, L. Poznámky z oboru soudní sexuologie. Česká a slovenská psychiatrie [online]. [cit. 2023-04-18]. Dostupné z: http://www.cspsychiatr.cz/detail.php?stat=35.

1. v případě, že se pachatel dopustil předmětné trestné činnosti, potom – s ohledem na další zjištěné odborně relevantní informace – je postižen poruchou sexuální preference;
2. pachatel je nepochybně postižen poruchou sexuální preference, bez ohledu na to, zda mu bude či nebude předmětné sexuálně motivované jednání prokázáno;
3. pachatel nepochybně není postižen poruchou sexuální preference, bez ohledu na to, zda mu bude či nebude předmětné sexuálně motivované jednání prokázáno.[54]

Při zkoumání přítomnosti ovládacích schopností pachatele v době činu, resp. jejich případného zmenšení, bude sexuologické zkoumání zaměřeno zejména na:

1. intenzitu pohlavní aktivity a pohlavního pudu pachatele;
2. rozsah a sílu jeho psychických zábran;
3. schopnost adaptace na společensky přijatelné formy sexuálního chování.[55]

9. Zapojení veřejnosti do vyšetřování a prevence

Vzhledem k vysoce latentní povaze kybergroomingu je pro účinnou ochranu společnosti před tímto společensky škodlivým jevem zásadní nejen to, aby rodiče, školy i orgány veřejné moci včasně a správně reagovaly na již proběhlý útok, ale klíčová je především jejich snaha o účinnou prevenci. Drtivá většina rizikových komunikací mezi potenciálními pachateli a potenciálními oběťmi kybergroomingu totiž zůstane při sebevětší snaze jejich zraku ukryta. Cestou, jejímž prostřednictvím lze s tímto stavem bojovat, není dítěti internet zakazovat či jej v jeho užívání nepřiměřené míře omezovat. Realitou současného světa je – chtě nechtě – přesun lidské komunikace a činnosti do kyberprostoru, přičemž ze samotné podstaty společnosti musí nutně docházet k přesunu společenských jevů pozitivních i negativních. Z tohoto hlediska je pak naopak žádoucí dětem při jejich interakci s kyberprostorem poskytovat tolik svobody, kolik je přiměřené jejich věku a psychologické zralosti. Je pak zásadní současně s poskytnutím dostatečného prostoru učit děti kybernetické gramotnosti a obecné ostražitosti při jednání s cizími lidmi, a to tak, aby si dítě dokázalo

[54] Tamtéž.

[55] PORADA, V. Kriminalistika: technické, forenzní a kybernetické aspekty. 2. aktualizované a rozšířené vydání., s. 656.

vytyčit vlastní hranice a aby se naučilo v síti bezpečně pohybovat. Jak již bylo ostatně uvedeno, jedním z významných faktorů ovlivňujících kriminalistickou situaci je právě úroveň ostražitosti dětí pohybujících se v kyberprostoru a míra kybernetické gramotnosti v populaci.

V České republice se tématem prevence nejen kybergroomingu zabývá Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci v čele s Kamilem Kopeckým a René Szotkowskim. Toto vědecké pracoviště mimo jiné realizuje projekt *E-Bezpečí*, který se při své činnosti zaměřuje na prevenci, vzdělávání, výzkum, intervenci a osvětu spojenou rizikovým chováním na internetu a se souvisejícími fenomény.[56]

Závěr

Ačkoliv je kybergrooming fenoménem moderním, svou historií nepřesahujícím časovou hranici 21. století, jedná se stále jen a pouze o jinou formu pradávného společensky škodlivého jevu, kterým je vylákání dítěte dospělou osobou na odlehlé místo mimo dohled jeho přirozených ochránců, a to za účelem realizace určitého způsobu sexuální interakce. Každý z nás v dětství slýchával varování rodičů o „zlých lidech" nabízejících sladkosti, které vzápětí dítě zatáhnou do tmavé dodávky nebo do křoví. Internet je prostorem bezrozměrným a zároveň nekonečným, kde se pomyslné „křoví" může skrývat v každém dětském pokojíčku či ve školní lavici. Onen „zlý člověk" může být v podstatě kýmkoliv, domnělým vrstevníkem ze stejného města, dospělým kamarádem, který jako jediný chápe problémy dvanáctiletého dítěte, nebo kreslenou postavičkou z videohry. A onou „sladkostí" mohou být v době bezhotovostních plateb a PayPalu klidně i peníze.

Při potírání kybergroomingu a jemu podobných jevů si je potřeba uvědomovat hranice možností orgánů činných v trestním řízení a jejich represivního přístupu k této problematice. Bohužel, drtivá většina groomingových aktivit vůči dětem na internetu zůstane neodhalena a většina pachatelů zůstane za své jednání nepotrestána. Klíčem přitom není pouze zdokonalování kriminalistických postupů a technického a personálního vybavení Policie České republiky. Zásadní je posílení přímé prevence cílené na děti a zvýšení jejich kybernetické

[56] Informace o projektu. E-Bezpečí [online]. [cit. 2023-04-03]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu.

gramotnosti. Dle průzkumu projektu E-Bezpečí 26,77 % dětských respondentů (7274 dětí z 27177) v průzkumu v roce 2019 uvedlo, že dostali od jiného uživatele či uživatelky internetu nabídku na setkání v reálném světě, přičemž tohoto uživatele znali pouze z internetu. Z pozvaných pak na schůzku dorazilo téměř 70 % dětí (5081 z 7274).[57] Ačkoliv z uvedené statistiky nevyplývá, že se ve všech případech jednalo o uživatele dospělého, natožpak že se jedná o případy kybergroomingu, alarmujícím zjištěním je již samotný fakt, jak vysoké procento dětí je ochotné se s člověkem známým pouze z kyberprostoru v reálném světě setkat.

Výše uvedenou hrozivou statistiku lze brát jako apel na to, aby byl boj proti kybergroomingu – krom jeho potírání cestou trestněprávní odpovědnosti a trestního stíhání – veden také na druhé frontě, a to odspoda, cestou lepší informovanosti veřejnosti o tomto jevu a o způsobech, jak mu předcházet a jak se mu účinně bránit.

Seznam literatury

Monografie

1. ČÍRTKOVÁ, L. *Forenzní psychologie. 3., upr. vyd.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN 978-80-7380-461-9.
2. GŘIVNA, T., RICHTER, M., ŠIMÁNOVÁ, H. (eds.). *Vliv nových technologií na trestní právo.* Praha: Auditorium, 2022, s. 345-359. ISBN 978-80-87284-95-7.
3. CHMELÍK, J. *Rukověť kriminalistiky.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-36-9.
4. KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.
5. KONRÁD, Z., PORADA, V., STRAUS, J., SUCHÁNEK, J.. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování. 2. rozšířené vydání.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4.
6. MUSIL, J., KONRÁD, Z., SUCHÁNEK, J. *Kriminalistika. 2., přepracované a doplněné vydání.* Praha: C. H. Beck, 2004. ISBN 80-7179-878-9.

[57] KOPECKÝ, K, SZOTKOWSKI, R. *České děti v kybersvětě: Jak se chovají online a co jim hrozí?* [online]. O2 Czech Republic a Univerzita Palackého v Olomouci, Centrum prevence rizikové virtuální komunikace, 2019. [cit. 2023-04-03] Dostupné z: https://www.e-bezpeci.cz/index.php. s. 26.

7. PORADA, V., STRAUS, J. *Kriminalistické stopy: teorie, metodologie, praxe*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012. ISBN 978-80-7380-396-4.
8. PORADA, V. Kriminalistika: technické, forenzní a kybernetické aspekty. 2. aktualizované a rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2.
9. SMEJKAL, V. *Kybernetická kriminalita. 2. rozšířené a aktualizované vydání.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.
10. STRAUS, J., PORADA, V.. *Teorie, metody a metodologie kriminalistiky*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. ISBN 978-80-7380-666-8.
11. ŠÁMAL, P. *Trestní řád: komentář. 7., dopl. a přeprac. vyd.* V Praze: C.H. Beck, 2013. Velké komentáře. ISBN 978-80-7400-465-0.

Odborné články

1. COHEN, L. E., FELSON, M. *Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review* [online]. 1979, 44(4) [cit. 2023-04-15]. ISSN 00031224. Dostupné z: doi:10.2307/2094589.
2. HEJDUK, M. *Kriminalistické aspekty odhalování, prověřování a vyšetřování počítačové mravnostní kriminality. Bezpečnostní teorie a praxe*. Praha: Policejní akademie. 2021 (1). Dostupné z: <https://veda.polac.cz/wp-content/uploads/2021/04/Kriminalisticke-aspekty-odhalovani-proverovani-a-vysetrovani-pocitacove-mravnostni-kriminality.pdf. s.71>.
3. KOLHE, M., AHIRAO, P. Live Vs Dead Computer Forensic Image Acquisition. *International Journal of Computer Science and Information Technologies*. 2017, 8(3), 455-457. ISSN 0975-9646.
4. KRUPIČKA, J. Kybergrooming – zrcadlo společnosti? In: GŘIVNA, T., RICHTER, M., ŠIMÁNOVÁ, H. (eds.). *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022, s. 345-359. ISBN 978-80-87284-95-7.
5. PORADA, V. Dokazování obsahu elektronických dokumentů. *Košická bezpečnostná revue*. Košice, 2012 (2), s. 104 - 108. ISSN 1338-6956.

Studie

1. KOPECKÝ, K. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: Univerzita Palackého v Olomouci, 2015. ISBN 978-80-244-4868-8.

2. VLACH, J., KUDRLOVÁ, K., PALOUŠOVÁ V. *Kyberkriminalita v kriminologické perspektivě*. Praha: Institut pro kriminologii a sociální prevenci, 2020. ISBN 978-80-7338-189-9.

Kvalifikační práce

1. AMIRIDU, R. *Zajištění integrity elektronického důkazu*. Brno, 2021. Diplomová práce. Masarykova Univerzita. Vedoucí práce JUDr. Mgr. Jakub Harašta, Ph.D.
2. KUDRLOVÁ, K. *Kriminalita spojená s využíváním nových médií dětmi*. Praha, 2019. Disertační práce. Katedra trestního práva. Právnická fakulta Univerzity Karlovy. Vedoucí práce doc. JUDr. Bc. Tomáš Gřivna, Ph.D.

Judikatura

Usnesení Nejvyššího soudu ze dne 25.11.2020 sp. zn. 8 Tdo 1041/2020.

Právní předpisy

1. Směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV.
2. Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, ve znění pozdějších předpisů.
3. Zákon č. 141/1961 Sb., zákon o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
4. Zákon č. 141/2014 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění zákona č. 105/2013 Sb.
5. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Internetové zdroje

1. *CyberTipline Reports* [online]. NCMEC [cit. 2023-04-15]. Dostupné z: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata#reports.
2. KOPECKÝ, K., SZOTKOWSKI, R. *České děti v kybersvětě: Jak se chovají online a co jim hrozí?* [online]. O2 Czech Republic a Univerzita Palackého v Olomouci, Centrum prevence rizikové virtuální

komunikace, 2019. [cit. 2023-04-03] Dostupné z: https://www.e-bezpeci.cz/index.php.
3. *Muž měl zneužívat malou holčičku*. Policie ČR [online]. [cit. 2023-04-15]. Dostupné z: https://www.policie.cz/clanek/muz-mel-zneuzivat-malou-holcicku.aspx.
4. *Online grooming and UK law. Childnet International* [online]. [cit. 2023-04-17]. Dostupné z: https://www.childnet.com/wp-content/uploads/2014/08/online-grooming.pdf.
5. PROCHÁZKA, L. *Poznámky z oboru soudní sexuologie. Česká a slovenská psychiatrie* [online]. [cit. 2023-04-18]. Dostupné z: http://www.cspsychiatr.cz/detail.php?stat=35.
6. *Standard vybavení speciální výslechové místnosti pro dětského účastníka trestního řízení* [online]. Policie ČR [cit. 2023-04-17]. Dostupné z: https://www.mvcr.cz/clanek/standard-vybaveni-specialni-vyslechove-mistnosti-pro-detskeho-ucastnika-trestniho-rizeni.aspx.

ŠPECIÁLNA SEKCIA

NOVÁ REGULÁCIA DIGITÁLNYCH SLUŽIEB: ZÁZRAČNÝ LIEK ALEBO PREMÁRNENÁ PRÍLEŽITOSŤ?

Vedecké články, ktoré sú zaradené v tejto špeciálnej sekcii, sú výstupom z konferencie Bratislavské právnické fórum 2023, sekcia práva informačných technológií a práva duševného vlastníctva. Konferencia sa konala 11. a 12. septembra 2023.

SPECIAL SECTION

NEW REGULATION OF DIGITAL SERVICES: MIRACLE CURE OR MISSED OPPORTUNITY?

The scientific articles included in this special section are the output of the Bratislava Legal Forum 2023 conference, Information Technology Law and Intellectual Property Law Section. The conference took place on September 11 and 12, 2023.

ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLII
2/2023

THE ROLE OF ARTIFICIAL INTELLIGENCE IN ALTERNATIVE DISPUTE RESOLUTION

Mgr. Jana Cihanová, LL.M.

Univerzita Komenského v Bratislave, Právnická fakulta
Katedra občianskeho práva
cihanova2@uniba.sk

Abstract: The article focuses on Alternative Dispute Resolution (ADR) as one of the areas where Artificial Intelligence (AI) can play a significant role, and it can be assumed that this role will grow even more. With the development of society, the methods used for efficient and fair dispute resolution must also evolve, which can facilitate access to justice in society. This article aims to contribute to the discussion regarding the possibility of implementing AI in ADR. Also, it addresses the potential benefits of implementing AI in ADR, its challenges and possible implications for the future of dispute resolution.

Key words: Alternative Dispute Resolution. Artificial Intelligence. Efficiency.

Introduction

ADR has been an important part of the legal landscape and provides an alternative to resolving disputes through the courts. The parties decide to use ADR mechanisms because of the court process's time-consuming and primarily financial demands.[1] With the development of society, the methods used for efficient and fair dispute resolution must

[1] HIBAH, A. The role of Artificial Intelligence in Online Dispute Resolution: A brief and critical overview, 2022, Information & Communications Technology Law, 31:3, p.320 [online]. [last accessed 10.09.2023] Available at: https://www.tandfonline.com/doi/epdf/10.1080/13600834.2022.2088060?needAccess=true

also evolve. Technology has emerged as a transformative force in this rapidly changing environment, with AI gaining the most attention. As already stated, the fact is that AI permeates almost all areas of society, and the legal field is no exception. This article analyses the potential use of AI in ADR and its implications. Also, it explores the prospective difficulties in integrating, its advantages, and potential consequences for future conflict resolution.

1. Why should we think about implementing AI in ADR?

One of the areas that AI can influence is the area of dispute resolution. Currently, disputes can be resolved through the courts, or alternative methods can be used. However, this article focuses only on *ADR*. Alternative dispute resolution mechanisms, such as arbitration, mediation, conciliation or negotiation, have become more prevalent in the past to resolve disputes rather than traditional court proceedings. ADR methods were created mainly as a reaction to the lengthy and financially demanding judicial resolution of disputes, as some of these methods may be faster and less financially demanding, mainly in mediation[2] and conciliation. Therefore, many companies and individuals use alternative methods to resolve disputes to save time and cost.[3]

With the rapid advancement of technology, especially AI systems, the impact of AI on ADR mechanisms has increasingly begun to be considered. According to some authors, the use of AI in ADR, mainly in online dispute resolution (*ODR)*[4], after the initial higher costs of implementing the technology, may improve efficiency and reduce the costs of the dispute resolution process.[5] We are already seeing the use of AI within the legal profession, and it can be expected that this use will continue to grow soon. The availability of AI systems makes it possible to use algorithms, for example, to analyze data to predict outcomes and identify patterns. This can lead to more efficient and

[2] GORNAĽOVÁ, D. Mediation as a prevention to court proceeding. In KUNDRÁT, R. - SKOLODOVÁ K. - MINČIČOVÁ , M. (eds.) Ochrana, prevencia a zodpovednosť v právnych vzťahoch: Conference Proceedings. 1st edition. Košice: Pavol Jozef Šafárik University, 2020. p. 164

[3] STRAŽIŠAR, B. Alternative Dispute Resolution. Law. Journal of the Higher School of Economics. (2018). pp. 214-233 [online]. [last accessed 10.09.2023] Available at: https://www.researchgate.net/publication/328580909_Alternative_Dispute_Resolution

[4] ODR is one of the forms of alternative dispute resolution that are completely or at least partially resolved over the internet (online)

[5] See *supranote* 1 p. 337

accurate dispute resolution. In society, we can already see the gradual infiltration of AI into dispute resolution. AI can be highly effective, as it relies on automation and performs tasks much faster than humans and on a much larger scale. This is precisely the purpose of algorithms - *the ability to handle mass decisions at high accuracy and low cost*.[6] However, in the case of dispute resolution, it is necessary to remember that this automation means - *that a human does not decide human problems*. This automation can appear problematic mainly because algorithms cannot easily learn human values, and this can cause a problem in the acceptance of the decision by the addressees, and this decision can thus be at the expense of legitimacy and justice in individual cases.[7]

Why should we think about the possibilities of implementing AI in ADR? Following the increase in demand for effective, less financially demanding and fast dispute resolution, such decision-making can be ensured by combining AI with ADR mechanisms. However, like any technology implementation into a specific process or activity in society, it brings advantages and certain risks or limitations, which must be carefully considered and resolved before implementation. The following chapters are dedicated to exploring the possibility of how AI can be implemented in ADR, but especially the above - the opportunities and limitations that this implementation offers.

2. The Integration of AI in ADR and its benefits

The most likely use of AI is through predictive analytics, which uses algorithms and machine learning to analyze data and predict future outcomes. This is one of the main ways AI is expected to impact ADR, particularly by examining data on previous disputes and their outcomes to predict how comparable disputes are likely to be resolved in the future.[8]

In the context of the possibilities of how to integrate AI into ADR, we can consider two ways. The first way is the complete automation of

[6] SCHERER, M. International Arbitration 3.0 – How Artificial Intelligence Will Change Dispute Resolution?, in: Austrian Yearbook on International Arbitration. (2019) [online]. [last accessed 15.09.2023] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3377234.

[7] HUSOVEC, M., MESARČÍK, M., ANDRAŠKO, J. Právo informačných a komunikačných technológií 1. Bratislava: TINCT, 2020, p. 108.

[8] SCHERER, M., Artificial Intelligence and Legal Decision-Making: The Wide Open? Study on the Example of International Arbitration Queen Mary School of Law Legal Studies Research (2019). [online]. [last accessed 10.09.2023] Available at: https://ssrn.com/abstract=3392669.

decision-making, and the second is using AI systems as a support tool in decision-making. However, the question is which method is currently feasible. The use of support systems in ADR can provide support to experts in ADR but also to individual parties to the dispute, they can also provide information or give recommendations. These technologies can also improve ADR outcomes by eliminating administrative tasks such as drafting documents or reports. AI can also influence ADR through *chatbots* or *virtual assistants* who can provide legal advice or information about their rights and obligations to the parties or help them draft some legal documents. This could improve access to justice because it should reduce legal aid costs.[9] Therefore, people who cannot afford a lawyer would be able to get access to it. As an example of a support system, we have to mention the beta version of the *Harvey system*[10] - a large platform based on a language model intended to facilitate the legal analysis of contracts, lawsuits and due diligence in several world languages. In particular, the system might provide faster and more cost-effective recommendations and predictions. However, the output so far requires a thorough review by lawyers - so it cannot be assumed that it will become a fully automated decision-making system shortly.[11] Currently, many support systems are being used in ADR mainly in *ODR*.[12] These systems are differentiated according to what functions they provide, and in the sense of the above, they can be divided, for example, into decision support systems or case reasoning systems.[13]

On the other hand, when we consider the possible fully automated decision-making, it can be mentioned that, unlike assistive technologies, this method faces more significant concerns because their outputs could be used to determine the outcome of ADR cases with little or no human supervision. Proponents of this approach note that if AI can detect correlational patterns in large data sets with a speed, scale and accuracy that often exceeds human capabilities, it could study past

[9] CARNEIRO, D., et al. Online Dispute Resolution: An Artificial Intelligence Perspective. Artificial Intelligence Review 41, no. 2 (2014): p. 211–240. [online]. [last accessed 12.09.2023] Available at: https://doi.org/10.1007/s10462- 011-9305-z.

[10] In November 2022, the international law firm Allen & Overy started testing the beta version of this platform, which is based on the latest Open AI models (GPT-4) improved and aimed mainly at the legal profession.

[11] *See more:* How's Harvey? The Pro and Cons of A&O's Audacious AI System [online]. [last accessed 9.09.2023] Available at: https://www.law.com/international-edition/2023/03/06/hows-harvey-the-pro-and-cons-of-aos-audacious-ai-system/?slreturn=20230822063127

[12] See more: *supranote* 9

[13] See more: *supranote* 1 p. 326

disputes and apply underlying functions, rules and insights to future disputes.[14] Although the existence of automated decision-making in dispute resolution is rare, there are some systems, such as British Columbia's Civil Resolution Tribunal (CRT)[15] or SmartSettle[16]. However, most existing automated systems[17] cannot perform significant tasks independently or without human supervision.[18]

Several potential benefits that the implementation of AI in ADR can bring are currently being discussed. As was mention, we can look at the use of AI in ADR from two points of view, i.e., the use of AI as a support system, or we can consider full automation of ADR. However, for both approaches, it can be determined that one of the most significant advantages is speed and efficiency when processing a large amount of data, which also leads to the acceleration of the dispute decision process itself.[19] Given that AI algorithms can analyze large amounts of data, supporters of the use of this type of technology assume that if AI can identify patterns or trends from previous disputes and their outputs, there is an assumption that such a system could analyze previous and apply fundamental rules and knowledge to future disputes. The faster process also significantly reduces costs for litigants, another potential benefit of using AI systems in ADR.[20] AI systems can also automate certain activities, such as various administration, which can reduce costs.

As it follows, AI in ADR can improve access to justice for the parties to the dispute because AI systems may provide less expensive legal

[14] ABBOTT, R., BRINSON, S. E. (2023).Putting the Artificial Intelligence in Alternative Dispute Resolution: How AI Rules Will Become ADR Rules. Amicus curiae : journal of the Society for Advanced Legal Studies, Vol.4(3) p. 690

[15] CRT is an AI expert system that independently performs case intake, management and communications and provides disputants with a negotiation forum. *See more:* https://civilresolutionbc.ca/about-the-crt/

[16] Smartsettle is a negotiation tool that can independently provide a compromise between disputants and provide a recommended settlement to a human neutral. *See more:* https://www.smartsettleresolutions.com/

[17] *See more*: ZELEZNIKOW J. Using Artificial Intelligence to provide Intelligent Dispute Resolution Support. Group Decis Negot. 2021;30(4):789-812.

[18] *See more:* McKendrick, J. & Thurai, A. AI Isn't Ready to Make Unsupervised Decisions https://hbr.org/2022/09/ai-isnt-ready-to-make-unsupervised-decisions

[19] See *supranote* 7, p. 689

[20] GYURÁSZ, Z. GORNAĽOVÁ, D. Use of Artificial Intelligence in Arbitration. In MALACHTA, R. - PROVAZNÍK P. (eds.) Cofola International 2021: International and National Arbitration – Challenges and Trends of the Present and Future: Conference Proceedings. 1st edition. Brno: Masaryk University, 2021. p. 81 [online]. [last accessed 12.09.2023] Available at: https://www.law.muni.cz/sborniky/cofola-international/cofola-international-2021.pdf

advice in real-time, allowing the parties to the dispute to obtain information about their position and so on. In the case of creating a decision, it can be stated that, in general, people can be influenced by various factors in their decision-making, including their subjective feelings, and they often select information that is relevant for them to make a decision. On the other hand, since emotions or personal biases do not influence AI systems[21], they are less likely to make decisions based on subjective factors. AI system decisions would not be affected by human errors like bias and unfairness. This system can be programmed to consider relevant legal principles and regulations or other rules and to analyze large amounts of data, including historical case data, to identify patterns and trends that can further improve the accuracy and fairness of decisions and using AI in direct communication between parties can play a role in mitigating conflict.[22]

3. Limitations, challenges and considerations of implementing AI in ADR

Despite these potential benefits, there are also concerns about the use of AI in ADR. One of the main concerns is the potential for bias in the data contained in the algorithms and datasets. An AI platform's accuracy and "fairness" is only as good as the data fed into it. The AI program would be limited only to the information the programmer and the party provided. If the data sets contain biased information, then the results generated by the AI will also be affected.[23] Another concern arising from using AI in ADR is the issue of transparency, or the need to understand how users make decisions through AI. Some AI systems may lack explainability and transparency, which means that the logic according to which they make any decisions or recommendations is not sufficiently explainable or not in a way that makes sense to system users. It follows from the above that the use of such non-transparent

[21] GYURÁSZ, Z. Ethics in the Age of AI. In SZAKÁCS, A. – HLINKA, T. (zost.) Bratislava Legal Forum 2020: Disruptive Technologies: Regulatory and Ethical Challenge. Bratislava: Právnická fakulta UK, 2020, p. 64 [online]. [last accessed 12.09.2023] Available at: https://www.flaw.uniba.sk/fileadmin/praf/BPF/2020/ZBORNI__K_IT_2020_- _

[22] RABINOVICH EINY, O., & KATSH, E. Artificial Intelligence and the Future of Dispute Resolution: The Age of AI-DR. In D. Rainey, E. Katsh, & M. Abdel Wahab (Eds.), Online Dispute Resolution: Theory and Practice. (2021). Eleven International Publishing. (2 ed.,) p. 477 [online]. [last accessed 15.09.2023] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3830033

[23] *Ibid.* p. 482

dispute resolution systems can weaken the right of individuals to a reasoned decision, as well as their right to challenge the decision. This fact thus he opponent's claims of this implementation, as they have concluded that decision-making using automated technologies should never replace existing human dispute resolution processes since technology cannot replace human reasoning and common sense nor achieve fairness and justice in the context of ADR. [24]

Another limitation that can be considered is that AI systems lack emotional intelligence. On the one hand, this fact represented an advantage in the form of the possibility of unbiased results, but these systems cannot read and interpret non-verbal cues that can be important for understanding the perspectives of the parties and making a decision; these systems are not empathetic and cannot react to emotions. Concerns about AI's accuracy, bias and fairness are significant, given the impact results can have on the rights of individuals. AI may need to be better equipped to successfully automate the interpretative human aspects since disputed facts are integral to many conflicts.[25]

Furthermore, it is necessary to mention that this implementation faces various challenges. The main challenge is the lack of flexibility in implementing AI in ADR. AI systems are designed to make decisions based on specific criteria, which can make it difficult to adapt to unique or complex cases. Given that, for example, the laws or the rules that can govern the ADR process do not provide "the kind of structure that can easily help an algorithm learn and identify patterns and rules, which presents a significant weakness.[26] Legislation needed to implement AI into ADR is also a challenge. There are currently no established guidelines or rules on how AI should be used in ADR. In connection with the legal framework, it is necessary to mention the so-called EU Artificial Intelligence Act (AI Act), which was proposed in 2021 and is awaiting enactment. The AI Act will regulate systems that pose a potential risk to fundamental rights and categorize AI use cases into

[24] CONDLIN, R. J., "Online Dispute Resolution: Stinky, Repugnant, or Drab?" (2017). Faculty Scholarship.1576. [online]. [last accessed 15.09.2023] Available at: https://digitalcommons.law.umaryland.edu/fac_pubs/1576 p.729

[25] SCHMITZ, A. J. et al. Researching Online Dispute Resolution to Expand Access to Justice," Giustizia Consensuale [Consensual Justice] (2022): P. 269-303 [online]. [last accessed 15.09.2023] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4018593

[26] ORR, D. RULE, C. Artificial Intelligence and the Future of Online Dispute Resolution. Presented at Artificial Intelligence and Its Impact on the Future of ADR, Albany, New York State Bar Association. (2019) [online]. [last accessed 15.09.2023] Available at: https://nysba.org/NYSBA/Sections/Coursebooks/Dispute%20Resolution/2019%20Fall%20Meeting/_Panel%205.pdf

levels of risk. According to the aforementioned law, the use of AI technologies in law enforcement was considered a high-risk application subject to the following mandatory requirements.

„High risk – Risk assessment and mitigation systems, high quality datasets, activity logging to promote traceability, appropriate levels of human oversight, and high levels of robustness, security, and accuracy."[27]

It can further be stated that in 2018, the European Commission for Efficiency of Justice (CEPEJ) adopted five ethical principles[28] (*respect for fundamental rights, non-discrimination, quality and security, transparency, impartiality and fairness and under user control*), for the use of AI in judicial systems, including ADR *or* ODR. In terms of this adopted document, it can be stated that the commission itself has acknowledged that the use of AI in ADR could significantly improve access to justice[29] but users should assess the appropriateness and degree of integration of AI into the dispute resolution process in order to ensure compliance with all requirements and that these technologies must not interfere with the rights guaranteed in all civil, commercial and administrative proceedings[30]. From the above, it can be assumed that the emerging AI rules will also apply to ADR.

From the above, it follows that there is a need to have clear ethical and legal frameworks that would guide the use of AI in ADR. It is also necessary to address issues related to the protection of personal data. AI systems need access to large amounts of personal data, which can have data security and privacy concerns. In the case of automated systems, CEPEJ refers to section 22 of Europe's data protection law, the General Data Protection Regulation (GDPR), which allows individuals "*to refuse to be the subject of a decision based exclusively on automated processing*" when the automated decision is not required by law and entitles them to decisions made by human decision-makers. At this

[27] *See more:* EU AI Act: first regulation on artificial intelligence [online]. [last accessed 15.09.2023] Available at: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence?&at_campaign=.

[28] *See more:* European Commission for the Efficiency of Justice (CEPEJ). 2018. "European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment" Council of Europe (2018) [online]. [last accessed 15.09.2023] Available at: https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf

[29] *See supranote* 20, p. 44

[30] For example: access to a court, adversarial principle, equality of arms.

point, it is necessary to appeal for compliance with the principle of personal data protection and to take measures to prevent their misuse.[31]

There is also the issue of the professional responsibility of lawyers and other experts who use the system in case of mistake; if the AI system gives incorrect advice in mediation, who is responsible for the error? Is it to seek an AI-based mediator, the party that implemented the system, or the party that relied on advice? For example, the European Parliament proposed that users of AI systems should be in control of the risks and have corresponding liability for damages caused by AI (Committee on Legal Affairs 2020). ADR experts can thus be liable for damages caused by AI systems they implement in a way that they would not be liable for similar damages they directly cause. For example, an ADR provider may be held liable for using an AI system that ultimately proves to have systemic racial bias, or ADR systems found to be operating with errors or unfair biases will need to be reprogrammed or decommissioned, creating another accountability mechanism for ADR.[32]

Conclusion

AI is becoming a part of our everyday life. Given the rapid technological progress, using AI in the legal profession cannot be avoided. The possibility of using AI in resolving disputes, including ADR, is gaining awareness in society. Using algorithms to analyze large amounts of data can significantly facilitate the work of lawyers, judges, or arbitrators. It can be assumed that AI integration will significantly impact ADR mechanisms' functions. This implementation presents many benefits, opportunities, and challenges that must be addressed. AI can become an important tool in the ADR process with the right approach. It is also essential to note that AI is not intended to replace human decision-making but to help and support it.

In conclusion, we believe that decisions should always be made by humans; however, AI systems should be used to the extent that they can provide suggestions and help make the process faster, more efficient and more objective, but the use of AI must be impartial, transparent and responsible. While AI has several potential benefits in ADR, risks and concerns need to be addressed. As AI technology advances, it will be

[31] *See supranote* 7, p. 696
[32] *See supranote* 7, p. 699

significant for ADR practitioners and policymakers to carefully consider the potential benefits and risks of integrating AI into ADR and to take measures to ensure that AI is responsible, impartial and transparent. However, more data and research is needed on the effectiveness and use of AI in ADR. Despite the existence of studies and pilot projects, further research will be needed to understand the impact of AI on the ADR process and its outcomes. However, one of the biggest challenges in the implementation of AI in ADR remains the issue of costs for the development and maintenance of the technology itself. AI systems require significant investment in terms of resources including data, computing power and skilled professionals. The use of AI in ADR mechanisms has its strengths and weaknesses. The use of these technologies may have the potential to make dispute resolution more efficient and reduce the costs of the process, but it also brings new concerns and challenges that are not yet sufficiently resolved. For example, it concerns issues of privacy and data protection, responsibility, legal and ethical consequences, but also the issue of admissibility of evidence that is generated by AI. Despite the fact, as we stated at the beginning of this chapter, that there are already pilot projects or supporting systems that make their activities easier for lawyers, it is necessary to further research the issue of AI in ADR and to pay attention to it in order to address the potential benefits but also the risks to the relevant policymakers as well as experts in the field of ADR and also programmers, and it is necessary to appeal for their cooperation in the implementation of AI in ADR.

Bibliography

1. ABBOTT, R., BRINSON, S. E. Putting the Artificial Intelligence in Alternative Dispute Resolution: How AI Rules Will Become ADR Rules. Amicus curiae : journal of the Society for Advanced Legal Studies, Vol.4(3), (2023). pp.685-706. [online]. Available at: https://www.jamsadr.com/files/uploads/documents/articles/abbott-ryan-amicuscuriae-putting-the-artificial-07-2023.pdf
2. CARNEIRO, D. et al. Online Dispute Resolution: An Artificial Intelligence Perspective. Artificial Intelligence Review 41, no. 2 (2014): pp. 211–240. [online]. Available at https://doi.org/10.1007/ s10462- 011-9305-z.
3. CONDLIN, R. J., Online Dispute Resolution: Stinky, Repugnant, or Drab?" (2017). Faculty Scholarship.1576. [online]. Available at: https://digitalcommons.law.umaryland.edu/fac_pubs/1576 717-758

4. GORNAĽOVÁ, D. Mediation as a prevention to court proceeding. In KUNDRÁT, R. - SKOLODOVÁ K. - MINČIČOVÁ , M. (eds.) Ochrana, prevencia a zodpovednosť v právnych vzťahoch: Conference Proceedings. 1st edition. Košice: Pavol Jozef Šafárik University, 2020. pp. 164-179 ISBN 978-80-8152-871-2
5. GYURÁSZ, Z. Ethics in the Age of AI. In SZAKÁCS, A. – HLINKA, T. (zost.) Bratislava Legal Forum 2020: Disruptive Technologies: Regulatory and Ethical Challenge. Bratislava: Právnická fakulta UK, 2020, p. 63-68. ISBN 978-80-7160-567-6, [online]. Available at: https://www.flaw.uniba.sk/fileadmin/praf/BPF/2020/ZBORNI__K_IT_2020_- _final_final_ocislovane.pdf
6. GYURÁSZ, Z., GORNAĽOVÁ, D. In MALACHTA, R., PROVAZNÍK P. (eds.) Cofola International 2021 : International and National Arbitration – Challenges and Trends of the Present and Future: Conference Proceedings. 1st edition. Brno: Masaryk University, 2021. p. 501 ISSN 2464-8485. [online]. Available at: https://www.law.muni.cz/sborniky/cofola-international/cofola-international-2021.pdf
7. HIBAH, A. The role of Artificial Intelligence in Online Dispute Resolution: A brief and critical overview. (2022). Information & Communications Technology Law. 31:3, pp. 319-342 [online]. Available at: https://www.tandfonline.com/doi/epdf/10.1080/13600834.2022.2088060?needAccess=true
8. HUSOVEC, M., MESARČÍK, M., ANDRAŠKO, J. Právo informačných a komunikačných technológií 1. Bratislava: TINCT, 2020, 262 p. ISBN 978-80-973837-0-1
9. Law reform Commission: Report on Alternative Dispute Resolution: Mediation and Conciliation (LRC 98-2010) (3rd Programme of Law Reform, Project 5) pp. 247 [online]. Available at: https://www.lawreform.ie/_fileupload/reports/r98adr.pdf
10. ORR, D. RULE, C. Artificial Intelligence and the Future of Online Dispute Resolution. Presented at Artificial Intelligence and Its Impact on the Future of ADR, Albany, New York State Bar Association. (2019) pp. 44 [online]. Available at: https://nysba.org/NYSBA/Sections/Coursebooks/Dispute%20Resolution/2019%20Fall%20Meeting/_Panel%205.pdf
11. RABINOVICH EINY, O., & KATSH, E. Artificial Intelligence and the Future of Dispute Resolution: The Age of AI-DR. In D. Rainey, E. Katsh, & M. Abdel Wahab Eds.), Online Dispute Resolution: Theory and Practice. (2021). Eleven International Publishing. (2 ed.,) p. 477 [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3830033
12. SCHERER, M. International Arbitration 3.0 – How Artificial Intelligence Will Change Dispute Resolution?, in: Austrian Yearbook

on International Arbitration. (2019) [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3377234
13. SCHERER, M., Artificial Intelligence and Legal Decision-Making: The Wide Open? Study on the Example of International Arbitration Queen Mary School of Law Legal Studies Research (2019). [online]. Available at: https://ssrn.com/abstract=3392669.
14. SCHMITZ, A. J. et al. Researching Online Dispute Resolution to Expand Access to Justice," Giustizia Consensuale [Consensual Justice] (2022): pp. 269-303 [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4018593
15. STRAŽIŠAR, B. Alternative Dispute Resolution. Law. Journal of the Higher School of Economics. (2018). pp. 214-233 [online]. Available at: https://www.researchgate.net/publication/328580909_Alternative_Dispute_Resolution
16. How's Harvey? The Pro and Cons of A&O's Audacious AI System [online]. Available at: https://www.law.com/international-edition/2023/03/06/hows-harvey-the-pro-and-cons-of-aos-audacious-ai-system/?slreturn=20230822063127
17. McKENDRICK, J. & THURAI, A. AI Isn't Ready to Make Unsupervised Decisions. https://hbr.org/2022/09/ai-isnt-ready-to-make-unsupervised-decisions
18. MNOOKIN, R., Alternative Dispute Resolution Harvard Law School John M. Olin Center for Law, Economics and Business, Discussion Paper Series. Paper (1998). p. 232 [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=117253
19. EU AI Act: first regulation on artificial intelligence [online]. Available at: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence?&at_campaign=
20. European Commission for the Efficiency of Justice (CEPEJ). 2018. "European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment" Council of Europe (2018) [online]. Available at: https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf

ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLII
2/2023

THE GERMAN PERSPECTIVE ON THE DEPLOYMENT OF AUTOMATED VEHICLES

Bc. Stela Košťálová

Comenius University in Bratislava, Faculty of Law
Institute of Information Technology Law and Intellectual Property Law[1]
kostalova49@uniba.sk

Abstract: Automated mobility is an increasingly important area in road transport primarily due to high accident rates caused by human failure, the need for inclusion, and the emergence of sustainable transport. Road transport makes a major contribution not only to getting from point A to point B but also has a significant impact on the economy and employment. The purpose of this paper is an analysis of the different legal approaches to the deployment of automated vehicles in Germany and Slovakia. This paper first gives a brief overview of the functional safety legislation of automated vehicles, then focuses on its market surveillance and the role of the driver in automated vehicles.

Key words: automated vehicle, functional safety, market surveillance, Digital Single Market, human driver

Introduction

Road transport depends on multiple factors to ensure the safety of all road traffic participants, such as drivers, passengers in vehicles, and vulnerable road users[2] (cyclists, pedestrians, and users of powered two-

[1] Student research assistant at the Institute of Information Technology Law and Intellectual Property Law, Faculty of Law, Comenius University in Bratislava.

[2] Art. 3 Sec. 1 Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their

wheelers). Digital development is fast becoming a key instrument in the fourth industrial revolution[3] and raises variety of questions regarding automated vehicles.

In recent years, there have been numerous accidents caused by human failure. In 2021, driver failure was the most common cause of traffic accidents in Germany. According to statistics published by the Statistical Office of Germany, up to 88% the total number of traffic accidents with personal injuries were caused by human failure.[4] Despite the lack of statistics in Slovakia with regards to the total number of traffic accidents with personal injuries caused by human failure, it can be stated that in 2021 there were at least 10,812 traffic accidents caused by human failure out of the total of 11,886 traffic accidents in Slovakia. According to the available data, accidents caused by human failure account for at least 90% of all road accidents in Slovakia. [5] It is clear from the above that the most road accidents are the result of human failure. These accidents are preventable through the sensitive use of technology.

Technology driving aids are improving to help the driver or replace the driver for certain tasks. Those improvements on a daily basis come along with the related legal aspects. One of the greatest challenges in automated mobility is the safety[6] and security[7] of the driving systems. It is established that 100% safety and security cannot be achieved.[8] Automated vehicles raise a natural scepticism in society mostly about their safety and it is therefore needed to have market surveillance to ensure road safety and rethink the role of the driver. There is also an

general safety and the protection of vehicle occupants and vulnerable road users (General Safety Regulation).

3 See SCHWAB, K. *The Fourth Industrial Revolution: what it means, how to respond.* [online]. [s.l.] World Economic Forum, 14.01.2016. [last accessed 2023-08-08]. Available at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

4 Destatis. Verkehrsunfälle 2021, Fachserie 8, Reihe 7, p. 50.

5 *Vyhodnotenie dopravno-bezpečnostnej situácie za 12 mesiacov 2021 (definitívne štatistické údaje).* [online]. [s.l.] Prezídium Policajného zboru, odbor dopravnej polície [s.a.]. [last accessed 2023-08-08]. Available at: https://www.minv.sk/?statisticke-ukazovatele-sluzby-dopravnej-policie&subor=471269

6 The term „safety" will be used in this paper to refer to functional safety.

7 The term „security" refer to cyber security.

8 See GALINSKI, M. Kybernetická bezpečnosť automatizovaných vozidiel – technické aspekty. In: ANDRAŠKO, J. et al. *Právne a technické aspekty kybernetickej bezpečnosti automatizovaných vozidiel*. Bratislava: Wolters Kluwer SR s.r.o., 2022. p. 36. ISBN 978-80-571-0554-1.

ethical conflict between safety and responsibility (other Trolley Case) in automated mobility. What is more important?

Germany and Slovakia are at the forefront of automotive production within the European Union. However, they have contrasting approaches to implementing automated vehicles on a national level.

This paper has been divided into three parts, starting with a brief overview of the functional safety legislation for automated vehicles, then focusing on market surveillance, and finally, we will have a look at the role of the driver in automated vehicles. These parts are crucial for safe and secure driving in road traffic.

1. Technical requirements

It is necessary here to clarify exactly what is meant by the automated vehicle and fully automated vehicle under the European Law and the standard SAE J 3016 last revised in April 2021. On the level of European Law, the **automated vehicle** is defined as a *motor vehicle designed and constructed to move autonomously for certain periods of time without continuous driver supervision but in respect of which driver intervention is still expected or required* and regarding the standard SAE J 3016, this falls under SAE level 0 – 4. **The fully automated vehicle** means a *motor vehicle that has been designed and constructed to move autonomously without any driver supervision* and which falls below SAE level 4 - 5, where the presence of a driver is not required.[9]

Slovak national legislation refers to the General Safety Regulation.[10] In contrast, the German definition of the highly or fully automated vehicle goes into more detail and presents **motor vehicles with a highly or fully automated driving function** as *those that have technical equipment:*

1. capable of controlling the vehicle in order to **perform the driving task** – including longitudinal[11] and lateral guidance[12] – after activation (vehicle control),

[9] Art. 3 Sec. 21-22 of the General Safety Regulation; *SAE J3016 Levels of driving automation*. [online]. [s.l.] SAE, 03.05.2021. [last accessed 2023-08-08]. Available at: https://www.sae.org/binaries/content/assets/cm/content/blog/sae-j3016-visual chart_5.3.2 1.pdf

[10] § 2 Sec. 2 Subsec. ac - ae of Act No. 106/2018 Coll. on the Operation of Vehicles in Road Traffic. [Zákon č. 106/2018 Z. z. o prevádzke vozidiel v cestnej premávke]

[11] Longitudinal guidance means accelerating, maintaining speed, or braking.

[12] Lateral guidance includes for instance steering.

2. capable of complying with the **traffic regulations addressed to the vehicle control** during highly or fully automated vehicle control,
3. capable to be manually overridden or deactivated by the driver of the vehicle at any time,
4. detection of the need for the driver to manually control the vehicle,
5. capable of indicating to the driver the need for manual control of the vehicle with a sufficient time reserve before the driver is given control of the vehicle by optical, acoustic, tactile or other perceptible signals, and
6. warns of any use contrary to the system description.[13]

German national legislation goes further and defines the **motor vehicle with an autonomous driving function** as the motor vehicle:

1. capable of ***performing the driving task independently, within a defined operating area, without a person driving the vehicle***, and
2. ***has*** certain ***technical equipment***.[14]

The Geneva Convention on Road Traffic and the Vienna Convention on Road Traffic are the fundamental part of the international transport law. The conventions have brought order to the rapidly developing road transport sector in the 20th century. The Geneva Convention in 1949 established standardised road traffic regulations, driver's eligibility criteria and international driving permit, which was followed by the Vienna Convention in 1968 amending the standardised road traffic regulations and requirements for the driver.

Given the diversity of mentalities and customs in various regions of the world, it was necessary to harmonise technical norms on the international level. International technical harmonisation has taken place based on the 1958 Agreement and the 1998 parallel Agreement. The 1958 Agreement was made by UNECE[15] to which are annexed UN No. 1 - 164 Regulations. The 1998 parallel Agreement was established to strengthen the process of existing international technical harmonisation by the development of Global Technical Regulations

[13] § 1a sec. 2 of the Autonomous Driving Act. BGBl. I p. 986. [Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen]

[14] § 1d sec. 1 of the Autonomous Driving Act. BGBl. I p. 986. [Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen]

[15] United Nations Economic Commission for Europe.

(GTRs)[16]. The European Union, as a contracting party, aims to ensure applicability of all these regulations under the European Law with *direct reference in European Union legislation*[17], extending the scope of harmonisation within the European Union.

European Union is progressively developing the legal regulations on automated mobility, the most important of these are Regulation on approval and market surveillance of the motor vehicle[18] complementing the type-approval requirements, the General Safety Regulation[19], Commission Implementing Regulation for the type-approval of the automated driving system (ADS)[20] and NIS 2[21] Directive on cybersecurity, which is relevant to systems of automated vehicle as well.

Member States of the European Union are obligated to establish their own type-approval authorities. Member States shall ensure that their own approval authorities and market surveillance authorities adhere **to a strict separation of roles and responsibilities** and that **they each function independently from each other**.[22]

The Federal Motor Transport Authority is the national type-approval authority[23] in Germany, including for highly or fully

---

16 Art. 6 of the 1998 Parallel Agreement.

17 See Recital 21 of the General Safety Regulation; Council Decision No. 2013/456/EU of 22 July 2013 amending Decision 97/836/EC with a view to accession by the European Community to the Agreement of the United Nations Economic Commission for Europe concerning the adoption of uniform technical prescriptions for wheeled vehicles, equipment and parts which can be fitted to and/or be used on wheeled vehicles and the conditions for reciprocal recognition of approvals granted on the basis of these prescriptions (Revised 1958 Agreement) In: *Official Journal of the European Union* L 245, p. 1; Council Decision No. 2013/454/EU of 22 July 2013 amending Decision 2000/125/EC concerning the conclusion of the Agreement concerning the establishing of global technical regulations for wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles (Parallel Agreement) In: *Official Journal of the European Union* L 245, p. 25;

18 Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles.

19 General Safety Regulation.

20 Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS).

21 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2).

22 Art. 6 Sec. 1 of the General Safety Regulation.

23 § 20 Sec. 2 of the Road Traffic Licensing Act. BGBl. I p. 679. [Straßenverkehrs-Zulassungs-Ordnung]

automated vehicles. The Federal Motor Transport Authority issues the following approvals regarding automated mobility:

- National type-approvals highly or fully automated vehicle corresponding to level 4,
- EU type-approvals for highly or fully automated vehicle corresponding to level 4 in small series production,
- Testing approvals for highly or fully automated vehicle from level 3 onwards,
- Type-approvals for highly or fully automated vehicle from level 3 onwards, which can be activated after registration of the motor vehicle.[24]

The Autonomous Driving Act sets 4 requirements for the type-approval for vehicles with autonomous driving function. The initial requirement is Manufacturer's Declaration on Functional Safety of Autonomous Vehicles, the following are required documents including instruction manual, functional safety concept, IT security concept, functional specification of the vehicle, catalogue of test scenarios and environmental assessment. Fulfilling functional requirements and avoiding collisions in a prescribed manner is the third requirement. The last condition required by the Federal Motor Transport Authority is most crucial, it requires safety of road traffic and does not put human live at risk.[25]

Act No. 429/2022 Coll. amending and supplementing certain laws relating to the development of automated vehicles[26], including the Act No. 575/2001 Coll. on the Organisation of Government Activities and the Organisation of the Central State Administration, to which it extended the competence of the Ministry of Transport of the Slovak Republic to the *creation and implementation of an intelligent mobility policy*.[27] The Ministry of Transport of the Slovak Republic is also

[24] *Erprobungsgenehmigung*. [online]. [s.l.] Das Kraftfahrt-Bundesamt, [s.a.]. [last accessed 2023-09-09]. Available at: https://www.kba.de/DE/Themen/ Typgenehmigung/Autonomes_ automatisiertes_Fahren/Erprobungsgenehmigung/erprobungsgenehmigung_node.html

[25] § 4 Sec. 1 of the Autonomous Driving Act. BGBl. I p. 986. [Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen]

[26] Translated from the official name of the Act: Zákon č. 429/222 Z. z. ktorým sa menia a dopĺňajú niektoré zákony v súvislosti s rozvojom automatizovaných vozidiel.

[27] § 8 sec. 1 subsec. p of the Act No. 575/2001 Coll. on the Organisation of Government Activities and the Organisation of the Central State Administration. [Zákon č. 575/2001 Z. z. o organizácií činnosti vlády a organizácií ústrednej štátnej správy]

responsible for road transport, combined transport, and roads[28], in addition to the creation and implementation of an intelligent mobility policy. This long-awaited legislation was intended to *consider all aspects of smart mobility, which have been overlooked and absent from the regulation of various legal relationships*[29] in Slovakia. Despite the considerable sophistication of German legislation, Slovakia only incorporates the requirements of international and European law into its national law, without going beyond them. In **Slovakia**, the national type-approval authority is the **Ministry of Transport of the Slovak Republic**.[30]

2. (Digital) Market Surveillance

There are two types of market surveillance, active and reactive market surveillance. Active market surveillance involves regular monitoring of the market, while reactive market surveillance includes investigation of violations reported by market participants.[31]

For autonomous vehicles, it is crucial to consider not only the interactions between the physical vehicle and subsequent actions but also to consider the evolving relationships within the various platforms that reside within the vehicle. The consumer must be protected from unfair practices not only in traditional legal relationships but also in those arising in the digital market. Identifying unfair practices in the digital market can be challenging but not impossible.

*Special attention should be given to emerging technologies, taking into account that consumers are increasingly using connected devices in their daily lives. **The Union regulatory framework** should therefore **address the new risks to ensure the safety of the end users**, which could*

[28] § 8 sec. 1 subsec. b-d of the Act No. 575/2001 Coll. on the Organisation of Government Activities and the Organisation of the Central State Administration. [Zákon č. 575/2001 Z. z. o organizácií činnosti vlády a organizácií ústrednej štátnej správy]

[29] Explanatory memorandum to Act No.429/2022 Coll. amending and supplementing certain laws relating to the development of automated vehicles. [online] Bratislava: NRSR, 24.08.2022. [last accessed 2023-09-09]. Available at: https://www.nrsr.sk/web/Dynamic /DocumentPreview .aspx?DocID=515513

[30] §135 sec. 2 of Act No. 106/2018 Coll. on the Operation of Vehicles in Road Traffic. [Zákon č. 106/2018 Z. z. o prevádzke vozidiel v cestnej premávke]

[31] *Marktüberwachung*. [online]. [s.l.] Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz. [s.a.]. [last accessed 2023-09-09]. Available at: https://www.bmuv.de/themen/kreislaufwirtschaft/marktueberwachung

contribute to the effective market surveillance.[32] *Market surveillance can improve the functioning of the EU internal market by doing the activities carried out and measures taken by market surveillance authorities to ensure that products comply with the requirements set out and to ensure protection of the public interest.*[33]

In heterogeneous relationships, which prevail in the market, there is a natural inequality – asymmetry that arises to be balanced. In the case of the highly or fully automated vehicle, there is a significant information asymmetry. The manufacturers or distributors of the highly or fully automated vehicle have extensive knowledge of this type of vehicle, while the consumer[34] may have varying degrees of understanding. Consumer protection policy is addressing market failures caused by information asymmetry.[35] Misuse of information asymmetry can lead to unfair competition[36], where technologies will, for example, rank in favour of a pre-selected network of charging or petrol stations.

The example mentioned above is not futuristic, however, several services are currently being implemented. These services aim to provide comfort of passengers while simultaneously increasing the revenues of the individual market players. Mercedes-Benz drivers can already pay for refueling directly from the car via the Mercedes-me app.[37] Another giant - Volkswagen Group launched App Store for selected Audi[38] models this year. Downloading apps from the store

[32] Recital 30-31 of the Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products.

[33] Art. 1 Sec. 1 and Art. 2 Sec. 3 of the Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products.

[34] Consumer is defined as a natural person entering a legal transaction outside the consumer's trade, business, or profession.

[35] KEBLER, W. Digital markets, data, and privacy: competition law, consumer law and data protection. In: *Journal of Intellectual Property Law & Practise*. November 2016, Volume 11, Issue 11, p. 861.

[36] Art. 5 of the Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive).

[37] LINDEN, M. *Mercedes verkauft Auto-Upgrades per Fingerabdruck*. [online]. [s.l.] golem.de, 06.03.2023. [last accessed 2023-09-09]. Available at: https://www.golem.de/news/in-car-payment-mercedes-verkauft-auto-upgrades-per-finger abdruck-2303-172404.html

[38] Volkswagen Group brand.

requires an in-car SIM card.[39] The App Store is an open ecosystem supporting services also from the outside of the Volkswagen Group[40] which is the first step to contractual chaining between individual market subjects. The Digital Markets Act aims to ensure fairness and competition in the digital sector. *To ensure that the end-user has a choice, access controllers should not prevent end users from uninstalling any pre-installed software applications on their operating system. Restrictions on uninstallation should only occur if such software applications are essential to the functioning of the operating system or device.*[41] *In ranking and related indexing and crawling, services and products offered* for example by the Mercedes- me App or Volkswagen Group App Store *shall not treat more favourably*, pre-selected services or products *than similar services or products of a third party* and *shall apply transparent, fair and non-discriminatory conditions to such ranking*.[42]

If a high or fully automated control function is activated, decision-making is transferred to technology, thereby limiting the decision-making freedom of the driver. Under the Automated Driving Act, it must be possible for such a function to be overridden or deactivated.[43] This legal norm was enshrined in the Autonomous Driving Act as a contractual obligation[44] arising from the Amendment of the Convention on Road Traffic in force from 23rd March 2016.[45] Closely related to this is the question of what to do if a vehicle that is allowed to use automated driving functions in Germany goes to the neighbouring Czech Republic, which has different legislation? If the drivers were compelled to deactivate the system outside of Germany, this would present a long-term barrier to the single market within the EU, which would lead to competition in the legal systems. The question

[39] *VW-Konzern entwickelt Appstore*. [online]. [s.l.] Welt, 01.03.2023. [last accessed 2023-09-09]. Available at: https://www.welt.de/motor/news/article244046833/Audi-startet-im-Juli-VW-Konzern-entwickelt-Appstore.html

[40] *CARIAD launches application store for the Volkswagen Group*. [online]. [s.l.] Cariad, 01.03.2023. [last accessed 2023-08-08]. Available at: https://cariad.technology/de/en/news/stories/launch-application-store-for-volkswagen-group.html

[41] Recital 49 of the Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products.

[42] Art. 6 Sub. 5 of the Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products.

[43] Art. 1a Sec. 2 Subsec. 3 of Road Traffic Act. BGBl. I p. 310, 919. [Straßenverkehrsgesetz]

[44] Art. 59 Sec. 2 Para. 1 of Basic Law for the Federal Republic of Germany. [Grundgesetz für die Bundesrepublik Deutschland]

[45] Art. 8 Para. 5 bis. of the Vienna Convention on Road Traffic.

appears complicated at first sight, but the solution can be partly found in the case law of the Court of Justice of the European Union in conjunction with Article 36 of the Treaty on the Functioning of the European Union. A vehicle with highly or fully automated driving system is considered as good in the context of free movement within the single market of the European Union. According to Article 34 of the Treaty on the Functioning of the European Union, it is considered a measure with an equivalent effect if a Member State designs its legislation relevant to the market in a way that distorts the movement of goods, in particular those that have been lawfully authorized.[46] *Dassonville* and *Cassis de Dijon* case law lay the foundations for the proper functioning of the single market.[47] The European Court of Justice of the European Union has followed these decisions on cases related to the use of products and has identified three types of national rules prohibiting access to the market:

1. Discriminatory rules
2. Imposing product requirements
3. Hindering or inhibiting market access.[48]

The European Court of Justice of the European Union stated in the case related to the use of product in context of the road safety *that a prohibition on the use of a product in the territory of a Member State has a considerable influence on the behaviour of consumers, which, in its turn, affects the access of that product to the market of that Member State*. *The prohibition to hinder access to the market* of other Member State for use of product which is *lawfully produced and marketed in* other *Member States, constitutes a measure having equivalent effect to quantitative restrictions on imports, unless it can be justified objectively.*[49] A potential buyer who is aware of the inability to use automated driving systems outside of the jurisdiction, which was sold,

[46] Dassonville formula: all trading rules enacted by Member States which are capable of hindering, directly or indirectly, actually or potentially, intra-Community trade are to be considered as measures having an effect equivalent to quantitative restrictions.

[47] Judgment of the Court of Justice of the European Union C-8/74 *Procureur du Roi v Benoît and Gustave Dassonville* from 11 July 1974; Judgment of the Court of Justice of the European Union C-120/78 *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein* from 20 February 1979.

[48] CRAIG, P., DE BURCA, G. *EU Law. Text, Cases, and Materials*. p. 724. ISBN: 9780198856641; Judgement of the Court of Justice of the European Union C-110/05 *Commision v Italy* from 10 February 2009; Judgement of the Court of Justice of the European Union C-142/05 *Åklagaren v Percy Mickelsson a Joakim Roos* from 4 June 2009.

[49] Judgement of the Court of Justice of the European Union C-110/05 *Commision v Italy* from 10 February 2009.

could lead to discouragement from buying. According to Article 36 of the Treaty on the Functioning of the European Union, prohibitions and restrictions relating to the goods can be considered under enumerated grounds, in particular public policy, public security, and the protection of the health and life of human, as objectively justified grounds. If the prohibition or restriction is justified by the need to ensure road safety, there is an urgent reason in the general interest capable of justifying an obstacle to the free movement of goods. Transport is a shared competence between the European Union and the Member States competence[50] and *in the absence of fully harmonising provisions, it is for the Member States to decide upon the level at which they wish to ensure road safety in their territory, whilst taking account of the requirements of the free movement of goods within the single market*. However, considering the variety of automated driving systems, it is important to acknowledge that each may require a different approach. Furthermore, the current state of harmonising devices present in road traffic and road signs, which have a significant impact on the behaviour of these vehicles, needs to be taken into consideration.

Digital Single Market removing virtual borders within the EU is now a reality. According to the Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements *in a connected environment, a cybersecurity incident in one product can affect an entire organisation or a whole supply chain, often propagating across the borders of the internal market within a matter of minutes. This can lead to severe disruption of economic and social activities or even become life -threatening*.[51] In order to meet market demands and to protect consumers from risky products and services, the Proposal leads to designation of *one or more market surveillance authorities* and *the market surveillance authorities shall cooperate with the national cybersecurity certification authorities, with other market surveillance authorities,* or *with the authorities supervising Union data protection law*.[52]

[50] Art. 4 Sec. 2 Subsec. g of the Treaty on Functioning of the European Union.

[51] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 from 15.09.2022.

[52] Art. 41 Para. 2-5 of Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 from 15.09.2022.

Each Member State of the European Union is required to establish, *inter alia*, their own independent market surveillance authorities.[53]

In **Germany**, market surveillance authority for highly or fully automated vehicles is the responsibility of the Federal Motor Transport Authority, as is the type-approval authority. The Federal Motor Transport Authority verifies through regular inspections fulfilment of the necessary requirements for a highly or fully automated vehicle has been met and makes risk assessment.[54] Type-approval and market *authorities may be within the same organisation provided that their activities are managed autonomously as part of separate structures*[55], as in Germany.

In **Slovakia**, the market surveillance authority for all motor vehicles including highly or fully automated vehicles is the Slovak Trade Inspection.[56]

3. The role of the driver in an automated vehicle

The Geneva Convention in 1949 established driver's eligibility criteria, which was followed by the Vienna Convention in 1968 amending requirements for the driver. Conventions differ mainly in the level of reflection on new technologies and human rights in international transport. The Vienna Convention acknowledges the impact of new technologies on human rights, resulting in more frequent amendments.

The conventions use the same definition of the driver of the vehicle as ***any person who drives a vehicle***, *including cycles, or guides draught, pack or saddle animals or herds or flocks* ***on a road****, or who is in actual physical control of the same*[57] *or* ***any person who drives a motor vehicle*** *or other vehicle (including a cycle), or who guides cattle, singly or in herds, or flocks, or draught, pack, or saddle animals* ***on a road***[58].

The conventions incorporate the concept of an "ever-present" driver inside the vehicle, which has been in force in the Vienna Convention

53 Art. 6 Sec. 1 of the General Safety Regulation.

54 § 5 of the Autonomous Driving Act. BGBl. I p. 986. [Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen]

55 Art. 6 Sec. 1 of the General Safety Regulation.

56 § 135 Sec. 6 and §139 Subsec. e of Act No. 106/2018 Coll. on the Operation of Vehicles in Road Traffic. [Zákon č. 106/2018 Z. z. o prevádzke vozidiel v cestnej premávke]

57 Art. 4 Para. 10 of the Geneva Convention on Road Traffic.

58 Art. 1 Para. v of the Vienna Convention on Road Traffic.

on Road Traffic and the Geneva Convention on Road Traffic since its earliest inception. This involves the driver's ability to sustain control of their vehicle and adapt the speed to the traffic conditions.[59] The Geneva Convention on Road Traffic requires continuously the driver's control of the vehicle while driving.[60] Compliance with SAE automatization level 0 is not problematic but the use of adaptive cruise control (ACC) alone, classified as SAE level 1-2, means that the way the vehicle is driven is influenced by the use of a driver-assist function (automated function). In addition, the Vienna Convention adapts itself for automated mobility forehead and states ***vehicle systems which influence the way vehicles are driven*** *and are not in conformity with the aforementioned conditions of construction, fitting and, utilization, shall be deemed to be in conformity with paragraph 5 of this Article and with paragraph 1 of Article 13, when such systems* ***can be overridden or switched off by the driver***.[61] In either case, a driver must be present in the vehicle. However, what sets them apart is the consideration of new technologies. The Vienna Convention currently does not include the possibility of driverless driving, but it does allow automated driving functions that can be switched off by the present driver.

European law does not define a driver.

The **German legal framework** goes beyond all established definitions. The German Road Traffic Act defines the term driver of the highly or fully automated vehicle as *person who engages a highly or fully automated driving function and utilises it to control a vehicle, regardless of whether they are driving the vehicle themselves or not, with the intended use of this feature*.[62] However, there is no legal definition of a "general" driver. Despite the absence of a driver definition, two requirements can be identified in the law concerning the person of a driver. Firstly, they must be authorized to drive a motor vehicle, and secondly, they must be in a suitable physical and mental condition to drive it.[63]

On the other hand, the **Slovak legislation** outlines a "general" driver, but does not further specify the role of the driver in a highly or fully automated vehicle. A driver is a *person driving or supervising*

[59] Art. 8 Para. 1,5 of the Vienna Convention on Road Traffic; Art. 8 Para. 1 of the Geneva Convention on Road Traffic

[60] Art. 8 Para. 5 of the Geneva Convention on Road Traffic

[61] Art. 8 Para. 5 bis. of the Vienna Convention on Road Traffic.

[62] § 1a Sec. 4 of the Road Traffic Act. BGBl. I p. 310, 919. [Straßenverkehrsgesetz]

[63] § 2 of the Road Traffic Act. BGBl. I p. 310, 919. [Straßenverkehrsgesetz]

a vehicle using an automated driving system.[64] An automated driving system is defined as a *vehicle management system, utilizing both hardware and software, to provide continuous dynamic control of the vehicle*.[65] However, this definition lacks an explanation of the intended meaning of supervising a vehicle. *A driver must be present in every moving vehicle and carriage.*[66]

The definitions of a driver in international law are consistent, however, they no longer reflect the requirements of the driver in light of new technologies. The Vienna Convention appears to have reached its limit and is waiting for the United Nations Economic Commission for Europe to present its new legal instrument on the use of automated vehicles in traffic, which will be able to define the appropriate regulation.

Conclusion

Computer or Software on wheels[67] as vehicles with automated driving functions are now called, require many sensor components, and use different combinations of them. It is important to remember that cybersecurity, in addition to functional security, must be maintained throughout the software lifecycle.[68] With the current pace of technological progress, there is a need for a flexible response to these changes and thus for the protection of fundamental rights and freedoms, not only technically but also from a legal point of view. It is important to show the interest of creating the foundations for automated mobility before it becomes a significant element of the road transport. Nowadays, automated driving systems are commonly available in vehicles classified under SAE Level 3, what corresponds to a highly automated vehicle. Germany timelessly regulates SAE level 5 of autonomous driving, even though there are no autonomous vehicles on

[64] § 2 Sec. 2 Subsec. v of the Road Traffic Act No. 8/2009 Coll. [Zákon č. 8/2009 Z. z. o cestnej premávke]

[65] § 2 Sec. 2 Subsec. ae of the Act No. 106/2018 Coll. on the Operation of Vehicles in Road Traffic. [Zákon č. 106/2018 Z. z. o prevádzke vozidiel v cestnej premávke]

[66] § 3 Sec. 4 of the Road Traffic Act No. 8/2009 Coll. [Zákon č. 8/2009 Z. z. o cestnej premávke]

[67] See *Computers on Wheels: Vehicles and Cybersecurity Risks in Europe*. [online]. [s.l.] Carnegie Europe. 24.03.2022. [last accessed 2023-09-09] Available at: https://carnegieeurope.eu/2022/03/24/computers-on-wheels-automated-vehicles-and-cybersecurity-risks-in-europe-pub-86678; *Cars Are Just Software Now*. [online]. [s.l.] Wired, 20.10.2022. [last accessed 2023-09-09]. Available at: https://www.wired.com/story/gadget-lab-podcast-571/

[68] See Para. 7.2.2.1 of UN Regulation No. 155 Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system.

the horizon that reach this level of performance. This may seem like redundant regulation, but Germany is setting the initial legislation for automated and later autonomous mobility in advance. Automated driving systems are now slowly becoming available. There is need to start thinking carefully about how to regulate these technologies without harming neither the potential of new technologies nor society at the same time. There is a need to consider that highly and fully automated vehicles raise entirely different set of regulatory challenges, which should be treated differently.

The proper technical requirements, consistent market surveillance and rigorous analysis of the driver's role in automated vehicles are the fundamental pillars of automated mobility. The technical specifications determine the construction and necessary capabilities of the automated vehicle. Compliance with the technical requirements is monitored by a market surveillance authority. Legal regulation should prevent information asymmetry through asymmetry management to eliminate unfair competition and protect the consumers. This paper discusses, among others, the possible prohibition of market access to the use of the product (automated vehicle) within the European Union's Single Market. Although the definition of the role of the driver's role in automated vehicles is consistent, it does not reflect the needs of today's vehicles alone. The driver's role in automated vehicles needs adjustment.

Bibliography

1. ANDRAŠKO, J. et al. *Právne a technické aspekty kybernetickej bezpečnosti automatizovaných vozidiel*. Bratislava: Wolters Kluwer SR s.r.o., 2022. 160 p. ISBN 978-80-571-0554-1.
2. Act No. 106/2018 Coll. on the Operation of Vehicles in Road Traffic. [Zákon č. 106/2018 Z. z. o prevádzke vozidiel v cestnej premávke]
3. Act No. 575/2001 Coll. on the Organisation of Government Activities and the Organisation of the Central State Administration. [Zákon č. 575/2001 Z. z. o organizácií činnosti vlády a organizácií ústrednej štátnej správy]
4. Act No.429/2022 Coll. amending and supplementing certain laws relating to the development of automated vehicles. [Zákon č. 429/222 Z. z. ktorým sa menia a dopĺňajú niektoré zákony v súvislosti s rozvojom automatizovaných vozidiel]
5. Autonomous Driving Act. BGBl. I p. 986. [Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen]

6. Basic Law for the Federal Republic of Germany. BGBl. I p. 2478. [Grundgesetz für die Bundesrepublik Deutschland]
7. CARIAD launches application store for the Volkswagen Group. [online]
8. Cars Are Just Software Now. [online]
9. Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS).
10. Computers on Wheels: Vehicles and Cybersecurity Risks in Europe. [online]
11. CRAIG, P., DE BURCA, G. *EU Law. Text,* Cases, *and Materials*. 7th Edition. Oxford: Oxford University Press, 2020, 1344 p. ISBN: 9780198856641.
12. Destatis: Verkehrsunfälle 2021, Fachserie 8, Reihe 7, 364 p. ZDB-ID 2168808-4.
13. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive).
14. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2).
15. Erprobungsgenehmigung. [online]
16. Ethik-Kommission: Automatisiertes und Vernetztes Fahren. [online]
17. Explanatory memorandum to Act No.429/2022 Coll. amending and supplementing certain laws relating to the development of automated vehicles. [online]
18. Geneva Convention on Road Traffic.
19. Judgment of the Court of Justice of the European Union C-8/74 *Procureur du Roi v Benoît and Gustave Dassonville* from 11 July 1974.
20. Judgment of the Court of Justice of the European Union C-120/78 *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein* from 20 February 1979.
21. Judgement of the Court of Justice of the European Union C-110/05 *Commision v Italy* from 10 February 2009.
22. Judgement of the Court of Justice of the European Union C-142/05 *Åklagaren v Percy Mickelsson a Joakim Roos* from 4 June 2009.
23. ISO: 26262 - Road vehicles – Functional safety.
24. KEBLER, W. Digital markets, data, and privacy: competition law, consumer law and data protection. In: *Journal of Intellectual Property Law & Practise*. November 2016, Volume 11, Issue 11, p. 856-866.

25. LINDEN, M. Mercedes verkauft Auto-Upgrades per Fingerabdruck. [online]
26. *Marktüberwachung*. [online]
27. Official Journal of the European Union L 245 from 14.09.2013, Volume 56. 32 p. ISSN 1977-0677.
28. OPPERMANN, B. H. et al. *Autonomes Fahren*. München: C. H. Beck, 2020. 501 p. 2. Auf. ISBN 978-3-406-73285-0.
29. Prezídium Policajného zboru, odbor dopravnej polície: Vyhodnotenie dopravno-bezpečnostnej situácie za 12 mesiacov 2021 (definitívne štatistické údaje). [online]
30. Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 from 15.09.2022.
31. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles.
32. Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products.
33. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users (General Safety Regulation).
34. Road Traffic Act. BGBl. I p. 310, 919. [Straßenverkehrsgesetz]
35. Road Traffic Act No. 8/2009 Coll. [Zákon č. 8/2009 Z. z. o cestnej premávke]
36. Road Traffic Licensing Act. BGBl. I p. 679. [Straßenverkehrs-Zulassungs-Ordnung]
37. SAE J3016.
38. SCHWAB, K. The Fourth Industrial Revolution: what it means, how to respond. [online]
39. The 1998 Parallel Agreement.
40. Treaty on Functioning of the European Union.
41. UN Regulation No. 155 Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system.
42. Vienna Convention on Road Traffic.
43. VW-Konzern entwickelt App store. [online]

ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLII
2/2023

AI CYBERSECURITY STANDARDISATION AND ITS OVERLAP WITH DSA AND CRA

JUDr. Michal Rampášek

Comenius University, Faculty of Law
Institute of Information Technology Law and Intellectual Property Law
rampasek1@uniba.sk

Abstract: The provision of digital products and digital services has in common that it integrates more and more artificial intelligence (AI) systems and, above all, the so-called foundation models. Using these elements of artificial intelligence brings several cybersecurity challenges. The key element in achieving the cyber security of digital products and digital services is, firstly, the achievement of a high level of standardization of artificial intelligence and subsequent technical standardization. AI cybersecurity is key to achieving trustworthiness of AI and vice versa. The mentioned facts are also reflected in the latest version of the draft Act on artificial intelligence (AI Act). As part of this paper, the focus is on standardization in the field of cyber security of artificial intelligence and the importance of the foundation models. At the same time the relations of the draft AI Act with the Digital Services Act (DSA) and the draft Cyber Resilience Act (CRA) are highlighted.

Keywords: cybersecurity, standardisation, ai, foundation models, ai act, dsa, cra

Introduction

Innovating digital products and services has become a critical component of business success. Artificial intelligence ("AI") is making significant advances in the way products and services are created and what features they offer to consumers. However, along with

commercial success, the security of such new products and services that integrate AI cannot be forgotten. In this paper, we explore how AI standardization in cybersecurity will support the development of trustworthy digital products and services, by extending the analysis to the draft AI Act[1] together with the draft Cyber Resilience Act ("CRA")[2] and the Digital Services Act ("DSA").[3]

1. Cybersecurity of AI

Cybersecurity of AI-featured digital products and services reaches far beyond the usual protection of digital assets. Cybersecurity is also considered instrumental to the correct implementation of trustworthiness features of AI, and vice versa, the correct implementation of trustworthiness features is key to ensuring cybersecurity.[4]

What is the cybersecurity of AI more specifically? Considering various interpretations, in a broader sense it complements protection of the confidentiality, integrity and availability of assets across the life cycle of an AI system, with trustworthiness features such as data quality, oversight, robustness, accuracy, explainability, transparency and traceability.

AI assets include machine learning („ML") models and algorithms, together with training data sets. ML techniques and algorithms are predominant in current AI systems or applications.

The real change of paradigm in building AI systems, or applications, however, came with development of large ML models, known as *foundation* models.

---

[1] In wording of amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), [cit. 4 September 2023] available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

[2] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (12429/22, COM(2022)454 final) known as the Cyber Resilience Act

[3] 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 (Digital Services Act)

[4] European Union Agency for Cybersecurity (ENISA). Cybersecurity of AI and Standardisation (Report). March 2023, p. 6. [cit. 31 August 2023] Available at: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation/@@download/fullReport

2. Foundation models

The Stanford Institute for Human-Centered Artificial Intelligence's Center for Research on Foundation Models introduced the term "foundation model" in 2021.[5] A foundation model is a large ML model that is trained on broad data, generally using self-supervised learning at scale, that can be adapted (fine-tuned) to a wide range of downstream tasks.[6] AI systems with specific intended purpose or general-purpose AI systems can be developed by using a general foundation model at their core, which means that each foundation model can be reused in countless downstream AI systems and products. Indeed, foundation models are fine-tuned to create customer-facing apps. For example, OpenAI's ChatGPT and GPT-4 have become the basis for many chatbots and applications requiring human language understanding.

From a technological point of view, foundation models predate 2021 — they are based on deep neural networks (a class of ML models), self-supervised learning and transfer learning algorithms, and large-scale datasets. Progress in research, engineering and supercomputing, particularly in scaling of these methods to ever larger training datasets and resulting models, led to an inflection point, when these models began to manifest emergent capabilities and became more generally reusable. Their effectiveness across so many tasks stimulates homogenization, with these models serving as the foundation to build upon.

Emergence and homogenization are therefore key traits of foundation models. However, the characteristics of current ML algorithms and of the training data, that are not fully annotated and vetted by humans, also lead to a degree of opacity. A resulting model emerges from the training procedure rather than being explicitly prescribed by the creators. It may exhibit emergent properties and capabilities, both good and bad, that were not anticipated. For example, a model trained on a large natural language dataset may learn to write its own stories without being explicitly programmed to do so, but may also acquire harmful biases or hallucinate false facts. Homogenization means useability across many domains. This allows significant progress, but also introduces the possibility of failure across different applications due to a single deficiency in the underlying model.

[5] Bommasani, R. et al.: On the opportunities and risks of foundation models (2021) [cit. 31 August 2023] available at: https://crfm.stanford.edu/report.html

[6] Ibid

Existing foundation models have been demonstrated to be particularly effective in fields such as Natural language processing and Computer vision with foundation models such as GPT-3 and 4, BERT, PaLM-2, Llama-2, Stable Diffusion, DALL-E 2. Most recent foundation models work with multiple data types. They are multimodal, meaning they can process information in not only text format, but also pictures or even videos. Foundation models can be applied to a wide range of industries, including healthcare, education, translation, social media, law, and more. Use cases that exist in all those industries include content creation, text summarization, translation, answering questions, image generation & classification, etc.[7]

Foundation models are distributed both as proprietary as well as open-source, while they may differ along key dimensions such as cost structure, time-to-market, latency, flexibility and transparency, and security and governance. In respect to the security and governance of large language models and generative models there exist large gaps. Proprietary and open-source models both exhibit risks in different aspects. Proprietary models offer added security and governance capabilities that open-source models lack. Although open-source models lack security and governance capabilities, they can be brought within businesses' security perimeter and securely fine-tuned on local data. That is why many enterprises avoid using or fine-tuning proprietary models.[8]

Despite the widespread deployment of foundation models, more research will be required since we currently lack a clear understanding of how these models work, when they fail, and what they are even capable of due to their emergent properties.[9]

From regulatory perspective, the foundation models are now being strongly focused on in the new draft AI Act.

[7] Dilmegani, C.: Foundation Models: Definition, Applications & Challenges in 2023, last updated 22 December 2022 [cit. 4 September 2023] available at: https://research.aimultiple.com/foundation-models/

[8] Lu. S,: Proprietary vs. Open Source Foundation Models, 15 May 2023, [cit. 5 September 2023] available at: https://tolacapital.com/2023/05/15/foundationmodels/

[9] Bommasani, R. et al.: On the opportunities and risks of foundation models (2021) [cit. 4 September 2023] available at: https://crfm.stanford.edu/report.html

3. AI Act

The draft AI Act states that cybersecurity is an important element of the requirement to ensure that high-risk AI systems are trustworthy and resilient against cyberattacks.

These high-risk systems are subject to a number of requirements, cybersecurity being one of them.[10] It follows that high-risk AI systems shall be designed and developed following the principle of security by design and by default.[11] The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training dataset ("data poisoning"), or pre-trained components used in training ("model poisoning"), inputs designed to cause the model to make a mistake ("adversarial examples" or "model evasion"), confidentiality attacks or model flaws, which could lead to harmful decision- making.

Generally, the draft AI Act permits high-risk AI systems subject to compliance with AI requirements and ex-ante conformity assessment.

The draft AI Act introduces presumption of conformity of AI systems, stating that high-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to the Cybersecurity Act[12] shall be presumed to be in compliance with the cybersecurity requirements set out in Article 15 of the AI Act, where applicable, in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.[13]

ENISA stresses the importance of the inclusion of cybersecurity aspects in the risk assessment of high-risk systems in order to determine the cybersecurity risks that are specific to the intended use of each system, as well as the lack of standards related to the cybersecurity of artificial intelligence to cover performing conformity assessments.[14]

---

[10] AI Act , Article 15

[11] AI Act, Article 15 par. 1

[12] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[13] AI Act, article 42 par. 2

[14] European Union Agency for Cybersecurity (ENISA). Cybersecurity of AI and Standardisation (Report). March 2023, p. 6. [cit. 31 August 2023] Available at: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation/@@download/fullReport

Together with the high-risk AI systems, the new draft AI Act expressly defines the foundation models[15] and focuses on obligations of providers of foundation models.[16]

In general, foundation models will not be classed as "high-risk" AI systems – unless they are directly integrated in such a high-risk AI system.[17] The obligations on providers of foundation models would apply regardless of whether the model is provided on a standalone basis or embedded in an AI system or a product. Foundation models would need to be also registered in an EU database.

The draft AI Act considers essential to clarify the legal situation of providers of foundation models. Foundation models should be subject to proportionate and more specific requirements including cybersecurity.

The providers would be obliged to „demonstrate through appropriate design, testing and analysis that the identification, the reduction and mitigation of reasonably foreseeable risks to health, safety, fundamental rights, the environment and democracy and the rule of law prior and throughout development", as well as draw up "extensive technical documentation and intelligible instructions for use" to help those that build AI systems using the foundation model to meet their own legal obligations.[18] They would further be required to meet obligations around data governance, ensure "appropriate levels" of performance, predictability, safety and cybersecurity, and conform to a range of sustainability standards.

Those providers of foundation models which are used in generative AI would face further obligation relating to transparency over when content has been created by an AI system and not a human and making publicly available a sufficiently detailed summary of the use of training data protected under copyright law.

Stanford researchers evaluated compliance of 10 major foundation model providers with draft AI Act requirements and found that they largely do not comply.[19] Foundation model providers rarely disclose adequate information regarding the data, compute, and deployment of

[15] AI, Act, recitals 60e to 60h, Article 3 par. 1 point 1c

[16] AI Act, Article 28b

[17] Cameron, S., Scanlon, L.: MEPs' EU AI Act proposals focus on 'foundation models' [cit. 4 September 2023] available at: https://www.pinsentmasons.com/out-law/news/meps-eu-ai-act-foundation-models

[18] AI Act, Article 28b

[19] Bommasani, R. et al.: Do Foundation Model Providers Comply with the Draft EU AI Act? [cit. 4 September 2023] available at: https://crfm.stanford.edu/2023/06/15/eu-ai-act.html

their models as well as the key characteristics of the models themselves. In particular, foundation model providers generally do not comply with draft requirements to describe the use of copyrighted training data, the hardware used, and emissions produced in training, and how they evaluate and test models.

Further, insightful is the comparison of different release strategies of foundation models. Open-source releases generally achieve strong scores on resource disclosure requirements (both data and compute), however, make it challenging to monitor or control their deployment. On the other hand, more restricted proprietary releases achieve better scores on deployment-related requirements, but tend to fall behind in resource disclosure. Open-sourcing a model makes it much more difficult to monitor or influence downstream use, whereas APIs or developer-mediated access provide easier means for structured access.[20]

It their conclusions Stanford researchers recommend[21] that foundation model providers should work towards industry standards that will help the overall ecosystem become more transparent and accountable.

4. Standardisation and Cybersecurity of AI

Standardisation should play a key role to provide technical solutions to providers to ensure compliance with the AI Act.

These standards have to be consistent and aimed at ensuring that AI systems or foundation models placed on the market or put into service in the Union meet the relevant requirements.[22]

The high-risk AI systems and foundation models which would be in conformity with such harmonised standards would be presumed to be in conformity with the requirements set in the AI Act.

Indeed, the Commission adopted Implementing decision[23] and requested the European Committee for Standardisation ("CEN") and the European Committee for Electrotechnical Standardisation

[20] Ibid

[21] Ibid

[22] AI Act, article 40 par. 1b

[23] Commission implementing decision of 22 May 2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence („Implementing decision") [cit. 4 September 2023] available at: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en

("CENELEC") to draft the new European standards or European standardisation deliverables, as listed in Annex I of the Implementing decision. The Implementation decision forms the basis for development of future 10 harmonised European standards:

1. Risk management systems for AI systems
2. Governance and quality of datasets used to build AI systems
3. Record keeping through logging capabilities by AI systems
4. Transparency and information provisions for users of AI
5. Human oversight of AI systems
6. Accuracy specifications for AI systems
7. Robustness specifications for AI systems
8. *Cybersecurity specifications for AI systems*
9. Quality management systems for providers of AI systems, including post-market monitoring processes
10. Conformity assessment for AI systems

The role of cybersecurity is within all sets of requirements that can be considered as referring to the trustworthiness of an AI ecosystem.

The current state in the field of standardisation related to cybersecurity of AI is influenced by the fact that some aspects of cybersecurity are still the subject of research and development, and therefore might not be mature enough to be standardised.

In common, existing general purpose technical and organisational standards (such as ISO-IEC 27001 and ISO-IEC 9001) can contribute to mitigating some of the risks faced by AI.

There are only a few existing specific standards related to the cybersecurity of AI, most of them are still being drafted or are under consideration and planned. One of the most notable is the US National Institute of Standards and Technology ("NIST") AI Risk Management Framework (AI RMF 1.0).[24]

CEN/CENELEC has identified a list of standards from International Organization for Standardization ("ISO") and International Electrotechnical Commission ("IEC"), that are of interest for AI cybersecurity and might be adopted/adapted by CEN-CENELEC based on their technical cooperation agreement. Identified standards include the ISO 27000 series on information security management systems, which may be complemented by the ISO 15408 series for the

[24] US National Institute of Standards and Technology (NIST). AI Risk Management Framework (AI RMF 1.0). [cit. 31 August 2023] available at: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

development, evaluation and/or procurement of IT products with security functionality, as well as sector-specific guidance.[25]

In addressing the extended scope of cybersecurity of AI, which includes trustworthiness characteristics, data quality, AI governance, AI management systems, etc., following standards has been identified as having direct applicability to the draft AI Act and is being considered for adoption/adaption by CEN/CENELEC:

- ISO/IEC 22989:2022, Artificial intelligence concepts and terminology (published),
- ISO/IEC 23053:2022, Framework for artificial intelligence (AI) systems using machine learning (ML) (published),
- ISO/IEC DIS 42001, AI management system (under development),
- ISO/IEC 23894, Guidance on AI risk management (publication pending),
- ISO/IEC TS 4213, Assessment of machine learning classification performance (published),
- ISO/IEC FDIS 24029-2, Methodology for the use of formal methods (under development),
- ISO/IEC CD 5259 series: Data quality for analytics and ML (under development).[26]

As noted above, it is likely that CEN and CENELEC will transpose standards from ISO and IEC, respectively, to future European standards to ensure compliance with the AI Act.

There are still standardisation gaps, thus we can expect further standards regarding AI systems risk catalogue and risk management, and AI trustworthiness characterisation (e.g., robustness, accuracy, safety, explainability, transparency and traceability). However, it is likely that additional standardisation gaps and needs may become apparent only as the AI technologies advance.

5. AI Act vs. DSA

The high-risk AI systems and foundation models hold growing importance to many downstream applications and systems, having direct impact also to digital services and digital products, as such

[25] European Union Agency for Cybersecurity (ENISA). Cybersecurity of AI and Standardisation (Report). March 2023, p. 12. [cit. 31 August 2023] Available at: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation/@@download/fullReport

[26] Ibid, p. 13

services or products may be classified, composed of, or use high-risk AI systems or foundation models. In other words, regulation and future cybersecurity standardisation of AI systems and foundation models will have a direct impact also on digital services regulated under the DSA, in particular online platforms, as well as on digital products that would be regulated under the CRA.

The DSA establishes harmonised rules for the online environment, aiming to ensure security, predictability, and trust by introducing mechanisms for the protection of the fundamental rights. The act regulates obligations of digital services that act as intermediaries in their role of connecting consumers with goods, services, and content. In particular sales platforms, social networking platforms, very large online platforms ("VLOPs") and very large online search engines ("VLOSEs"). The rules are designed asymmetrically, so that larger intermediary services with significant societal impact (VLOPs and VLOSEs) are subject to stricter rules.

The draft AI Act follows the above-mentioned stricter rules for VLOPs stating that AI systems used by those online platforms in their recommender systems would comply with the requirements laid down under the AI Act, including the technical requirements on data governance, technical documentation and traceability, transparency, human oversight, accuracy and robustness. Compliance with the AI Act should enable such VLOPs to comply with their broader risk assessment and risk-mitigation obligations in Article 34 and 35 of the DSA.[27]

AI systems intended to be used by social media platforms designated as VLOPs, in their recommender systems to recommend to the recipient of the service user-generated content available on the platform are newly expressly included to the high-risk systems category in the draft Annex III of the AI Act.

The DSA imposes transparency reporting obligations for providers of intermediary services (other than micro or small enterprises), in particular to make publicly available, in a machine-readable format and in an easily accessible manner, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period.[28] That includes any use made of automated means for the purpose of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the

[27] AI Act, recital 40b

[28] DSA, Article 15

accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied.

VLOPs and VLOSEs are subject to enhanced transparency obligations, including annual independent audits to assess their compliance with their obligations.[29]

In this respect it is worth noting also the Commission's draft delegated regulation laying down rules on the performance of audits for very large online platforms and very large online search engines („Audit rules").[30]

The purpose of the Audit rules is to set out the necessary rules for the procedures, methodology and templates used for the audits of VLOPs and VLOSEs as required under Article 37 of the DSA.

The Audit rules pay attention inter alia to auditing methodologies for algorithmic systems. In its explanatory note the Audit rules stress that algorithmic systems such as *advertising systems, content moderation technologies, recommender systems* and other functionalities used by online platforms and search engines relying on novel technologies such as generative models (i.e. foundation models) are particularly important elements to analyse when assessing compliance with risk assessment and risk mitigation obligations.

6. AI Act vs. CRA

The draft CRA aims to impose cybersecurity obligations on all products with digital elements (digital products) meaning any software or hardware product and its remote data processing solutions, including software or hardware components if placed on the market separately.[31] The regulation impacts a broad scale of products including critical products such as browsers, password managers, virtual private networks, operating systems, firewalls, IDS/IPS, routers, switches, smart cards, etc. This piece of horizontal legislation introduces cybersecurity by design and by default principles and imposes a duty of care for the lifecycle of products. The act also covers AI systems,

[29] DSA, Article 37

[30] Draft Commission Delegated Regulation (EU) supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines (2023), [cit. 4 September 2023] Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits_en

[31] Draft CRA, Article 3 par. 1

including the cybersecurity of products with digital elements that are classified as high-risk AI systems.

Manufacturers of digital products would have to ensure that digital products comply with essential cybersecurity requirements and conformity assessment procedures before placing them on the market. Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks, without any known exploitable vulnerabilities.

The Commission's Implementing decision[32] in European standards/standardisation deliverables on Cybersecurity specifications for AI systems expressly mention the draft CRA, stating that *these standards shall take due account of the essential requirements for products with digital elements as listed in Sections 1 and 2 of Annex I to the CRA.*[33]

The CRA introduces the presumption of conformity, stating that products with digital elements classified as high-risk AI systems fulfilling the requirements of the CRA (Annex I), shall be deemed in compliance with the cybersecurity requirements of the AI Act.[34]

Conclusions

Wave of AI in recent years is attributable mainly to the foundation models. Although AI is not just about foundation models, it is their utility that accelerates AI's potential as a general-purpose technology with broad applicability throughout the whole economy. While the potential benefits are enormous, it is important not to overestimate the capability of foundation models.

Firstly, it is inevitable to support international and European standards development work focused on establishing common definitions, specifications for risk management systems, risk classification criteria, and other elements of effective cybersecurity of AI. Work on the AI-related standards has already begun, however

[32] Commission implementing decision of 22 May 2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence („Implementing decision") available at: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en

[33] Ibid, Annex II, point 2.8

[34] Draft CRA, Article 8 par. 1

standards most likely will not be ready before the regulation enters into force.

In the AI regulation a risk and context-based approach remains the most effective strategy to minimize the risks of all AI, including those posed by foundation models. Following the results of the Stanford research cited above, we believe that the AI Act should consider additional critical factors to ensure adequate transparency and accountability of foundation model providers, including the disclosure of usage patterns. Such requirements would mirror transparency reporting for online platforms under the DSA. To avoid overburdening micro and small size companies these requirements should apply only to the foundation model providers that have a significant societal and economic impact.

Bibliography

1. BOMMASANI, R. et al.: *On the opportunities and risks of foundation models* (2021). 5 September 2023. [online], URL: https://crfm.stanford.edu/report.html
2. BOMMASANI, R. et al.: *Do Foundation Model Providers Comply with the Draft EU AI Act?* 5 September 2023. [online], URL: https://crfm.stanford.edu/2023/06/15/eu-ai-act.html
3. CAMERON, S., SCANLON, L.: *MEPs' EU AI Act proposals focus on 'foundation models'.* 4 September 2023. [online], URL: https://www.pinsentmasons.com/out-law/news/meps-eu-ai-act-foundation-models
4. DILMEGANI, C.: *Foundation Models: Definition, Applications & Challenges in 2023*, last updated 22 December 2022. 4 September 2023. [online], URL: https://research.aimultiple.com/foundation-models/
5. European Union Agency for Cybersecurity (ENISA). *Cybersecurity of AI and Standardisation (Report)*. March 2023, 4 September 2023. [online], URL: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation/@@download/fullReport
6. European Union Agency for Cybersecurity (ENISA). *Securing Machine Learning Algorithms* (Report). December 2021, 4 September 2023. [online], URL: https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms
7. European Union Agency for Cybersecurity (ENISA). *Standardisation in support of the Cybersecurity Certification*. February 2020, 4 September 2023. [online], URL: https://www.enisa.europa.eu/

publications/recommendations-for-european-standardisation-in-relation-to-csa-i
8. LU. S,: *Proprietary vs. Open Source Foundation Models*, 15 May 2023. 5 September 2023. [online], URL: https://tolacapital.com/2023/05/15/foundationmodels/
9. Proposal for the Regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) in wording of amendments adopted by the European Parliament on 14 June 2023, 4 September 2023. [online], URL: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html
10. Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (12429/22, COM(2022)454 final) (Cyber Resilience Act) 4 September 2023. [online], URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454
11. 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 (Digital Services Act)
12. Commission implementing decision of 22 May 2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence, 4 September 2023. [online], URL: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en
13. Draft Commission Delegated Regulation (EU) supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines (2023), 4 September 2023. [online], URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits_en
14. US National Institute of Standards and Technology (NIST). AI Risk Management Framework (AI RMF 1.0). 31 August 2023. [online], URL: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLII
2/2023

REGULATION OF DIGITAL HEALTHCARE SERVICES – (NOT) COVERED UNDER THE DIGITAL SERVICES ACT?

doc. JUDr. Soňa Sopúchová, PhD.

Comenius University in Bratislava, Faculty of Law
Institute of Information Technology Law and Intellectual Property Law
sona.sopuchova@flaw.uniba.sk

Abstract: The regulation of digital services is currently experiencing significant growth, primarily due to the adoption of new legal regulation at the European Union level, specifically the Digital Services Act. Digital services play a pivotal role in a country's economy by facilitating cross-border trade and enabling entrepreneurs to reach a vast user base, often comprising consumers. Despite their advantages, these services also entail substantial risks, particularly in relation to their widespread and more challenging-to-regulate usage. Alongside their positive impact, they also contribute significantly to the dissemination of illegal and harmful information. In recent years, there has been a notable development and utilization of new electronic information systems within the healthcare sector, accompanied by electronic healthcare services. This connection is not limited to the Covid-19 pandemic but is also a result of the dynamic evolution of information and communication technologies and their potential in healthcare provision. In this paper, the author analyzes the research question regarding which digital healthcare services in the Slovak Republic fall within the scope of the new European legislation. The author examined European regulations, focusing on the types of electronic healthcare services existing in Slovakia. By synthesizing and applying available information and rules to selected electronic healthcare services, the study concludes that the Digital Services Act has only a limited impact on the functioning of these selected digital healthcare services.

Keywords: electronic healthcare services, e-Health, healthcare digitization, digital healthcare services

Introduction

In 2022, the European Parliament and the Council of the European Union adopted a new legal regulation known as the Digital Services Act[1]. Its primary aim is to contribute to the proper functioning of the internal market for intermediary services by creating harmonized rules to establish a safe, predictable, and trustworthy online environment. This environment seeks to foster innovation while effectively protecting fundamental rights, including the principle of consumer protection.[2] The Digital Services Act is a long-awaited piece of legislation intended to regulate digital services meeting specific criteria. Simultaneously, in the same year, a month earlier, another legal regulation was adopted, also in the form of a regulation, known as the Act on Digital Markets.[3] This regulation establishes common rules to create competitive and fair digital sector markets for the benefit of all users across the European Union.[4] These two pieces of legislation have introduced significant changes to the digital services sector, affecting all digital service providers falling under their regulatory scope throughout the European Union.

The objective of this paper is to analyze and draw concrete conclusions regarding which digital healthcare services are subject to the new regulation and the corresponding requirements that apply to them. The rationale for selecting this research question arises from the dynamic nature of the development and implementation of electronic healthcare services. These services encompass a wide range of aspects, including electronic patient records containing personal data, online healthcare portals, virtual assistants, platforms for patient appointment booking, and healthcare professional reviews, among others. The research delves into the broader regulatory framework for these digital services, emphasizing aspects such as cybersecurity, data protection, privacy, and artificial intelligence.

In this paper, we formulate a fundamental hypothesis: digital healthcare services cannot be unequivocally categorized or aligned with

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the single market for digital services and amending Directive 2000/31/EC (Digital Services Act).

[2] Article 1, paragraph 1 of the Digital Services Act.

[3] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on competitive and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[4] Article 1, paragraph 1 of the Digital Markets Act.

the provisions of the Digital Services Act, resulting in a scattered legal regulation landscape within the Slovak Republic.

To provide context, it is essential to clarify the legal terminology prevalent in this field, as it may give rise to ambiguity in its correct usage. With the widespread adoption of information and communication technologies (ICT)[5] in various spheres of life, terms like "**informatization**" and "**electronicization**" have emerged. While they share similar content, they are not synonyms. Informatization emphasizes processing information using ICT, whereas electronicization is a narrower term, focusing on the introduction and utilization of electronic ICT in all activities. Another term often encountered is "**digitalization**," which involves the conversion of material content into a form processed by information and communication technologies. Subsequently, terms such as "**information service**," "**electronic service**," or "**digital service**" may also be encountered. The term "**electronic service**" is quite general and we find several theoretical explanations for its definition. Author Boyer defines electronic services as "*interactive services that are provided on the Internet using modern telecommunications, information and multimedia technologies*."[6]

In addition to theoretical distinctions among these terms, local legislation further defines specific technical terminology in the field of information technology from a legal perspective. For instance, "information technology" and "information system" are defined in Act no. 95/2019 Coll. on information technologies in public administration (referred to as the "Act on ITVS"). According to this law, information technology encompasses means or procedures used to process data or information in electronic form, including information systems, infrastructure, information activities, and electronic services.[7] An

[5] ICT are defined in many sources, e.g. UNESCO. *Developing and Using Indicators of ICT Use in Education*. Bangkok: UNESCO Asia and Pacific Regional Bureau for Education, 2003, p. 7.: "*Information technology is understood as a term used to describe the elements of equipment (hardware) and computer programs (software) that enable us to access, retrieve, store, organize, manipulate and present information electronically. The category of hardware includes personal computers, scanners or digital cameras. Data storage programs and multimedia programs can be included in the software category. Communications technology is seen as a term used to describe telecommunications equipment through which information can be made available. This is mainly about telephones, faxes or television."*

[6] BOYER, K., HALLOWELL, R., ROTH, A. V. *Eservices: operating strategy – a case study and a method for analyzing operational benefits*. In: Journal of Operations Management. 2002, vol. 58, ed. 2, p. 175.

[7] Provision § 2 par. 1 of the Act on ITVS.

information system, as an example of information technology, represents a functional unit that ensures purposeful and systematic information activity through technical and programmatic means.[8]

While the aforementioned law does not explicitly address the term "**communication technology**," the legislator includes communication technology under information technology, given that part of information technology focuses on information activity, including data acquisition, processing, making available, transmission, archiving, and disposal.[9] In practice, the term "**digital technology**" is also used to refer to electronic technology that creates, transmits, and processes data and information using binary code (ones and zeros), with each unit referred to as a "bit."

It is noteworthy that despite its title, the Digital Services Act does not provide a precise definition of the concept of digital services. Instead, it outlines the content of terms such as "**information society service**" and "**intermediary service**." These terms will be elucidated further in subsequent sections of the paper. For the purposes of this paper, the foundational terminological thesis to consider is that informatization, electronicization, and digitalization share a common denominator: information and communication technologies. These activities primarily occur through the use of ICT, often within the virtual realm of cyberspace and frequently via the global Internet.

Digital services in healthcare

Following the clarification of terms, it is evident that both European and Slovak strategic and legislative documents employ the term "**electronic health services**" to refer to health services provided electronically using information and communication technologies. We argue that these services can also be referred to as "**digital services**" since they rely on electronic technology operating based on binary code, a form that can be processed by computers, one of the most prevalent information and communication technologies. Consequently, in the subsequent sections of this paper, we will use these terms interchangeably depending on the context, but they will always pertain to services within the realm of electronic healthcare, commonly referred to as e-Health. The term “e-Health” conceptually includes all aspects of

[8] Provision § 2 par. 2 of the Act on ITVS.
[9] Provision § 3 letter a) of the Act on ITVS.

health, not only health care or healthcare, for example, individual health promotion measures, perhaps in homes, medical facilities or schools.[10]

The development and implementation of digital healthcare services represent a prominent trend in the contemporary world. However, certain prerequisites must be met to enable the development and utilization of digital services. These prerequisites include political will for their introduction, the provision of electronic identification and authentication capabilities for users and service providers, the necessary hardware and software infrastructure, access to the Internet, an online portal encompassing essential information, forms, and service access, and, importantly, information systems from which data is derived to support individual electronic services.[11]

Based on an examination of national strategic documents, legislation, and other sources, including European Union programs and non-legislative legal information available on professional websites[12], we present the following overview of digital healthcare services in the Slovak Republic:

- **E-health** – National health portal,
- **Electronic health book**,
- **Patient summary**,
- **E-ordering** – electronic appointment booking with healthcare professionals,
- **E-prescription** – electronic prescriptions for medicines, medical devices, and dietetic foods,
- **E-examination** – electronic recording of medical examinations,
- **E-vaccination** – electronic vaccination records,
- **E-lab** – electronic records of laboratory examination results,
- **E-PN** – electronic confirmation of temporary incapacity for work,
- **E-birth** – electronic notification of child births,
- **My Health application**,
- **eAlerts application**[13].

[10] STŘEDA, L., HÁNA, K. *eHealth a telemedicine.* Prague: Grada Publishing, 2016, p. 14.

[11] ANDRAŠKO, J. et al. *Regulatory challenges of e-Government in the Slovak Republic in the context of European Union law*. Prague: Wolters Kluwer CR, 2022, p. 286.

[12] For example, the eHealth portal operated by the National Center for Health Information.

[13] More information about digital healthcare services in the Slovak Republic: SOPÚCHOVÁ, S. *Electronic healthcare in the Slovak Republic. E-Health and telemedicine*. Bratislava: Wolters Kluwer, 2022.

These services are provided to natural persons, including citizens of the Slovak Republic and foreigners who are part of the national social and health system. They also offer advantages to healthcare providers and professionals. The mentioned services are administered by the state in accordance with legislation.

In addition to these services, the private sector also provides other electronic services in the healthcare sector. These services primarily include:

- **Online appointment booking with healthcare professionals,**
- **Virtual consultations with healthcare professionals,**
- **Provision of professional articles,**
- **Healthcare professional´s evaluation.**

1.1 Scope of the Digital Services Aut

The scope of the Digital Services Act is defined in Article 2, paragraph 1, with the modification that it applies to intermediary services offered to recipients of services residing in or located within the European Union, regardless of the location of the service providers.[14] The Digital Services Act imposes several obligations on providers of intermediary services, subject to the harmonization rules of the European Union concerning its member states. The objective is to "ensure a safe, predictable, and trustworthy online environment, combat the dissemination of illegal content on the Internet, mitigate societal risks associated with disinformation or other content, and effectively safeguard fundamental rights enshrined in the charter while fostering innovation."[15] Consequently, the regulation establishes conditions conducive to the development of innovative digital services and their expansion within the internal market. However, it is important to acknowledge that the increased usage of these services, even for legitimate and beneficial purposes, has also led to a rise in the dissemination of illegal or harmful information and activities.

It is evident that the Digital Services Act introduces a new term into legal usage, namely "**intermediary service**," which it defines within its glossary of terms. An integral part of this definition is the concept of an "**information society service**." Therefore, we conclude that the Digital Services Act applies exclusively to providers of specific information

[14] Article 2, paragraph 1 of the Digital Services Act.
[15] Recital (9) of the Digital Services Act.

society services, specifically intermediary services. Our analysis suggests that it is necessary to first clarify the concept of "information society services" and subsequently delve into the definition of "intermediary services." While the original definition of information society services can be found in another legislative act of the European Union, the term "intermediary services" is primarily used within the context of the Digital Services Act.[16]

Information society service constitute a significant segment of the European Union's economy and the daily lives of its citizens. All services provided within the realm of the information society can be categorized as such, encompassing services typically offered for a fee, delivered remotely, electronically, and in response to individual requests from service recipients.[17] This definition is further enriched by specific defining characteristics that merit reproduction:

- "*remotely*" signifies that the service is provided without both parties being physically present at the same location,
- "*by electronic means*" indicates that the service is transmitted from the point of origin to the destination using electronic equipment designed for data processing (including digital compression) and storage, with the entire transmission occurring via wire, radio waves, optical means, or other electromagnetic methods,
- "*based on the individual request of the recipient of the services*" implies that the service is provided through data transfer initiated by the individual recipient's request.[18]

In addition to the positive definition of information society services, Directive 2015/1535 of the European Parliament and the Council of the European Union, which establishes the procedure for providing information related to technical regulations and rules governing information society services, includes an indicative list of services that do not fall under this term.

Returning to the concept of intermediary services, which we categorize broadly as information society services, the second part of

[16] The Digital Markets Act defines the term "online intermediary services", which it includes among basic platform services.

[17] Article 1, paragraph 1, letter b) Directive 2015/1535of the European Parliament and the Council of the European Union, which establishes the procedure for providing information in the field of technical regulations and rules relating to information society services.

[18] Article 1, paragraph 1, letter b) Directive 2015/1535 of the European Parliament and the Council of the European Union, which establishes the procedure for providing information in the field of technical regulations and rules relating to information society services.

their definition is found within the Digital Services Act itself. Intermediary services, as a subset of information society services, encompass services that:

a) transmit information provided by the service recipient through a communication network or provide access to a communication network, which constitutes "**ordinary transmission**" services.
b) transfer information provided by the service recipient through a communication network, temporarily and automatically storing it solely to facilitate its subsequent transmission to other recipients upon their request, constituting "**caching**" services.
c) store information provided by the service recipient upon their request, in which case they are referred to as "**hosting**" services.[19]

All three categories of intermediary services involve the transmission or storage of information provided by the service recipient. Consequently, they are subject to the liability of providers for foreign content. The Digital Services Act delineates provider liability by specifying under what circumstances they are not liable. Furthermore, the act imposes various obligations on these providers, including duties of due care to foster a transparent and safe online environment. It is worth noting that Directive 2000/31/EC of the European Parliament and the Council on certain legal aspects of information society services in the internal market, particularly regarding electronic commerce, addresses the liability of intermediaries and service providers. This directive, established in 2000, was transposed into Slovak law by Act no. 22/2004 Coll. on electronic commerce and amendments and additions to Act no. 128/2002 Coll. on state control of the internal market concerning consumer protection and amendments and supplements to various laws, as amended by Act no. 284/2002 Coll.

1.2 Digital healthcare services and the Digital Services Act

The effective operation of state digital healthcare services and e-Health applications necessitates several technical and legal instruments, primarily established by Act no. 153/2013 Coll. on the National Health

[19] Article 3, letter g) Digital Services Act.

Information System and on amendments and additions to certain laws (hereinafter referred to as the "NHIS Act"). These services are further supported by other legally binding regulations and by-laws. Key tools for digital healthcare services include the National Healthcare Information System, the citizen's electronic identity card, electronic proof of residence for foreigners, electronic ID cards for healthcare professionals, and health informatics standards.

The primary research objective stated in the introduction of this paper is to determine whether the Digital Services Act is applicable to the existing digital healthcare services in the Slovak Republic or if the regulation represents a new framework for governing these services.

The initial question we must address is whether the digital healthcare services qualify as services of the information society. Subsequently, we need to assess whether they fall under the category of intermediary services. This evaluation is conducted in connection with both the positive and negative definitions of information society services.

As previously mentioned, information society services, according to the positive definition, encompass all services provided by an information society, typically offered for a fee, delivered remotely, electronically, and in response to the individual request of the service recipient. The negative definition, found in Annex I of Directive 2015/1535, specifies certain services that do not exhibit all the defining characteristics of an information society service. The issue at hand pertains to examples like a medical examination or treatment in a healthcare clinic, which, despite the potential use of electronic equipment, involve the physical presence of the patient and thus do not qualify as services provided at a distance. Furthermore, services such as consultations with a doctor via telephone are not considered services provided electronically. Consequently, medical examinations, treatments, and phone consultations with a doctor do not constitute information society services due to the absence of some defining features.

It is important to note that the list of services that do not qualify as information society services is merely indicative. Digital healthcare services provided in the Slovak Republic do not appear on this list, necessitating an assessment based on the positive definition of an information society service. Despite being offered remotely and electronically, these services are not typically fee-based and may not always align with individual requests from service recipients. Therefore, we assert that none of the digital healthcare services

provided by the state qualify as information society services. Consequently, considering the above, they also do not qualify as intermediary services since they fail to meet the fundamental requirement of being an information society service.

1.2.1 Digital healthcare services provided by private sector

Within the realm of electronic healthcare provision, especially in fields like telemedicine and robotics, dynamic developments are underway, driven significantly by the widespread adoption of artificial intelligence. These innovations are making significant inroads in the healthcare sector, not excluding the direct provision of healthcare services.

In addition to digital services covered by the state and constituting the e-Health initiative in Slovakia, the private sector offers supplementary healthcare services. These services lack official recognition, names, or inclusion in the e-Health project. Upon analyzing the online landscape, these services can be categorized into several levels:

- Online appointment booking with healthcare professionals,
- Virtual consultations with healthcare professionals,
- Provision of professional articles,
- Healthcare professional´s evaluation.

Since many of these services are typically provided through a single website, we will examine them collectively as a package of services. The services are notably diverse, encompassing online healthcare consultations (akin to telemedicine), appointment booking for precise doctor visits, and doctor evaluation services with attributes of an information society service. In the following section, we delve into an analysis of these digital services.

Online appointment booking with healthcare professionals

Private portals within the healthcare sector (hereinafter referred to as "private healthcare portals") offer the option of booking appointments with healthcare professionals for a fee. Considering the additional attributes of information society services, we assert that the service constitutes an information society service. This classification is based on several factors, including the service's fee-based nature, remote delivery through electronic means, and its provision upon individual request by the recipient.

This service does not involve the mere transmission of information provided by the service recipient via communication networks or providing access to such networks. It also does not entail the automatic, temporary storage of recipient-provided information for streamlining further transmission to other recipients upon their request. Moreover, it does not encompass the storage of information provided by the service recipient upon their request. From these considerations, it becomes evident that booking patient appointments with specific healthcare professionals via the Internet does not fall within the scope of an intermediary service as defined in the Digital Services Act.

Nevertheless, a pertinent question remains for further research: What is the legal basis for this type of appointment booking service? This inquiry arises because Act no. 576/2004 Coll. on healthcare, services related to healthcare provision, and the amendment of certain laws (hereafter referred to as the "Health Care Act") governs the legal framework for booking appointments. The Health Care Act allows for the possibility of booking free appointments with healthcare professionals from a waiting list during regular office hours or, alternatively, the option of booking appointments during extended office hours for a fee, with a maximum charge of EUR 30.[20] This service is delivered through a state-provided digital E-ordering system.[21]

Virtual consultations with healthcare professionals

Virtual, or online, consultations with doctors are offered by private healthcare portals primarily for informative and advisory purposes. These portals explicitly state that their services do not serve as a substitute for personal medical examinations and diagnostics conducted through conventional medical procedures. Similar to appointment booking, virtual consultations involve fees and align with the characteristics of an information society service. However, they do not meet the criteria for an intermediary service. It is worth noting that virtual consultations as a form of telemedicine are also supported by the state, especially during crisis situations, pursuant to amendments to the Health Care Act.[22] In this case, the Slovak legislator had in mind outpatient care, because experience has shown that the provision of

[20] Provisions of § 2a of the Health Care Act.

[21] Additional analysis of E-ordering system provided by state: SOPÚCHOVÁ, S. *Electronic healthcare in the Slovak Republic. E-Health and telemedicine*. Bratislava: Wolters Kluwer, 2022.

[22] The provisions of § 49k par. 1 of the Health Care Act.

consultations by telephone or e-mail is common, but these have not yet been supported by law (e.g. verification of results by telephone, health consultation, etc.).[23]

Healthcare professional's evaluation

Healthcare professional's evaluation service represent a relatively recent addition to private-sector healthcare services, lacking state-provided alternatives. These services enable users to provide voluntary feedback about specific doctors. However, such ratings are typically contingent on having personally consulted with the doctor. Providers of these services typically disclaim responsibility for the accuracy and truthfulness of the ratings. They reserve the right to remove user-generated content if it conflicts with the doctor's right to protect their personal reputation.[24] Notably, these services, although free for users (service recipients), can be a source of revenue for providers through advertising-related compensation or other means. This makes them an economic activity.

Healthcare professional's evaluation services exhibit characteristics of an information society service, as they are provided remotely through electronic means, based on individual service requests. While they are offered free of charge to users (service recipients), providers may earn compensation from third parties, contributing to their status as an economic activity.[25] Healthcare professional's evaluation service also fall within the scope of intermediary services, particularly as "hosting" services. Operators of these private healthcare portals, functioning as service providers, store user-generated information at the recipient's request.

The Digital Services Act establishes that hosting service providers bear no responsibility for stored information unless specific conditions are met. These conditions encompass a lack of actual knowledge regarding illegal activity or content and a lack of awareness of facts or circumstances indicating obvious illegality. If such knowledge or

[23] SOPÚCHOVÁ, S. *Artificial intelligence and its use in the process of providing health care. In: Human rights.* From reality to the virtual world. Josefow: Alcide De Gasperi University of Euroregional Economy in Józefów, 2021, p. 94.

[24] Internet portal TopDoktor. Business conditions. Available online: https://www.topdoktor.sk/p/obchodne-podmienky

[25] ANDRAŠKO, J. et al. *Law of Information and Communication Technologies* 2. Bratislava: TINCT, 2021, p. 63.

awareness arises, hosting service providers must promptly remove or disable access to the unlawful content.[26]

In practice, situations may arise where user-generated content on healthcare professional's evaluation may exhibit signs of illegal activity or unlawful content.[27] While portal operators may provide doctors with the ability to delete ratings from their profiles, the legal obligation remains with the portal operator, not the doctor, to remove illegal content. This raises legal questions about the doctor's authority to assess what constitutes a violation of their personal rights and what qualifies as legitimate criticism - a form of freedom of speech. This situation presents two legal issues: determining who is obligated to remove illegal content (as clarified by the Act on Digital Services) and the subjective nature of content removal decisions, which could potentially infringe on freedom of speech.

Conclusion

Digital services have become increasingly prevalent across various sectors of society, including healthcare, which is undergoing a transformation driven by information and communication technologies. However, healthcare services, including medical examinations, do not always fit neatly within the framework of the Digital Services Act, and this holds true for other areas such as autonomous vehicles and education. In this discussion, we have assessed whether digital healthcare services can be categorized under the Digital Services Act, a European Union regulation. Our examination led to several conclusions and raised some pertinent issues:

Public vs. private sector digital healthcare services

We divided digital healthcare services into those provided by the state (public sector) and those offered by private companies (private sector). This distinction reflects the current situation in the Slovak Republic, shaped by the state's inability to provide comprehensive digital healthcare services.

[26] Article 6 par. 1 of the Digital Services Act.

[27] According to Article 1 letter h) of the Digital Services Act is illegal content "*any information that, by itself or by referring to any activity, including the sale of products or the provision of services, is not in accordance with the legal regulations of the Union or any member state, regardless of the precise subject matter or nature of such legislation.*

Our research revealed that the Digital Services Act primarily applies to electronic healthcare services in the private sector, while public sector services do not fall under its purview. The fundamental reason for this differentiation is that public sector services do not meet the criteria of information society services or intermediary services as defined by the Act.

Private sector intermediary services

Within the private sector, certain services could be considered intermediary services. Notably, healthcare professional's evaluation services and platforms for publishing professional articles stand out in this regard. These services involve the storage of user-generated content, which is an essential characteristic of intermediary services under the Digital Services Act.

Content moderation and removal

The issue of content moderation and removal becomes significant in the context of healthcare professional's evaluation services. It raises questions about balancing freedom of speech with the protection of individual personality rights. The Digital Services Act places the responsibility for content removal on service providers, creating a potential tension between these two fundamental rights.

Duplication of services

A peculiar situation has arisen in Slovakia concerning the duplication of digital healthcare services. For instance, the state offers a service for making appointments with doctors called E-ordering, while private health portals also facilitate online appointment booking with healthcare professionals for varying fees. The legal basis for such private services differs, and the market pricing for these services varies significantly.

Virtual consultations and non-standard approaches

Virtual consultations with doctors are another point of contrast between public and private sector offerings. The state regulates electronic consultations quite restrictively, allowing them only during crisis situations. In contrast, private healthcare portals offer consultations with doctors for a fee but emphasize that these consultations are not a replacement for traditional healthcare. This approach raises concerns about cybersecurity, personal data protection, and liability for damages, which remain inadequately addressed.

In summary, our research confirmed initial hypothesis that digital healthcare services cannot be neatly categorized and subjected to the Digital Services Act's provisions. The complex landscape arises from the coexistence of services provided by both the state and private entities in Slovakia. This situation underscores the need for comprehensive legal frameworks to govern digital healthcare services and ensure they meet the highest standards of safety, security, and quality.

References

1. ANDRAŠKO, Jozef. et al. Law of information and communication technologies 2. Bratislava: TINCT, 2021, 324 p.
2. ANDRAŠKO, J. et al. Regulatory challenges of e-Government in the Slovak Republic in the context of European Union law. Prague: Wolters Kluwer ČR, 2022, 286, 380 p.
3. BOYER, K., HALLOWELL, R., ROTH, A. V. Eservices: operating strategy – a case study and a method for analyzing operational benefits. In: Journal of Operations Management. 2002, vol. 58, ed. 2.
4. Directive 2015/1535 of the European Parliament and of the Council of the European Union establishing the procedure for providing information in the field of technical regulations and rules relating to information society services
5. Law no. 576/2004 Coll. on health care, services related to the provision of health care and on amendments to certain laws
6. Law no. 95/2019 Coll. on information technologies in public administration
7. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the single market for digital services and amending Directive 2000/31/EC (Digital Services Act)
8. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on competitive and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)
9. SOPÚCHOVÁ, S. Electronic healthcare in the Slovak Republic. E-Health and telemedicine. Bratislava: Wolter Kluwers, 2022, 135 p.
10. SOPÚCHOVÁ, S. Artificial intelligence and its use in the process of providing health care. In: Human rights. From reality to the virtual world. Jósefów: Alcide De Gasperi University of Euroregional Economy in Józefów, Poland, 2021, 368 p.

11. STŘEDA, L., HÁNA, K. eHealth and telemedicine. Prague: Grada Publishing, 2016, 160 p.
12. UNESCO. Developing and Using Indicators of ICT Use in Education. Bangkok: UNESCO Asia and Pacific Regional Bureau for Education, 2003, 138 p.
13. https://www.topdoktor.sk/p/obchodne-podmienky