Правни факултет Универзитета у Нишу
Faculty of Law, University of Niš

Међународна научна конференција
International Scientific Conference

„ПРАВО И ДИГИТАЛИЗАЦИЈА”
”LAW AND DIGITALIZATION”

Зборник радова
Collection of papers

Ниш, 2021.

МЕЂУНАРОДНА НАУЧНА КОНФЕРЕНЦИЈА / INTERNATIONAL SCIENTIFIC CONFERENCE
„ПРАВО И ДИГИТАЛИЗАЦИЈА" / „LAW AND DIGITALIZATION"
Зборник радова / Collection of papers

Издавач / Publisher
Правни факултет Универзитета у Нишу / Faculty of Law, University of Niš

За издавача / For the Publisher
Проф. др Горан Обрадовић, декан

Организатор Конференције / Conference organizer
Центар за правна и друштвена истраживања

Уредници Конференције / Editors-in Chief
Проф. др Горан Обрадовић, редовни професор Правног факултета Универзитета у Нишу
Доц. др Марко Димитријевић, доцент Правног факултета Универзитета у Нишу

Рецензенти / Reviewers
Проф. др Мирослав Лазић, редовни професор Правног факултета Универзитета у Нишу
Проф. др Срђан Голубовић, редовни професор Правног факултета Универзитета у Нишу
Проф. др Небојша Раичевић, редовни професор Правног факултета Универзитета у Нишу

Технички уредник / Desktop Publishing:
Владимир Благојевић

Превод резимеа / Proofreading:
Гордана Игњатовић

Корице / Cover:
Владимир Благојевић

Штампа / Print:
Медивест, Ниш

Тираж / Circulation: 80

ISBN: 978-86-7148-286-8

Штампање овог Зборника је финансијски помогло Министарство науке, просвете и технолошког развоја Републике Србије.

САДРЖАЈ

Реч уредника Међународне научне конференције „Право и дигитализација”

Међународна научна конференција „Право и дигитализација“ одржана је на Правном факултету у Нишу, у периоду од 23 - 24. априла 2021. године. Услед текућих друштвених прилика, међународна конференција је одржана у хибридном формату и уз пуно поштовање епидемиолошких мера, чиме су учесници допринели одговорном и савесном понашању у време пандемије COVID - 19.

На Конференцији је учешће узело преко седамдесет домаћих и иностраних стручњака из различитих области права (Турска, Бугарска, Русија, Румунија, Пољска, Босна и Херцеговина, Хрватска, Северна Македонија, Црна Гора). Међународни карактер конференције огледао се и у већем броју светских језика на којима су радови презентовани, услед чега је та структура задржана и у овом Зборнику.

Учесници су у радовима настојали да укажу на главне дилеме, изазове и отворена питања у правној теорији и пракси у условима свеприсутне дигитализације уз чињење конкретних препорука и предлога за њихово оптимално правно регулисање.

Актуелност конференцијске проблематике, пажња јавности и позитивне критике коју је Конференција добила најбоља су потврда њеног високог научног нивоа. Један број радова објављен је у Зборнику радова Правног факултета у Нишу, док су остали, након поступка рецензирања, учињени доступним широј научној и стручној јавности путем ове публикације. Искрено се надамо да ће објављени радови пружити оправдан и добар основ за свеобухватне научне полемике.

У Нишу, 19.11.2021.

Уредници Конференције

Проф. др Горан Обрадовић

Доц. др Марко Димитријевић

Mustafa Yasan, LL.D.,
Associate Professor,
Faculty of Law Commercial Law Department, Sakarya University,
Turkey

UDK: 347.748:004(560)

THE FIRST STEP FOR DIGITALIZATION IN CHEQUES IN TURKISH LAW: THE OBLIGATION OF THE USE OF DATA-MATRIX IN CHEQUES

Abstract: *The digitalization of law is a phenomenon that has gained importance in Turkish Law in recent years, just as it is in comparative law. The Turkish legal system has not been indifferent to the developments in technology, and the innovations brought about by digitalization have been the subject of codification frameworks in almost all areas of law. One of these codification frameworks was about the cheques. Unlike other bills of exchange, the cheques, which have a more active role in market stability, the use of Data-Matrix was regulated as an obligation to ensure transparency and prevent informality. Thus, in this period in which the institution of electronic bills of exchange is presented as a project, the first stages of digitalization have been completed thanks to the Data-Matrix application on cheques.*

Keywords: *Negotiable Instruments Law, Cheque, Data-Matrix, Digitalization in Turkish Law, Central Bank of the Republic of Turkey.*

1. Introduction

In Turkish Law, the cheque is regulated as a type of negotiable instrument in both specific chapter of the Turkish Code of Commerce No. 6102[1] (TCC) and the Cheque Code No. 5941[2] (CC), a cheque-specific codification. The purposes of the provisions related to cheques are to increase the confidence in the cheque, to give validity to the confidence-building measures and sanctions and thus to spread the circulation of the cheques. In order to achieve this ratio-legis, the leg-

[1] Turkish Code of Commerce, Official Gazette Republic of Turkey, Date:14.02.2011, Number:27846

[2] Cheque Code, Official Gazette Repuplic of Turkey, Date: 20.12.2009, Number:27438

islator made a radical change in the CC and the TCC in 2016. With the amending Code No. 6728, two more elements were added to the validity of the cheques. According to TCC Art.780/2, thanks to the Data-Matrix, cheque creditors can access data regarding the cheque account holder and the cheque issuers with the cheque they hold. They canthus make evaluations and examinations regarding the reliability of the cheque. This regulation regarding the Data-Matrix card can be considered the first step of digitization in cheques in Turkish Law. The next and possibly the final step in completing the digitalization of cheques in Turkish Law is the codification effort for electronic cheques, which is still in the draft version and waiting to be enacted in the Parliament. To assess whether digitalization can be completed in cheques in Turkish Law, it is necessary and helpful to examine the essentials and consequences of the Data-Matrix application in cheques as the first step of digitalization.

2. Frameworks for Digitalisation in Turkish Law

As a technical concept, digitalization can be defined as the presentation of accurate information in a way that is not tied to a physical source. Digitization, which contributes to companies becoming more flexible and adapting to the market even faster, also has ordinary consequences such as increasing technology standards, thus causing the companies to develop in a stabilised way (Ümütlü, 2021: 61).Analysing the information produced and therefore turning to new markets for the companies are among the other advantageous results of digitalization.One point should be underlined. Although digitalization is a concept that impacts social and professional life and has been keeping up to date for a long time, it has increased its importance in recent years, primarily due to technological developments and innovations in informatics (Ümütlü, 2021: 60). Since the beginning of 2020, due to the Covid-19 Pandemic, digitalization has emerged as an inevitable end in every field of life,from economy to health, from art to sports, from religious rituals to the legal system (Şentürk, 2021: 758). Although digitalization efforts in Turkish law had already started before the Covid-19 Pandemic and significant progress had been made, especially in areas such as commercial law, tax law and contract law, labor law, the Pandemic has increased the speed of digitalization in Turkish Law to an unpredictable extent (Kubilay, 2020: 259).

Keeping in mind that digitalization has shown its effect more clearly during the pandemic process, different exemplary aspects of digitalization in various fields of law can be pointed as follows.In labor law, digital platforms have been accepted as one of the main concept of the 4Th generation of industrial relations (Yangın, 2020: 1214). In criminal law, it has emerged as a necessity and a re-

quirement of digitalization that the proceedings and evidence collection activities are carried out online, especially in the context of cybercrimes (Şentürk, 2021: 761).The ability to monitor tax crimes in tax law on the internet can be counted among the reflections of digitalization in tax law and tax enforcement law (Yıldız, Günay, 2018: 4009). In terms of the law of procedure, digitalization is an older concept compared to other branches of law.Because the artificial intelligence technology applied in the determination of the courts where the cases will be held can be accepted as the starting point of the close relationship between digitalization and judicial law.Conducting hearings online and conducting mediation and arbitration negotiations via teleconference have been among the measures applied, especially during the pandemic and which are the benefaction of digitalization. This measure proves that digitalization and judicial law are in a close relationship. This measure, which is mainly applied on a temporary basis, can be considered among the results of digitalization as innovations that can be concerned even after the pandemic, especially due to its advantages such as speedy trial and faster resolution of disputes. Digitalization has essential consequences also in terms of contract law. The preparation, interpretation and legal audit of smart contracts show the close relationship between law and digitalization (Üstün, 2021: 59).Contracts in insurance sector are also established thanks to the advantages of digitalization (Kubilay, 2020: 276). Wills prepared electronically prove the increasing importance of digitalization in inheritance law. The fact that e-mails have evidence capability is another development caused by digitalization in the law of proof. The rising importance and acceptability of cryptocurrencies cannot be denied (Üstün, 2021: 43). Although the legal nature of crypto/virtual/digital currencies is debated even still today, it is seen that the applications and practices where cryptocurrencies are accepted as payment instruments are increasing. For this reason, in terms of Turkish banking law, efforts for legal regulations with cryptocurrencies still continue as of today (Karakuş, Altundaş, 2021: 27). Company law is also one of the areas where digitalization has a strong impact. The fact that general assembly meetings and board of directors' meetings can be held electronically in joint-stock and limited companies has been validated in principle with Law No. 6102 (Turkish Code of Commerce), and due to the pandemic, the public authority has provided incentives for companies to benefit from this opportunity (Möslein, 2020: 707). Keeping and storing commercial books in an electronic environment is one of the applications that has been possible for a long time in Turkish law. It must be underlined that it is impossible to perform audits of companies, especially fraud audits, in a compatible way without using information technology. As a matter of fact, digitalization should be accepted as one of the basic concepts in terms of audit law. Although the legal framework has not been completed yet, the fact that companies can be established in the electronic

environment, to put it more accurately, the validity of the virtual company concept also shows what kind of changes and reforms digitalization can cause in company law.The issues we have mentioned so far are only examples and prove that the impact of digitalization in Turkish law has been felt and will continue to be felt for a long time with the effect of both the European Union candidate country status and globalization.

One of the branches of law in which digitalization makes its impact felt is the negotiable instruments law. The concept of non-leaf securitiesrefers to the stock certificates issued especially for capital companies switched in the stock exchange.Share certificates, which are traded electronically but lack a physical presence, are referred to as non-leaf securities and have been legally accepted in Turkish Capital Market Law for a long time. The concepts of electronic promissory notes and electronic cheques, which are still being worked on at the Ministry of Commerce, also prove that digitalization has and will have a substantial effect on negotiable instruments law. Perhaps the concepts of electronic promissory notes and cheques, which will lead to radical changes in the negotiable instruments law, can also reveal the social engineering dimension of digitalization (Demirci, 2020: 5). One of the areas where digitalization has already started to show its effect in the negotiable instruments law is the legislation related to cheques. In Turkish Law, commercial bills are among the particular types of negotiable instruments and consist of bills of exchange, promissory notes and cheques. Cheques stand out as the commercial bills that are most suitable for digitalization, as they are in close relationship with the banking system, have international payment capabilities and are preferred in secure payment methods (Demirci, 2020: 5). As a matter of fact, the legislator validated the Data-Matrix application in 2016 as the first step of digitalization in cheques. This preference is undoubtedly correct. However, to express in advance, the Turkish legislator was late in bringing legality to the Data-Matrix application when evaluated in terms of comparative law.

3. The Beginning of the Digital Era in Cheques: The Obligation to Apply the Data-Matrix

3.1. Data-Matrix Obligation as One of the Amendments Performed by the Law Dated 15.06.2016 and Numbered 6728

As a type of commercial bills, the cheque is a very crucial factor in money markets. The cheques are listed in the active part of the accounting systems and recorded immediately after the cash in the list of actives. In other words, the cheques are the commercial bills with the highest liquidity capability (Öztan,

2012: 234).Cheques are also essential tools for the stability and reliability of the money markets. The widespread use of cheques in a market is an important indicator of the trust in that market. Therefore, the cheques do not only concern the legal and economic interests of the parties involved in the cheque relationships (Öztan, 2012: 235). The cheques are market instruments that gain importance in terms of public interest, which are also in economic law (Kendigelen, Kırca, 2019: 274).

Although the cheques are already regulated in the TCC in the section dedicated to the law of negotiable instruments, due to the importance I have pointed out above, the legislator also needed a code specific to the cheques.Cheque Law No. 5941, which entered into force in 2009, regulates the cheque with public law priorities (Yasan, 2021: 146). The ratio-legis of this law is to increase the trust in the cheque and spread their use. In order to realize this purpose, the Central Bank of the Turkish Republic has been given a number of critical powers and duties (Ülgen, Helvacı, Kaya, NomerErtan, 2019: 282). Although the Cheque Law is a new codification, it has been the subject of amendments reflecting different preferences of the legislator in a short time. In order to realize the purpose stated in the Cheque Law, the drawing of unpaid cheques was defined as a crime and both judicial fines and the prohibition of issuing cheques were envisaged as sanctions (Bozer, Göle, 2020: 259).

The legislator has also shown his interventionist approach to cheques in the provisions of the TCC regarding cheques. With Law No. 6728, which entered into force on 15.07.2016, two new elements were added to the validity elements of cheques. These are the serial number given by the bank and the Data-Matrix. The absence of these two new elements causes the cheque to be invalid, just like other validity elements (Demirci, 2020: 20).This obligation only applies to cheques printed by Turkish banks. These two new elements were accepted among the validity elements of the cheque to prevent informality and increase the confidence in the cheques (Ülgen et all., 2019: 283). As a matter of fact, thanks to the serial number and the data Matrix, the transparency of the cheque relationship will be ensured. For those who want to enter into a cheque relationship and who wish to take legal action as the payee of the cheque, it will be possible to make a more accurate decision regarding the reliability and encashment ability of the cheque (Kendigelen et all., 2019: 283). At least, this is the result that the legislator wants to achieve with the serial number and Data-Matrix requirement.

3.2. Content of Data-Matrix Obligation on Cheques

The details of the Data-Matrixobligation are regulated by the Communiqué issued by the Ministry of Trade.The task and authority of issuing communiqué

have been given to the Ministryby TCC Article 780/4. Data-Matrix is defined as follows in the Communiqué[3] issued pursuant to the TCC: It is a two-dimensional barcode, which is one of the elements of the cheque and can be printed on the cheque as a square or rectangle, based on the ISO/IEC 16022 International Symbology SpecificationData-Matrix ECC 200 Version, which allows accessing and reporting data on the cheque, the cheque account holder and the cheque issuer (Bozer et all., 2020: 259, 260).Therefore, although the Data-Matrix application is seen as an initiative of the Turkish legislator, international standards have been adopted, and aimed to harmonize with the applications in comparative law.

The Data-Matrixobligation is considered as the first step of digitalization in bills of exchange in Turkish Law.As an obligation, Data-Matrix plays a very significant role in ensuring transparency in cheques (Sumer, 2020: 320). Thanks to the Data-Matrix, cheque creditors can access the data of the cheque account holder and the issuers without seeking the cheque account holder's or endorser's consent (Ülgen et all.,2019: 284). The data in question does not provide transparency only for those who will be creditors in the cheque relationship.In addition, the Data-Matrix application has essential functions in order to ensure market control for the public authority that wants to prevent informality. So, which data can be accessed thanks to the Data-Matrix application for both the creditors in the cheque relation and the public authority? According to TCC Article 780/2,

a) Name, surname or trade name of the cheque account holder,

b) In case the cheque account holder is a merchant, the name, surname or trade name of the authorized persons registered in the trade registry,

c) The total number of banks with which the cheque account holder has a cheque account,

d) The number and amount of cheques that have not been presented to the banks of the cheque account holder,

e) Number and amount of cheques issued and delivered to banks,

f) Number and amount of cheques paid on presentation within the last five years,

g) The date of presentation of the first cheque presented,

h) The date of submission of the last cheque submitted,

ı) The submission date of the last cheque paid on its presentation,

[3] Communiqué by the Ministery of Trade on the Application of Data-Matrix on Cheques, Official Gazette of Republic of Turkey, Date:31.12.2016, Number:29935.

i) The number and amounts of unpaid cheques that have been "bounced" in the last five years,

j) The number and amount of cheques that have been "unpaid" in the last five years and paid later,

k) The submission date of the last cheque that has been treated as "non-refundable" in the last five years,

l) Whether there is a ban on opening a cheque account against the cheque account holder,

m) Whether there is an injunction record for each cheque sheet,

n) If the cheque account holder is a merchant, whether the bankruptcy decision has been made, and if the bankruptcy has been decided, the date of the decision.

3.3. Implementation of Data-Matrix Obligation on Cheques

A specific system is needed for the Data-Matrix to be functional and to perform its functions, in other words, to provide the expected benefits from the Data-Matrix obligation of the legislator. This system is called "The Data-Matrix Reading and Information Sharing System". The task of establishing this system has been given to the Banks Association of Turkey, which has been given the authority to coordinate and regulate the Turkish banking system.As a result of this appointment, the Data-MatrixReading and Information Sharing System was established by the Risk Center of the Banks Association of Turkey (Bozer et all., 2020: 264).

Banks have a vital role to play for the Data-Matrix system to function properly. According to this role, banks register the real persons and legal entities for which they open a cheque account, and if the cheque account holder is a legal entity, the real persons are notified by the legal entity and authorized to perform all transactions on behalf of the legal entity as of the account opening date, in the Data-Matrix Reading and Information Sharing System.In an opposite situation, in other words, the failure of banks to fulfil their registration obligations in the system causes bank legal entities to face administrative and penal sanctions (Demirci, 2020: 24).

For the Data-Matrix system to function properly, besides the banks, those who deal with cheques must also fulfil their obligations. Accordingly, the real or legal person in whose favour a cheque with a Data-Matrix is drawn should record the received cheque in the Data-Matrix Reading and Information Sharing System until the date of submission at the latest. The date of submission of the cheque is regulated in the TCC in three ways. Accordingly, if the cheque is to be paid at the

place where it was issued, the legal submission period for the cheque is 10 days from the issuance date of the cheque. If the cheque is to be paid in a place other than where it was issued, the legal submission period of the cheque is 1 month. If the cheque is to be paid in a different continent than the one in which it was issued, the legal submission period for the cheque is 3 months from the date of issue (Bozer et all., 2020: 264). The beneficiary or the holder shall be obliged to record this cheque in the Data-Matrix Scanning and Information Sharing System established by the Banks Association of Turkey Risk Center from the above-mentioned legal submission deadlines until the date of presentation of the cheque.

Another critical step in the operation of the Data-Matrix system is the sharing of the collected information. It is the Banks Association of Turkey Risk Center that will carry out this sharing obligation. Risk Center shares the information it collects with the "Authorized Information Exchange Institution". So what is Authorized Information Exchange Institution? Authorized Information Exchange Institution can be expressed as the company with which the Risk Center of the Banks Association of Turkey carries out information exchange. For this reason, two institutions and organizations authorized as system operators are defined in the Data-Matrix system. Accordingly, the Banks Association of Turkey Risk Center and the Authorized Information Exchange Institution are accepted as the "System Operator" in the Data-Matrix system in Turkish Cheque Law.

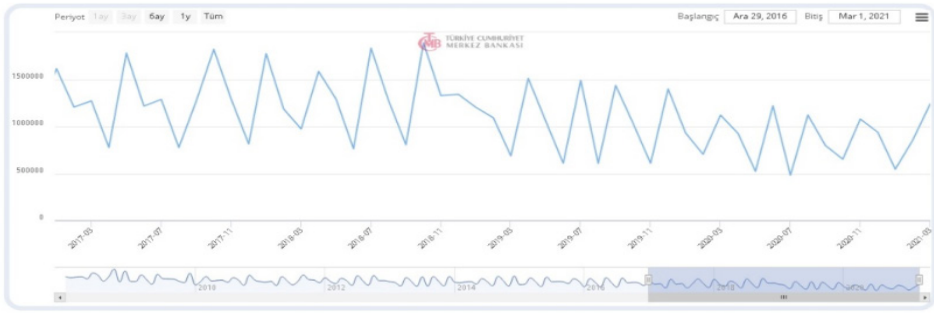
Data-Matrix codes have a function in the form of collecting information. The data in the Data-Matrix, which is obligatory on the cheques, can be accessed by having the Data-Matrix codes scanned. After the Data-Matrix codes are scanned, the report should also be prepared. As a matter of fact, the Data-Matrix system operator will issue the report by scanning the Data-Matrix. In other words, the Risk Center of the Banks Association of Turkey and authorized information exchange institutions are supposed to function as system operators by scanning the Data-Matrix and preparing the report. The system operators are only responsible for the scanning and reporting the information transmitted to them through the system. The accuracy or timeliness of the data is the responsibility of the bank or source institution, not the system operator.

4. Evaluation of the Success or Unsuccess of the Data-Matrix Obligation Application

Has the Data-Matrix system that has been tried to explain briefly succeeded? In other words, has the ratio-legis of the legislator with the Data-Matrix been realized? Thanks to the Data-Matrix system, has there been a decrease in unpaid cheque practices by providing transparency in cheques? In this way, is there an increase in the confidence in the cheque and the ability to circulate? To answer

these questions, it is necessary to examine the data obtained from the official website of the Central Bank of the Republic of Turkey[4] regarding the amount and number of unpaid cheques since the adoption of the Data-Matrix system.

The first chart shows the number of cheques submitted to banks from **01.01.2017 to 01.03.2021**, right after implementing the Data-Matrix obligation[5].



The Number of Cheques Submitted to the Banks (01.01.2017—01.03.2021)

In the second chart, the changes in the total amounts of cheques submitted to banks within the same period **(01.01.2017-01.03.2021)** is seen[6].

The Amount of the Cheques Submitted to the Banks (01.01.2017-01.03.2021)

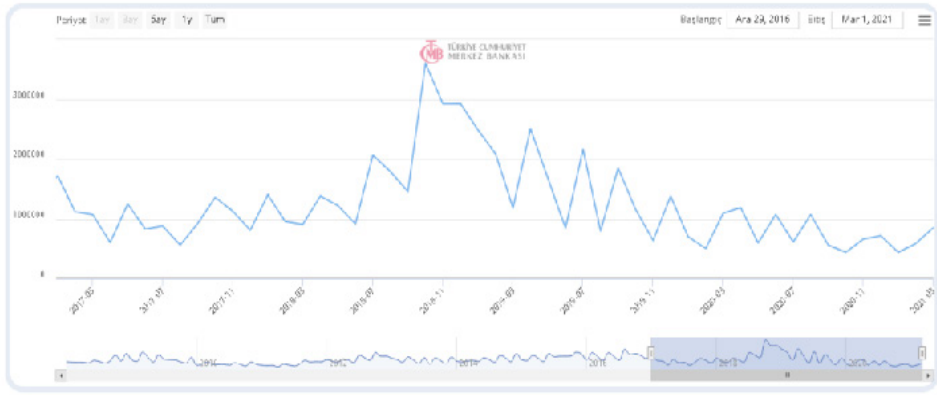
In the third chart, the change in the total values of the unpaid cheques can be observed in the same period **(from 01.01.2017 to 01.03.2021)**[7].

[4] https://evds2.tcmb.gov.tr

[5] https://evds2.tcmb.gov.tr/index.php?/evds/searchEvdsValue/QMOnZWtsZXJA

[6] https://evds2.tcmb.gov.tr/index.php?/evds/searchEvdsValue/QMOnZWtsZXJA

[7] https://evds2.tcmb.gov.tr/index.php?/evds/searchEvdsValue/QMOnZWtsZXJA



Total Value of the Unpaid Cheques (01.01.2017-01.03.2021) 1.716.507.000 TL-853.709.000 TL

The fourth chart is also about unpaid cheques. In this chart, year-based changes in the total number of unpaid cheques can be observed in the period **between 01.01.2017 and 01.03.2021**[8]**.**

Total Number of Unpaid Cheques (01.01.2017-01.03.2021) 50.391 - 11.437

From the graphs, when the databetween the Data-Matrix system was adopted, and the latest updated are compared, it is understood that there is no change in the number of cheques submitted to banks. There has even been a decrease in the number of cheques submitted. On the other hand, a limited increase is observed in the total value of cheques submitted to banks from the graphics. However, the reason for this increase is not the positive effect of the Data-Matrix system. The reason for this increase is the inflationary economy experienced for a long time in Turkey. Again, as can be seen from the graphs, it is understood that there

[8] https://evds2.tcmb.gov.tr/index.php?/evds/searchEvdsValue/QMOnZWtsZXJA

is a significant decrease in the total amount of unpaid cheques and the number of unpaid cheques. However, it is understood from the data in the graphics that this decrease is not stable and sustainable. The reason for the instability is the negative effects of political developments on the economy and money markets.

As a result, the adoption of the Data-Matrix system undoubtedly increases the possibilities of accessing information in favour of cheque creditors and public authorities. However, the data in the graphs show that the decrease in unpaid cheque practices as of today cannot be attributed only to the Data-Matrix system. In the perspective of de legeferanda, in addition to the Data-Matrix system, it is necessary to realize the universal requirements of institutional reforms that strengthen the independence of the Central Bank, a transparent monetary policy management, a realistic and impartial public audit and, of course, the rule of law, especially the independence of the judiciary.

5. Conclusion

Digitalization is a phenomenon that has shown its effect in law and every aspect of life, especially with the impact of the Covid-19 Pandemic. Commercial law and negotiable instruments law, a sub-branch of commercial law, is included in the legal disciplines in which digitalization makes its impact felt. Codification efforts on electronic cheques and electronic promissory notes still remain on the agenda. However, digitalization has already shown its effect in the negotiable instruments law. As one of the obligatory elements in cheques, with Law No. 6728, the Data-Matrix application has been made valid together with the serial number element. The legislator's purpose in applying the Data-Matrix obligation is to provide transparency in the cheque relationship and prevent informality. In this way, the trust in the cheque system, the circulation and the cheques' preferability will increase even more. Looking at the 5-year balance sheet on the graphics, has the legislator achieved this goal? Have the legislator's expectations been met? Considering the data of the Central Bank of the Republic of Turkey, it is not possible to give a positive answer to these questions. So what should it be? What needs to happen is that the legislator is not affected by populist approaches, the law does not apply to the social engineering function for short-term expectations, institutional and structural reforms, including the independence of the Central Bank, are carried out at the EU standards, the requirements of the rule of law are met, and the public audit is validated realistically and impartially. In this way, the expected benefit from the cheque, which is one of the commercial bills, can be obtained in all aspects.

References

Bozer, A., Göle, C. (2020). Kıymetli Evrak Hukuku. Ankara: Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayınevi

Demirci, S. (2020). *Türk Hukukunda Elektronik Çeke Doğru, Dünü ve Bugünüyle Çek*. Ankara Barosu Dergisi. Year: 2020, Issue: 3, p.1-47.

Karakuş, H.,Altundaş, A. O. (2021). *Finteklerin Bankacılık Hukuk Sistemindeki Yeri.*Ahkam Aktüel Hukuk Dergisi. Issue: 1, p.24-33.

Kendigelen, A., Kırca, İ. (2019). Kıymetli Evrak Hukuku. İstanbul: Oniki Levha Yayınevi

Kubilay, H. (2020). *SigortacılıkSektöründeDijitalleşmeninHukukiYöndenDeğerl endirilmesi*. UyuşmazlıkMahkemesiDergisi. Volume: 18, Issue: 16, p.259-288.

Möslein, F. (2020). *Yönetim Kurulu Toplantı Odasındaki Robotlar: Yapay Zeka ve Şirketler Hukuku*. İstanbul Hukuk Mecmuası. Volume: 79, Issue: 2, p.699-728.

Öztan, F. (2012).KıymetliEvrakHukuku. Ankara: TurhanKitapevi

Sumer, A. (2020). Ticaret Hukuku Ders Kitabı. İstanbul: Beta Yayınevi.

Şentürk, C. (2021).*CezaMuhakemesiHukukuÖzelindeYargıdaDijitalleşme*Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi.Volume: 25, Issue: 2, p.755-785.

Ülgen, H.,Helvacı, M., Kaya, A., Nomer Ertan, N.F. (2019). Kıymetli Evrak Hukuku. İstanbul: Vedat Kitapçılık

Ümütlü, A.Y. (2021). *FelsefiAçıdanHukukunDijitalleşmesiveİnsanHaklar*.CyberpolitikJournal. Volume: 6, Issue: 11, p.59-72.

Üstün, E.S. (2021). Akıllı Sözleşmeler Blokzincir Teknolojisi. Ankara: Seçkin Yayınevi

Yangın, D. D. (2020). *Endüstri 4.0, Dijitalleşme ve İş Hukukunun Geleceği-Dijital Platformların Ortaya Çıkardığı Hukuki İlişkiler Çerçevesinde Değerlendirilmesi*. İstanbul Hukuk Mecmuası. Volume: 78, Issue: 3, p.1209-1237.

Yasan, M. (2021). Kıymetli Evrak Hukuku. Ankara: Seçkin Yayınevi

Yıldız, B., Günay, H. F. (2018). *Türk Vergi Hukuku Eksenin den Dijital Ekonomiye Genel Bir Bakış*. 3. Ulus lararası Meslekive Teknik Bilimler Kongresi. Gaziantep. p.4004-4012.

Legislation:

Cheque Code, Official Gazette Repuplic of Turkey, No. 27438 (2009)

Communiqué by the Ministery of Trade on the Application of Data-Matrix on Cheques, OfficialGazette of Repuplic of Turkey, Date:31.12.2016, Number:29935.

Turkish Code of Commerce, Official Gazette Republic of Turkey, No. 27846 (2011).

Др Мустафа Јасан,
Доцент,
Правни факултет Универзитета у Сакарији,
Турска

ПРВИ КОРАК КА ДИГИТАЛИЗАЦИЈИ ЧЕКОВА У ТУРСКОМ ЗАКОНУ: ОБАВЕЗА УПОТРЕБЕ МАТРИЦЕ ПОДАТАКА У ЧЕКОВИМА

Апстракт

Дигитализација права је појава која је добила на значају у турском праву последњих година, баш као и у упоредном праву. Турски правни систем није остао равнодушан према развоју технологије, а иновације које је донела дигитализација биле су предмет кодификационих оквира у готово свим областима права. Један од ових оквира кодификације односио се на чекове. За разлику од осталих меница, чекова, који имају активнију улогу у стабилности тржишта, коришћење Data Matrix-а је регулисано као обавеза да се обезбеди транспарентност и спречи неформалност. Тако су у овом периоду у којем се институција електронске менице представља као пројекат, завршене прве фазе дигитализације захваљујући Data Matrix апликацији на чековима.

Кључне речи*: Закон о преговарачким инструментима, Чек, Data Matrix, Дигитализација у турском праву, Централна банка Републике Турске.*

Др Татјана Јованић,
Редовни професор,
Правни факултет Универзитета у Београду,
Србија

UDK: 336.74:004

КРИПТО-ИМОВИНА КАО ПРИМЕР УТИЦАЈА ДИГИТАЛИЗАЦИЈЕ НА ПРАВО И ПРАКСУ РЕГУЛАТОРНИХ ОРГАНА

Апстракт*: Пораст трговања виртуелним валутама и другим облицима криптоимовине, као и употребе технологије тзв. дистрибуиране главне књиге (digital ledger technology), за правни систем представља један од највећих изазова данашњице. Овај рад се неће бавити детаљнијом анализом правне природе криптоимовине и класификацијом облика исте, већ превасходно утицај дигитализације на праксу надзора као одговор националних регулатора који се суочавају са дилемом да ли, и до које мере би требало да се регулише оба област, а да се истовремено на тај начин не спута финансијска иновација. Ово се не односи само на регулаторне органе из земаља са развијеним финансијским тржиштем, већ и земаља које покушавају да иновативним приступима осигурају конкурентно место својих земаља у свету алтернативних финансија, које се све више развијају. У том смислу, доминантни фокус у овом раду односиће се на правце развоја оквира јавноправне регулације овог тржишта и иновативних пракси у супервизији националних регулаторних тела.*

Кључне речи: *криптоимовина, блокчејн технологије, регулација, супервизија, финансијске иновације.*

1. Увод

Дигитална имовина, односно крипто-имовина, представља један облик технолошких иновација која може представљати супституит појединим услугама у области банкарског и тржишта капитала, нарочито у домену платних услуга и улагања на тржишту капитала. Нови финансијски посредници који нуде услуге сличне традиционалним финансијским посредницима попут комерцијалних и инвестиционих банака, берзи капитала и

институција електронског банкарства, су ван домашаја многих прописа из области регулативе бонитета и законитости пословања, па тако остварују предности тзв. регулаторне арбитраже (*regulatory arbitrage*). Савремени регулатори финансијских услуга суочени су са дилемом да ли је подстицање финансијских иновација компатибилно циљевима очувања финансијске стабилности и заштите корисника финансијских услуга. Из тог разлога многи финансијских регулатори су заузели став да не спутавају развој нових технологија у области финансијског инжењеринга, те своје прилагодљиве регулаторне стратегије заснивају на процени и управљању ризиком и развијају специфичне проактивне контролне механизме. Опсег мера финансијских регулатора варира од забране емисије и трговине инструментима и правима која проистичу из криптоимовине, упозорења и информационих кампања, приступа који чврста правила замењује меким принципима, примене постојећих правила на функционално сличне трансакције, па све до доношења посебних прописа који се односе на дигиталну имовину, као најновији тренд.

Иако су некада нови ризици постали инхерентна карактеристика финансијских услуга (нпр. прање новца), употреба нових технологија као инфраструктуре тржишта појачава значај тих ризика (нпр. употреба криптовалута на тзв. *dark web* интернету) и отвара питања нових ризика који се специфично односе на дигиталну имовину. Ово је условило појачан интерес регулатора који настоје да постигну баланс између потребе да регулишу овај нови облик финансијског посредовања заснован на технологијама чији домашај још увек није јасно одређен. Поред ризика који произилазе из коришћења финансијских услуга, у фокусу регулатора су и ризици самих технологија.

2. Дигитална имовина као један од облика иновација финансијске технологије (*Fin Tech*)

Дигитална имовина заснована је у највећој мери на специфичној технологији јавно доступне разуђене (главне) књиге (*distributed ledger technology – DLT*). Укратко, спајање блокова у ланцу (*block chain*) документује се у јавно доступној бази јединствене историје трансакција. Блокови података о трансакцијама се формирају кроз решавање алгоритама. Било да је реч о потврди трансакција кроз процес назван рударење (*mining*), где се потврда алгоритмова врши кроз разуђене мреже компјутера, или консензусом кроз нове дистрибуиране апликације, алгоритамске односно тзв. паметне уговоре, у сваком случају потврда трансакција и размена вредности обавља се испуњењем унапред одређеног услова. Нова технолошка инфраструктура

подразумева да се трансакције одвијају испуњењем унапред постављених параметара и задовољењем технолошких параметара, као и у потребом јавних и приватних кључева, што се записује кроз дисперзоване компјутерске чворове који задржавају копије свих трансакција. Инфраструктура дигиталне имовине тако представља алтернативу централизованим базама података, па неки сматрају да се нови систем верификације трансакција изграђује као један приватноправни оквир правила заснованих на консензусу и кодовима (*lex cryptographica*). (Filippi, de, Wright, 2018)

У области финансијских тржишта, технологија дистрибуиране платне књиге представља алтернативни облик корпоративног финансирања, нарочито када су у питању стартап компаније. Примера ради, и понуда инвестиционих жетона (*investment tokens*) омогућава прикупљање капитала. Због другачије инфраструктуре, дигитална имовина као облик иновација уноси велике промене у модерне финансијске системе, а тако и нове ризике. Популарно назване финансијске технологије (*FinTech*) уносе промене не само у погледу начина обављања финансијских услуга, већ и уводе нове конкуренте, што пред регулаторе представља изазов у погледу проширења надлежности. Финансијске технологије, са једне стране, представљају алтернативу традиционалним финансијским институцијама, али са друге стране утичу на стварање нових облика сарадње традиционалних и нових посредника на тржишту, што усложњава пословне односе и ствара нове ризике. (Enriques, Ringe, 2020) Кључни ризици употребе дигиталне имовине су ризици њихове употребе у сврхе прања новца и финансирања тероризма, угрожавања монетарне и финансијске стабилности, укључујући ту и заобилажење прописа о финансијским услугама, финансијским тржиштима и опорезивања. Због њихових инхерентних карактеристика (нпр. анонимност децентрализованих система), могућности за злоупотребу су велике. (FATF, 2014)

Под новом одредницом "финансијске технологије" (*FinTech*) обухваћене су иновације у области индустрије финансијских услуга изазване развојем информационих технологија чији су резултат нови пословни модели, производи и услуге у оквиру једне организације или више, производа, процеса или система. (Puschmann, 2017:74) За разлику од традиционалних финансијских институција које су обично високо капитализовани субјекти, финансијске технологије омогућавају мањим, недепозитарним институцијама, које нису подвргнуте пруденционој регулативи, приступ финансијским тржиштима, потрошачима и улагачима. Финансијске технологије доводе у питање начело конкурентске неутралности на финансијском тржишту, али са друге стране поспеешују његов развој, доприносе развоју и нарочито приуштивости и доступности финансијских услуга. (Gabor,

Brooks, 2017: 423) Из угла регулатора, дигитална имовина представља облик иновација финансијског инжењеринга који има потенцијал да утиче на пословање регулисаних финансијских институција, обзиром да многи облици дигиталне имовине представљају супституте традиционалних инструмената на банкарском и берзанском тржишту.

Пракса је обично бржа од законодавца, нарочито када су у питању технолошке иновације. Све већи ниво комплексности финансијског окружења поставља нове изазове пред регулаторе. Нови пословни модели, нове услуге и очекивања корисника услуга је утицало на промену парадигме финансијске регулације. (Arner, Barberis, Buckley, 2017) Једна од најзначајнијих карактеристика новог регулаторног оквира је неизвесност у погледу ризика употребе нових технологија, што налаже потребу за флексибилним приступом у погледу још непознатих ризика нових пословних модела и нових услуга. Претерано превентивни приступ би одређене облике финансијских иновација дискриминисао, што би утицало на међународну конкурентност домаћег регулаторног оквира. У том смислу, прерано регулисање когентним прописима спутало би иновације. Због тога се пракса регулаторних органа креће управо ка мекшем приступу, који је често заснован на тзв. меком праву и принципима уместо обавезујућих прописа, као и иновацијама у самом процесу регулисања и надзора над финансијским субјектима. (Ringe, Ruof, 2020: 613) У основи, многе финансијске иновације подразумевају структурне промене, те регулатори морају да процене да ли такве промене носе са собом нове ризике и да ли су обухваћене постојећим регулаторним оквиром. Са друге стране, раније укључивање регулатора финансијских тржишта у праћење процеса финансијских иновација, ће иноваторима обезбедити правну сигурности и могућност да прилагоде своје пословање разумним трошковима усклађености пословања. (Fenwick, Vermeulen, Kaal, 2017: 651)

3. Прилагођавање регулаторног оквира

3.1. Нове технологије у области финансијских услуга и принцип технолошке неутралности

Као што је напред већ истакнуто, финансијски регулатори настоје да постигну баланс између потребе да се регулишу нови облици финансијске интермедијације засновани на технологијама чији домашај још увек није јасно одређен, а да притом не наруше потенцијал ових технологија да увођењем конкуренције побољшају остваривање основних циљева финансијске регулације. Нове технологије, иако представљају нове ризике, чини

се да имају потенцијал да регулаторима помогну да ефикасније користе своје ресурсе. Једна од последица технолошких иновација које се везују за IT сектор јесте и дигитализација процеса супервизије над финансијским посредницима, што ће бити приказано у последњем сегменту рада посвећеног регулаторним иновацијама.

Један од кључних изазова дигитализације финансијског посредовања је потреба за технолошки неутралним приступом. Принцип технолошке неутралности регулације, првобитно развијен у домену информационо-комуникационих технологија, изражава се кроз три равни. (Koops, 2006: 77) Прва раван односи се на исход, те се принцип тумачи као обавеза регулатора да регулише исход односно резултат, а не саму технологију. Друга раван односи се на активности и подразумева да се истим правилима подвргну исте активности, без обзира на технологију која је у основи појединачних активности. Трећа раван представља у основи принцип регулаторне неутралности, јер подразумева да се употребном инструмената регулације не сме дискриминисати једна у односу на друге технологије. У литератури се истиче неколико позитивних аспеката технолошки неутралног приступа. (van derHaar, 2007) Трошкови регулације се смањују услед смањења потребе да се константно доносе и мењају нови прописи како би право пратило технолошки развој. У условима неизвесности у погледу ризика и употребе нових технологија, технолошки неутрални приступ иноваторима, инвеститорима и корисницима нових технологија даје извесну јасноћу и подстиче иновације.

Ипак, имајући у виду технолошке карактеристике и ризике информационих технологија, као и потенцијал блокчејн технологија у области финансијског система који се злоупотребљава у сврхе прања новца, у условима таквог децентрализованог система технолошки неутралан приступ не може бити доминантна карактеристика регулаторног приступа.

3.2. Основни приступи регулисању феномена дигиталне имовине

Имајући у виду сукоб циљева подстицања иновација, са једне стране, и финансијске стабилности и заштите корисника, као фундаменталних циљева финансијске регулације, са друге стране, регулатори у многим земљама су веома опрезно приступили феномену регулисања дигиталне имовине. Многи регулатори до пре неколико година нису предвидели никакве мере, осим континуираног надгледања тржишта и евентуалних упозорења превасходно усмерених ка корисницима нових услуга. У то време регулаторне интервенције су се углавном односиле на спречавање прања новца и финансирање тероризма, обезбеђење интегритета тржишта и заштиту

корисника, нарочито у погледу криптовалута као првог облика дигиталне имовине. (Auer, Claessens, 2018)Без обзира на активности које су предузели регулатори у појединим земљама, ефекти употребе финансијских технологија су свакако прекогранични, јер криптоимовина је предмет трансакција на глобалном нивоу. Неке земље, као што су Малта, Литванија, Бахами, Уједињени Арапски Емирати, али и Србија доношењем Закона о дигиталној имовини,[1]у дигиталној имовини виделе су потенцијал за раст финансијског сектора и конкурентност на међународном нивоу. Тако фрагментиран приступ и различитости у националним правним оквирима, у условима када не постоје глобална правила, може представљати основ регулаторне арбитраже.

Још увек није постигнут глобални консензус у погледу криптотржишта, изузев донекле ризика прања новца и финансирања тероризма прометом криптовалута. (FATF, 2019) Важно је истаћи да је на нивоу Европске Уније област криптоимовинеу фокусу. Наиме, септембра 2020. године Европска комисија објавила је Стратегију дигиталних финансија и низ докумената,[2] међу којима се издваја нацрт Уредбе о тржиштима крипто-имовине[3] којом се обухватају различити појавни облици дигиталне имовине. За неке се предвиђа нови регулаторни оквир, док се у погледу инвестиционих токена, који имају карактеристике хартија од вредности и инструмената тржишта капитала предвиђасходна примена регулативе о тржишту капитала ЕУ. (Zetsche, Annunziata, Arner, Buckley, 2021) Нацрт Уредбе предвиђа посебна правила за емитенте криптоимовине у Европи и пружаоце услуга повезаних са криптоимовином: дозволу за рад на јединственом тржишту, захтеве у погледу капитала и ликивидности, обавезе информисања улагача и захтеве у погледу решавања притужби, као и права улагача у односу на емитенте. Поменутом нацрту Уредбе претходиле су активности и истраживања европских регулаторних агенција за финансијске услуге (EBA 2019, ESMA 2019), као и Европске централне банке (ЕЦБ, 2015).

На међународном нивоу, неколико организација је укључено у разматрање ризика употребе криптовалута и дефинисање глобалног приступа. Комитет за плаћања и инфраструктуре тржишта (*Committee on Payments and Market Infrastructures*)при Банци за међународна поравнања, углавном је фокусиран на област дигиталних валута централних банака. Међународна организација регулатора хартија од вредности (*International Organization of Securities Commissions*) имала је низ иницијатива у погледу тзв. иницијалне

[1] Закон о дигиталној имовини, *Сл. гласник РС*, 153/2020

[2] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

[3] EuropeanCommission, Proposalfor a RegulationoftheEuropeanParliamentandoftheCouncil on Markets in Crypto-assets, andamendingDirective (EU) 2019/1937COM/2020/593 final.

јавне понуде криптоимоивне инвестиционог карактера, док је Базелски комитет за супервизију банака (*Basel Committee on Banking Supervision*) разматрао питање ризика изложености банака криптоимовини.

Услед бојазни од принудне регулације и традиционалног регулаторног приступа, саморегулаторне организације, створене да заступају интересе *FinTech* индустрије, све се више ангажују у промовисању саморегулаторних правила. Саморегулаторне организације имају за циљ да формулишу заједнички сет смерница и професионалних стандарда понашања за промовисање интегритета, правичности и ефикасности тржишта криптоимовине. Један од најбољих примера је Кодекс понашања који је развила Асоцијација за тржишта дигиталне имовине (ADAM).[4] Други пример је Удружење за виртуелну робу (VCA) које је најавило пројекат формирања саморегулаторне организације за издавање упутстава о најбољим праксама за крипто-имовину, са циљем да створи основу за будућу регулацију сектора и сарадњу са постојећим регулаторним телима.[5]

Криптовалуте су први облик дигиталне имовине који је био предмет регулисања. Из угла глобалне регулаторне перспективе, могу се издвојити четири сценарија (Gaudamuz, Marsden, 2015; Јованић 2020):

> *1) Забрана.* Иако су неки иницијално сматрали да би ризично тржиште криптовалута требало бити забрањено, због чињенице да власти не могу блокирати приступ интернету, потпуна забрана коришћења виртуелних валута у пракси вероватно не би успела и овај сценарио је најмање реалан. Постоје примери земаља које су експлицитно забраниле криптовалуте, односно *bitcoin*: нпр. Бангладеш, Непал, Киргистан, Боливија, Еквадор, Индонезија и Алжир.
>
> *2) Делимична забрана*. Како би умањиле утицај криптовалута на реалну економију, регулатори у неким земљама забрањују поједине начине коришћења криптовалута. На пример, могу бити забрањени продају производа и услуга за криптовалуте, или оснивање берзи криптовалута са седиштем на територији земље. Ту се убрајају и забране са циљем спречавања употребе криптовалута за нелегалне активности (прање новца), што представља најчешћи облик делимичне забране.
>
> *3) Делимична регулација*. Ово подразумева доношење прописа у вези криптовалута којима се омогућава њихово регулисано коришћење и јасан третман у појединим, за државу битним аспектима. На пример,

[4] http://www.theadam.io/code/

[5] www.virtualcommodities.org

прописивање пореског третмана употребе криптовалута. Упоредноправне анализе показују да се највећи број земаља креће ка умереном приступу, где се по правилу не регулишу или не регулишу детаљније трансакције унутар криптовалутних тржишта (нпр. размена једне криптовалуте за другу), а пажња је усмерена ка спречавању коришћења виртуелних валута на начин који може да угрози потрошаче, финансијску стабилности или јавни интерес. У том смислу се делимична регулација може идентификовати са делимичном забраном (нпр. посебан режим спречавања употребе криптовалута као мера спречавања прања новца и финансирања тероризма).

4) Детаљна регулација. Детаљна регулација криптовалута може бити усмерена на учеснике, услуге које пружају, као и на могуће ризике. Организаторима криптовалутних шема и пружаоцима услуга даје се статус финансијских посредника (најчешће кроз различите шеме лиценцирања). Као носиоцима тих статуса додељују им се различите обавезе којима регулаторни органи настоје да обухвате ризике употребе криптовалута и односе се на тржишно понашање учесника, спречавање сајбер превара, интегритет пословања и др. У неким системима посебно се регулишу тзв. чворишта ризика, као што су провајдери дигиталних новчаника, берзе криптовалута. (IMF, 2017) Најзад, и сами алгоритми који се користе у *fintech* иновацијама могу се регулисати с циљем контроле њихове исправности и транспарентности.

Обухват детаљнијег облика регулације посредника, услуга и инфраструктуре шема зависи од врсте дигиталне имовине. У том смислу, једно од основних правила је "иста активност, исти регулаторни оквир", што значи да се криптоимовина по економској функцији уподобљава осталој криптоимовини, или другим финансијским производима и ризицима који произилазе из њихове употребе. Дакле, полазну основу у регулисању требало би да представља њихова доминантна економска функција (плаћање, улагање, остваривање неких користи), као и сличности и разлике у поређењу са другим облицима реалне и финансијске активе.

Уколико се као критеријум за одабир регулаторног приступа постави избор облика регулације и регулаторних инструмената, класификацију коју је предложио Комитет за плаћања и инфраструктуре тржишта, као стално тело при Банци за међународна поравнања, требало би укратко представити. (BIS, 2015:1) Ако се изузме забрана као модалитет интервенције, на националном нивоу шеме могу бити предмет следећа четири облика регулације: 1) информациона регулација и морални притисак; 2)

регулација специфичних финансијских посредника; 3) примена постојећих прописа и 4) проширење опсега примене прописа укључујући и доношење нових прописа.

1) Морални притисак као облик утицаја на тржиште нарочито виртуелних валута, уз фокус на информациону регулацију, усмерен је на ризике и опасности инвестирања у виртуелну имовину и отварања овог тржишта ка широј јавности.Типични примери овог приступа су јавна упозорења о ризицима улагања у криптовалуте, информационе кампање о виртуелним валутним шемама и слично (EBA, 2013, FCA, 2017). Овај облик регулације, са најмање притиска, често представља прекурсор увођењу других облика.

2) Унутар инфраструктуре дигиталне имовине појављују се различити посредници, од којих многи представљају пружаоце специфичних услуга. Примери специфичне регулације финансијских посредника су берзе криптовалута и пружаоци услуга дигиталних новчаника. Начешће се успостављају системи лиценцирања посредника на тржиштима криптовалута, којима се намеће низ обавеза као што су минимални стандарди заштите улагача (нарочито потрошача), обавезе извештавања о ризицима и слично.

3) Посебан метод регулације је примена постојећих прописа, тако да се одређени облици посредовања и одређене услуге обухвате већ постојећим правилима. Један од најбољих примера је примена прописа о тржиштима финансијских инструмената и регулативе о забрани манипулација на тржишту приликом тзв. иницијалне јавне понуде новчића, који по својој природи, као инвестициони токени, представљају еквиваленте финансијских инструмената.

4) Проширивање опсега примене постојећих прописа и евентуално доношење нових прописа је опција која се чини неопходном у ситуацијама када није могуће применити постојеће прописе због специфичности криптовалута. Примера ради, прописи о спречавању прања новца и финансирању тероризма су, услед иницијативе на међународном нивоу која је иницирана од стране FATF-а, проширени како би се обухватиле и трансакције криптовалутама. Поред тога што је потребно обухватити нове пружаоце услуга и нову инфраструктуру (нпр. виртуелни новчаници), дигиталне валуте пред право постављају и низ других питања као што је коначност поравнања, крађе криптовалута и грешке.

3.3. Директна versus индиректна регулација, когентна правила versus принципи

FinTech захтева да се регулаторни оквир заснива на специфичној активности или функцији, а не на облику пружаоца услуге или врсти технологије на којој је заснован. Принцип технолошке неутралности често подразумева регулацију засновану на принципима. Принципи, као општи захтеви који изражавају основне обавезе које сви учесници на тржишту треба да поштују, често су подржани детаљнијим стандардима. Уопштено говорећи, регулација заснована на принципима означава помак од ослањања на детаљна, прескриптивна правила, ка шире формулисаним принципима на вишем нивоу. (Black, Hopper, Band, 2007) У променљивом окружењу, регулаторни приступ треба да буде отпоран и прилагодљив. Ово подразумева да сви нови закони и смернице и будуће измене треба да обезбеде брзе промене и да буду прилагодљиви како би омогућили примену на технологије у настајању. Усвајање фазног и једнообразног приступа заснованог на ризику је у складу са овим принципом. Већи број регулатора сматра да регулаторне мере треба благовремено проценити пре него што се наметну строги захтеви. Сигурност, стабилност и интегритет финансијског система је основни разлог за њихову интервенцију и мере треба да буду сразмерне нивоу ризика, узимајући у обзир потенцијалне користи. Једнообразни приступ значи да сви регулаторни органи на ко је се то односи треба да заједно одреде своје активности како би се обезбедио јасан и доследан третман учесника на тржишту.

Међу свим изазовима са којима се суочавају централизовани директни регулаторни приступи, три се посебно истичу у регулисању крипто-тржишта: ограничења надлежности јавних органа, одређивање опсега регулисаних субјеката и регулаторна арбитража. (Nabilou, 2019: 266) Пошто крипто-имовина често има мешовите карактеристике различитих производа, надзор би подразумевао комбинацију овлашћења различитих регулатора. (BIS, 2018: 108) Недостатак консензуса о природи крипто-имовину (шта регулисати) спречава појаву јединственог приступа регулацији. Сходно томе, намеће се још једно практично питање: кога регулисати? У децентрализованој блокчејн структури, ентитет према коме би регулатива могла да буде усмерена не може се лако идентификовати. На примеру криптовалута, постоји одређени број посредника који играју различите улоге, као што су издаваоци новчића, рудари, берзе и разни други актери. (ECB, 2015: 7-8) Стога се чини да је индиректна регулација прикладнији начин, јер би се могла фокусирати на укрштање дигиталног простора са стварним светом и циљаним посредницима као што су берзе и пружаоци услуга крипто новчаника. Регулација би се могла применити на месту

где се криптовалуте укрштају са банкама и платним институцијама. Директна регулација се, међутим, може суочити са бројним изазовима, као што је регулаторна арбитража, која би се могла ублажити само глобалном координацијом регулатора.

Децентрализована природа нових технологија чини индиректну регулацију посебно погодном за режим тзв. „полицентричне корегулације" заснованом на технологији. Према овом приступу, финансијски супервизори би надгледали субјекте који би омогућили интеракцију између крипто-имовине и новца, финансијских инструмената или других облика стварне имовине. Например, банке и платне институције које нуде рачуне у криптовалутама или инвеститори који купују инвестиционе новчиће могу бити подвргнути пруденцијалним мерама постављеним за управљање ризицима ликвидности. Такав приступ би претпостављао прилагођавање корпуса пруденцијалних правила.

Уопштено посматрано, приступ крипто-имовини се може класификовати у оквиру рестриктивног модела или одобрења. Рестриктивни модел, као што му име сугерише, подразумева да регулатива забрањује неке или све активности које се односе на дигиталну имовину. Такав приступ може негативно утицати на иновације, спречити развој добрих тржишних стандарда, повећати ризик од криминалних активности у вези са виртуелном имовином. Овај модел треба јасно да разграничи шта је дозвољено, а шта није, како би учесници на тржишту разумели обим ограничења. Други модел, у којем је дозвољено, подразумева да се путем тврдог или меког права утврђује обим дозвољених активности. Може се заснивати на све обухватним принципима или обавезним циљевима, који се морају постићи да би активност била дозвољена. Спровођење је свакако изазов за овај приступ, посебно због екстратериторијалног карактера криптотржишта. Да би се избегла забуна у примени принципа и постизању резултата, као и да би се предузећа одвратила од пословања у сивим зонама, правила и стандарди требало би да буду формулисани на јасан начин. Када је заснован на принципима и упутствима, овакав регулаторни режим осигурава флексибилност учесницима у погледу тога како ће се придржавати задатих циљева.

Због њихове еволуирајуће природе и сложености, индиректна регулација крипто-имовине више је подобна регулацији кроз принципе, уместо чврсто дефинисаних когентних правила. Индиректни приступ регулацији помера фокус са регулације засноване на правилима на регулацију засновану на принципима, када је спроводе посредници који обављају трансакције са пружаоцима инфраструктуре или услуга на крипто тржиштима. То је због чињенице да ће такви посредници, као сурогат регулатори, спрово-

дити правила на децентрализованији начин, са више флексибилности у имплементацији, што је условљено самом природом иновација у финансијске технологије, које се стално развијају. (Nabilou, Pacces, 2015) Међутим, претерано ослањање искључиво направила или само на принципе, није довољно, јер принципи служе да би обезбедили више простора за усклађивање пословања у поређењу са статичним правилима из закона. Одатле следи закључак да би финансијска регулатива требало да буде скуп сложених норми које садрже и правила и принципе, пошто већина сложених режима ризика у пракси садржи мешавину правила и принципа. (Ford, 2008) Ако је примарни циљ регулаторне стратегије подстицање иновација као и уштеда ресурса, модел ослањања на принципе омогућава флексибилнији приступ. Међутим, овај регулаторни модел се суочава са једним кључним проблемом: његовом ефикасном имплементацијом. Претерано генерализовање принципа и њихова неодређеност могу одвратити оператере од иновација у областима које нису регулисане, или их мотивисати да заобиђу правила која се односе на услуге које имају сличну економску функцију и које су предмет детаљне регулације (нпр. прописи о електронском новцу, платним услугама, тржиште хартија од вредности и др.).

Модел заснован на принципима подразумева да се оквир истих дефинише прописом или неким актом супервизора који подразумева квазирегулативу. То може бити и упутство регулатора, којима се одређује обухват активности и захтеви који морају бити задовољени да би се добила лиценца или сагласност за обављање одређених услуга. Један од најбољих примера у том смислу је Гибралтар, где постоји широко постављен модел заснован на упутствима који се односи на читав спектар употребе технологије дистрибуиране књиге. Неопходна је лиценца Финансијске комисије Гибралтара за све такве активности, уобличена кроз девет широких принципа, од којих је сваки праћен појединачним упутствима, који омогућавају супервизору флексибилност у доношењу одлуке да ли да дају или одузму дозволу за рад.6 За разлику од овако широког приступа који се односи на целу грану индустрије засноване на блокчејн технологији, пример британске Управе за финансијски надзор (*Financial Conduct Authority*) показује да је приступ заснован на принципима подобан и да се одреде врсте услуга. Наиме, у Упутству о криптоимовини (*Guidance on Cryptoassets*), (FCA, 2019) Управа је формулисала низ препорука финансијским посредницима у циљу избегавања ризика примене постојећих прописа из области тржишта капитала. Уводећи инструмент за процену (регулаторни периметар – *regulatory perimeter*), чија сврха је да се разграниче облици

[6] Gibraltar Financial Services Commission, Distributed Ledger Technology Providers - Guidance Notes, https://www.gfsc.gi/downloads?section=19&type=0

крипто-имовине на које се примењује и они на које се не примењује неки постојећи пропис, постиже се већи ниво правне сигурности.

4. Регулаторне иновације

Многи регулатори су одуговлачили са доношењем регулативе и првобитно издали саопштења у вези ризика употребе криптовалита, како би сагледали могуће користи од *DLT* технологије за своје потребе. У неким земљама регулатори не желе да коче развој финансијских иновација, па прихватају приступ тзв. ограниченог слободног окружења и дозвољавају *start-up* компанијама које желе да започну бизнис заснован на блокчејнтехнологији да послују у релативно повољном и контролисаном окружењу у одређеном времену, како би се сагледале предности и недостаци примене нових технологија. На тај начин се постиже да учесници у развоју нових технологија не буду оштећени, а са друге стране даје им се могућност да наставе са финансијским иновацијама у чијој основи су технолошке иновације. Примера ради, америчка Комисија за трговину робним фјучерсима покренула је пројекат LabCFTC, у оквиру којег се дозвољава тестирање иновативних производа, услуга и пословних модела на реалном тржишту, са реалним корисницима. Сличне иницијативе покренуте су у земљама које настоје да се изборе за место на светском финансијском тржишту. Оваквиприступи могли би представљати облик селективне регулације који је усмерен на тржишта и иновативне финансијске производе.

Савремени регулатори који намеравају да подстакну финансијски инжењеринг настоје да регулисане субјекте ослободе непотребних регулаторних оптерећења и омогуће окружење које омогућава међусобну размену знања између супервизора и надзираних субјеката. Нови регулаторни приступ омогућава регулатору као органу надзора да подстакне дијалог са *FinTech* индустријом и боље разуме нове технологије, што пружа флексибилност да се реагује на непознате ризике. Овај институционализовани дијалог је контролисани простор у којем *FinTech* компаније могу тестирати и валидирати иновативне производе, инфраструктуру и услуге, на ограничено време, а где регулатори дају тумачења и помажу им да се придржавају, и познат је као „*regulatory sandbox*", што би се евентуално могло превести као „ограничено регулаторно окружење". Иако постоје разлике и варијације између њих у различитим земљама, ови механизми имају низ заједничких карактеристика, односно циљева: обезбеђивање заштите потрошача и инвеститора, интегритета тржишта и промовисање иновација и конкуренције. (FSB, 2017) Сваки регулатор може дефинисати услове под којима се надгледаном субјекту одобрава приступ и безбедносни захтеви које

потенцијални учесник треба да испуни. Такав приступ омогућава компанијама које започињу посао заснован на блокчејн технологиј и да у датом тренутку послују у релативно повољном и контролисаном окружењу, како би тестирале предности и мане примене нових технологија. Периоди тестирања су по правилу ограничени на 6 до 12 месеци, одређују се од случаја до случаја. Већина разлика међу националним приступима односи се на ниво компромиса и степен растерећења регулаторних захтева. Без обзира на разлике у приступима, овај модалитет смањује регулаторну несигурност и подстиче компаније да експериментишу у “сивој зони”. Главна предност овог приступа је спречавање преурањених реакција регулатора и убрзавање процене ризика нових технологија. Међутим, неки ризици се могу појавити тек по истеку пробног периода. Овакав приступ може захтевати интензивне ресурсе и претпоставља да постоји искусно особље у кадровски и финансијски добро опремљеним органима јавне управе. Либерални приступ регулатора који немају стручност и ресурсе може довести до појаве неприхватљивих ризика и угрожавања финансијске стабилности. (Zetzche, Buckley, Barberis, Arner, 2017)

Развој финансијске инфраструктуре и финансијског инжењеринга условио је и пораст норми усмерених ка контроли ризика и повећање обавеза извештавања регулатора у циљу побољшања транспарентности. Бројност тих норми и различитост информационих система путем којих регулисани субјекти обрађују податке утицали су на настанак нових механизама за праћење усклађености пословања. Као што је напред већ указано, регулација путем правила није оптимални облик регулације, јер непотпуна правила још увек не могу да обухвате све ризике финансијског инжењеринга. Самим тим приступ заснован на санкцијама, на који се ослања традиционална командно-контролна регулација, не може се сматрати оптималним. Технолошке иновације нису само захватиле регулисане посреднике и њихове услуге, већ и начин извештавања регулатора, као и механизме за вршење контроле пословања од стране супервизора.Ове технолошке иновације у области самог процеса регулације посредника на тржишту дигиталне имовине за свој крајњи циљ имају унапређење усклађености пословања (*compliance*) извршења документарне контроле од стране супервизора. Док такве облике аутоматизације који примарно омогућавају усклађеност пословања регулисаним субјектима и извештавање регулатора неки називају регулаторном технологијом (*RegTech*), други истичу да пандан томе представља тзв. супервизорска технологија (*SupTech*). (Broeders, Prenio, 2018; Arner, Barberis, Buckley, 2016) Супервизорска технологија представља употребу иновативних технологија од стране органа надзора која им омогућава дигитализацију извештавања и разли-

читих сегмената регулаторног процеса, што за циљ има ефикасније и проактивније надгледање ризика финансијског сектора и нивоа усклађености пословања финансијских институција. Примера ради, то су могућности да се повуку подаци из информационих система банака, аутоматски обраде потрошачке притужбе како би се добили потенцијални сигнали у којим областима постоји потреба за детаљнијим надзором и слично.

4. Закључак

Регулатори који прате *FinTech* суочавају се са изазовом како да осмисле флексибилно регулаторно окружење како би се прилагодили фундаменталним променама на финансијском тржишту и подстакли конкуренцију у финансијским услугама. Такви регулатори схватају да високе тржишне баријере у финансијском сектору и недостатак конкурентског притиска успоравају развој финансијског посредовања, те су стога више фокусирани на оснаживање конкуренције и иновације у финансијском систему и склонији регулацији путем принципа као оквирних и флексибилних правила. Да би нове учеснике учинили привлачнијима, владе и финансијски регулатори развијају и/или спонзоришу јединице за подршку иновацијама које су посвећене подстицању финансијских иновација. Институционални подстицаји иновацијама су се појавили као алтернативни и експериментални модели управљања у циљу промовисања технолошких иновација. Било да је реч о институционалној структури којом се од стране регулатора пружају необавезујуће смернице, или да регулатори имају активну улогу у надзору кроз ограничено тест окружење за иновативне посреднике, такав приступ омогућава регулаторима да прате интегритет тржишта и да кроз податке о потенцијалним ризицима остварују заштиту инвеститора, што је један од основних циљева финансијске регулације.

Литература

Arner, D.W., Barberis, J., Buckley R.P. (2017). FinTech, RegTech, and the reconceptualization of financial regulation. *North Western Journal of International Law and Business*. 37(3). 371-414

Auer, R., Claessens, S. (2018) Regulating cryptocurrencies: assessing market reactions. (2018) *BIS Quarterly Review*.51

Bank for International Settlements (BIS). (2015). Committe on Payments and Market Infrastructure. *Digital Currencies*, Basel 2015.

Bank for International Settlements (BIS). (2015). 'Cryptocurrencies: Looking Beyond the Hype', *Annual Econ Report*

Black, J., Hopper, M., Band, C. (2007) Making a success of principles-based regulation. Law and *Financial Markets Review*. 1/3. 191

Broeders, D., Prenio J. (2018), *Financial Stability Insights on Policy Implementation No. 9 Innovative technology in financial supervision (suptech) – the experience of early users*, Financial Stability Institute, BIS, Basel.https://www.bis.org/fsi/publ/insights9.pdf, Преузето 10.09.2021.

Gabor D., Brooks S. (2017). The digital revolution in financial inclusion: International development in the fintech era. *New Political Economy*. 22/7. 423.

Guadamuz A., Marsden C. (2015) Blockchains and Bitcoin: Regulatory responses to cruptocurrencies, *First Monday – Peer Reviewed Journal of the Internet*, 20(12), https://firstmonday.org/ojs/index.php/fm/article/view/6198/5163. Преузето 20.09.2021.

Enriques, L., Ringe WG. (2020) Bank-FinTech Partnerships, Outsourcing Arrangements and the Case for a Mentorship Regime. *Capital Markets Law Journal*. 15. 374

European Banking Authority - EBA (2013). *Warning to Consumers on Virtual Currencies*, EBA/WRG/2013/01, 12. 12. 2013.

European Banking Authority - EBA (2019). *Report with advice for the European Commission on crypto-asset*.

European Central Bank - ECB. (2015).*Virtual Currency Schemes – a further analysis*, Frankfurt am Main, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, Преузето 10.09.2021.

European Commission. (2019).*Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*COM/2020/593 final.

European Securities and Markets Authority - ESMA. (2019).*Advice on Initial Coin Offerings and Crypto-Assets*, Reference No. ESMA50-157-1391, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, Преузето 10.09. 2021.

European Central Bank - ECB. (2015).*Virtual Currency Schemes – a further analysis*, Frankfurt am Main https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf Преузето 05.09. 2021.

Fenwick, M., Vermeulen, Erik P., Kaal, W. (2017). Regulation Tomorrow What Happens When Technology is Faster than the Law. *American University Business Law Review*. 6/3. 561-594.

Financial Action Task Force (FATF). (2014). *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, Преузето 1.10. 2021.

Financial Action Task Force (FATF). (2019). *Guidance for a risk-based approach "Virtual assets and virtual asset service providers",* https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html, Преузето 1.10.2021

Financial Conduct Authority - FCA. (2019). Guidance on Cryptoassets, *Consultation Paper 19/3*, January 2019. https://www.fca.org.uk/publication/consultation/cp19-03.pdf, Преузето 1.10.2021

Financial Conduct Authority - FCA. (2017). *Consumer Warning about the Risks of Initial Coin Offerings ('ICOs'*), (https://www.fca.org.uk/news/statements/initial-coin-offerings, Преузето 1.10.2021

Financial Stability Board - FSB. (2017). Financial Stability Implications from Fintech: Supervisory and Regulatory Issues that Merit Authorities' Attention (27 June 2017) 4f, www.fsb.org/wp-content/uploads/R270617.pdf, Преузето 1.9.2021

Filippi, P. de, Wright, A. (2018). *Blockchain and the Law: The Rule of Code*, Harvard University Press Cambridge.

Ford, C.L. (2008). New Governance, Compliance, and Principles-Based Securities Regulation. *American Business Law Journal*. 45/1. 1-60

International Monetary Fund - IMF. (2017). Fintech and Financial Services: Initial Considerations. *IMF Staff Discussion Note 17/05*, Washington.

Јованић, Т. (2020). Актуелни приступи регулаторном оквиру виртуелних валута - у сусрет закону о виртуелној имовини. У Радовић В. (Прир.) Зборник радова *Усклађивање пословног права Србије са правом ЕУ (2020)*, Београд, Правни факултет Универзитета у Београду.

Koops, BJ. Should ICT Regulation Be Technology-Neutral? (2006).Y Koops, B.J, et al., Starting Points for ICTRegulation: Deconstructing Prevalent Policy One-liners 77 Bert-JaapKoops et al. Starting Points for ICTRegulation, T.M.C. Asser Press.

Nabilou, H. (2019). 'How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency', *International Journal on Law and Technology*. 27/3. 266.

Nabilou H., Pacces A.M., (2015.) The Hedge Fund Regulation Dilemma: Direct Vs. Indirect Regulation. *William and Mary Business Law Review*. 6. 183

Ringe W.G., Ruof C. (2020). Regulating Fintech in the EU: the Case for a Guided Sandbox. *European Journal of Risk Regulation* 3/11. 604

Puschmann, T. (2017). Fintech. *Business and Information Systems Engineering* 59. 69-76.

van der HaarI, M. (2007).Technological Neutrality; What Does it Entail? 23 *TILEC Discussion Paper*, Paper No. 2007-009.

Zetsche D.A., Annunziata F., Arner D.W., Buckley R.P. (2021). The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy.*Capital Markets Law Journal*. 16/2, 203-225

Zetzsche D.A., Buckley, R.B.,Barberis. J., Arner D.W. (2017). Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation. *Fordham Journal of Corporate and Financial Law*, 23(1). 31

Tatjana Jovanić, LL.D.,
Full Professor,
Faculty of Law, University of Belgrade,
Serbia

CRYPTO-ASSETS AS AN EXAMPLE OF THE IMPACT OF DIGITALIZATION ON LAW AND THE REGULATORY PRACTICE

Summary

The increase in trading in virtual currencies and other forms of crypto-assets, as well as the use of the distributed ledger technology is one of the biggest challenges for a modern legal system.This paper does not aim to provide a detailed analysis of the legal nature of cryptocurrencies and the classification of their forms, but primarily the response of national regulators, who are facing the dilemma of whether and to what extent this issue should be regulated, without at the same time stifling financial innovation. This applies not only to regulatory authorities from countries with developed financial markets, but also to countries that are trying to use innovative approaches to ensure a competitive place of their countries in the world of alternative finance, which is developing. In that sense, the dominant focus in this paper will be cast on the directions of development of regulations in the domain of public law and innovative practices in the supervision invoked by national regulatory bodies.

Keywords: *crypto-assets, blockchain technology, regulation, supervision, financial innovations.*

Др Игор Камбовски,
Редовни професор,
Правни факултет Универзитета „Гоце Делчев", Штип,
Северна Македонија

UDK: 004.738.5:347

Е-УГОВОР – ЗАКЉУЧЕЊЕ И ПУНОВАЖНОСТ

Апстракт: *Електронски уговор је споразум (сагласност воља) закључен на даљину електронским средствима комуникације, уз употребу информационих технологија. Међутим, електронска средства се користе не само за закључење уговора, већ и за договарање његовог садржаја и елемената или за утицање на његово извршење. Као и код традиционалног уговора, он настаје у тренутку прихватања понуде или у тренутку постизања сагласности воља две уговорне стране. Да би се правно регулисало закључење уговора разменом електронских докумената, потребно је утврдити: да ли се закључење уговора на овај начин може подвести под већ постојећу разлику закључења уговора inter absentes и inter praesentes, или је реч о новој врсти договарања; и да ли и када употреба електронских докумената задовољава правни и договорени писани (ad solemnitatem или ad probationem) облик. Главно питање које се поставља у анализи електронског уговора је питање пуноважности, односно да ли је уговор закључен електронским путем валидан и да ли се на основу таквог уговора може тражити одговорност за испуњење и извршење обавеза. Брзина и динамика развоја информационих технологија и њихова све већа употреба од стране учесника у трговинским трансакцијама у оквиру е-трговине указују на могућност да ће електронски уговор у блиској будућности „превладати" над формалним писаним уговором због низа предности.*

Кључне речи: *Електронски уговор, закључење, пуноважност.*

1. Увод

Промовисање добара или услуга или активности трговаца у трговинским комуникацијама могу евентуално довести до закључења уговора коришћењем услуга информационог друштва. Интернет не само да омогућава промоцију роба и услуга, већ пружа могућност закључивања уго-

вора електронским путем и испуњавања обавеза онлајн. Услуга се може унапред програмирати подешавањем тзв електронских, аутоматизованих заступника трговца, који ће поруџбине примати у име и за рачун трговца. Већина веб страница је дизајнирана у смеру да могу опслужити потенцијалне купце, односно да им понуде уговор попуњавањем апликације-документа преко којег купац извршава поруџбину одређене робе или услуге. Даље, купац може унети податке о својој кредитној картици и платити цену, а затим се роба или услуге могу одмах испоручити електронским путем, ако постоји таква могућност брзе испоруке[1]. Читаво „преговарање” на Интернету може потрајати само неколико минута.

Електронски уговор је новина у правном уређивању облигационих односа. Заснован је на начелима класичног уговорног права и у свим аспектима прихвата успостављена правна правила која се односе на традиционални уговор. У последњих 20 година многи правници, појединачно или колективно, покушали су да величају или оскврнаве електронски уговор, сваки са својим аргументима. Међународне институције и тела усредсређена на правно регулисање обавеза и трговинских односа вредно су радили и припремили су одличан правни оквир за регулисање ове врсте уговора, који је у облику конвенција, прописа и директива већ прихватила већина држава. Дематеријализација, утврђивање идентитета страна у споразуму, верификација и аутентификација докумената, безбедносни аспекти - све то је дефинисано и регулисано међународним или националним правним инструментима.

2. Закључење електронског уговора

У конкретном случају, две заинтересоване стране могу да користе услуге информационог друштва, као што је е-пошта, за преговарање, достављање понуде и закључење уговора. Директива о Е-трговини 2000/21[2] и не настоји да регулише сваки могући проблем или правно питање које произлази из закључења и извршења ових уговора, већ је остављено да уговорним режимом управљају национална права држава чланица. У сваком случају, Директива уклања законске препреке које могу ометати функционисање јединственог онлајн тржишта усклађивањем одређених аспе-

[1] Овде је нагласак на разлици између индиректне е-трговине (наручивање материјалних добара електронским путем која се затим достављају на традиционалан начин, путем доставне службе, поште итд.) и директне е-трговине (наручивање путем интернета), плаћање и испорука нематеријалних добара и услуга као што су компјутерски софтвер и апликације, музика, филмови и слично).

[2] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031, преглед 30.09.2021 г.

ката уговорног процеса. Такође, утврђује обавезе за добављаче услуга да повећају транспарентност онлајн трансакција и степен заштите права потрошача, у складу са посебном природом Интернета као медија за ове трансакције.

Члан 9 Директиве садржи одредбу која обавезује државе чланице да њихови правни системи неће умањити вредност и валидност електронских уговора или других уговора закључених електронским путем. Ова је одредба примењива и прихваћена и ван Европске уније и све земље које нису чланице ЕУ су транспоновале ту одредбу у домаћим законима о електронској трговини. У стварности, странке могу да обезбеде пуноважност електронских уговора зато што њихови домицилни закони пружају широк спектар радњи које се односе на слободу страна да регулишу своје међусобне односе. Међутим, постоје ситуације у којима је ова слобода ограничена у функцији заштите одређене категорије лица (потрошачи или радници) или када је јавни интерес угрожен (власништво над имовином, породични закон). У тим случајевима валидност уговора може зависити од испуњења неколико формалних захтева: писмене форме уговора, учешћа представника администрације, присуства сведока итд. Одредба обавезује државе чланице, као и све остале државе које су је прихватиле, да елиминишу такве захтеве или да их преименују или прераде у другачијем смислу, како би се омогућило закључивање електронских уговора једнаке важности и правоснажности. Ова обавеза се посебно односи на заштиту права потрошача, где се најчешће инсистира на закључивању уговора у строго писаној форми. Међутим, ова одредба неће и не би требало да спречи све државе да у својим законима задрже одређене специфичне захтеве за одређене врсте уговора, али са могућношћу да се закључе електронским путем.

Према општим принципима уговорног права, уговор се сматра закљученим прихватањем понуде. Сама понуда, као испољавање воље усмерене ка одређеној особи ради закључења уговора, може се поднети, пренети електронским путем, путем е-поште или веб странице. У сваком случају, понуда мора бити прецизна, упућена једној или више одређених особа, а не недефинисаном широком кругу људи који приступају веб локацији као потенцијални купци или партнери, са намером да се, на пример, само информишу о цени одређеног производа. Понуда важи за примаоца у тренутку испоруке понуде, односно тренутка када је примаоцу постала доступна. Опште је прихваћено да се порука-понуда испоручује када се преноси у сферу, у окружењу, у непосредној близини примаоца и прималац се у нормалним околностима може упознати са њом, чак и ако за то није био свестан. (на пример, писмо или порука је достављена у електронско

поштанско сандуче које прималац још није отворио). Овај став је у складу са Директивом 2000/21. Електронска порука можда и неће стићи до примаоца у тренутку чим је послата. Такве поруке могу бити послане ван радног времена или током ноћи, са јасним сазнањем пошиљаоца да ће бити прочитане са закашнењем[3]. Такође је могуће да ће се порука дистрибуирати путем мрежа или сервера који су из техничких разлога блокирани или су успорили пренос. Постоји много варијација на ову тему, али не постоји универзално правило које би покрило и регулисало све ситуације.

Е-директива из 2000 године не садржи одредбе о времену и тренутку закључења уговора, ово питање је остављено да се регулише у националним правима држава чланица. Различите државе с друге стране, регулишући овај важан део договарања, нуде решења заснована на различитим становиштима, према теорији слања, саопштења (изјаве), сазнања или пријема[4]. Тако се, према енглеском праву, излагање производа на веб локацији (веб страници) трговца сматра позивом за закључење уговора, док се према холандском праву сматра јавном, општом понудом или понудом упућеној неограниченом броју лица. Холандски закон регулише да се поруџбина производа или услуга онлајн, под објављеним условима сматра прихватањем понуде и закључењем уговора, док се у енглеском праву поруџбина сматра понудом за куповину, тако да постоји још један корак-прихватање понуде купца од стране продавца, како би се могло сматрати да је уговор закључен[5].

Генерално, већина законодавства је прихватило теорију пријема понуде као најрелевантнију. Након пријема понуде, прималац у условима електронске трговине може прихватити понуду, чиме се сматра да је уговор закључен. Ово је основно правило које се практикује у традиционалној трговини, међутим, у условима електронске трговине прихватање понуде је дискутабилно и помало контроверзно, с обзиром на чињеницу да су понудилац и прималац удаљени један од другог, у времену и простору. Стога остаје неколико отворених питања: где је и када постигнут споразум

[3] Македонски Закон о облигационим односима регулише ово питање у члану 35, став 1-„прихватање понуде са закашњењем сматра се као нова понуда од стране понуђеног". Став 2 гласи: „Уговор је закључен, ако је изјава о прихватању понуде направљена на време, али је стигла до понудиоца по истеку рока за прихватање, а понуудилац је знао или је могао знати да ће се изјава послати на време". Слично и код: Le Tourneau Ph., *La Notion de Contrat Electronique,* Les deuxiemes journees internationals du droit du commerce electronique, Litex, Paris, 2003, стр.10

[4] Le Tourneau, op. cit., стр.13

[5] Коевски Г., *Европската правна рамка за електронска трговија*, Деловно право бр.16/2006, Здружение на правниците од стопанството, Скопје, 2006, стр.272

о уговорним елементима? Може ли се сматрати да веб страница коју је потенцијални купац посетио претставља позив за давање понуде, да је одговор купца, у ствари, понуда, и да трговац овом логичком инверзијом и пермутацијом добија фактичку улогу понуђеног и да је прихватањем понуде заправо закључио уговор[6]?

Тренутак прихватања понуде сматра се тренутком закључења уговора. Овај тренутак, као и место на коме се е-уговор сматра закљученим, веома је важан са аспекта сигурности трговине, као и због могућих правних препрека, спорова и сукоба надлежности које треба да реши суд или арбитража . Историјски гледано, време настанка уговора није било толико важно с обзиром на чињеницу да су стране уговора најчешће биле из истог места или из исте државе, а већина уговора закључена је директно, у присуству обе стране. Откако је трговина почела да користи нове технологије у својим трансакцијама - пошта, телефон, факс или телекс, а у новије време и Интернет и е-пошта, глобална е-трговина била је принуђена да значај времена стварања споразума подигне на виши ниво. Дакле, сматра се да у тренутку када купац изврши онлајн наруџбину на веб локацији трговца, трговац мора одмах, без непотребног одлагања, прихватити наруџбину и о томе обавестити купца, електронским путем. У супротном, уговор није закључен и не обавезује стране[7]. Ово је, као што сам већ навео, најчешће омогућено коришћењем аутоматизованог софтвера, са унапред постављеним параметрима (класични адхезиони уговор!) тако да трговац уопште и нема контакт ни сазнање о закључењу конкретног уговора.

Члан 10 Директиве о електронској трговини покушава да осигура основно начело уговорног права: свака трансакција захтева од заинтересованих страна у том погледу да покажу мотивисану вољу за закључење уговора, због чега морају бити добро информисане о садржају и условима уговора и његовим ефектима и импликацијама на Интернету. У том погледу, Директива обавезује пружаоце услуга информатичког друштва да јасно, прецизно и експлицитно снабдевају уговорне стране са свим информацијама које се односе на уговор или су на било који начин у вези са садржајем и условима уговора. Ове информације укључују различите техничке кораке који воде до закључења електронског уговора, без обзира на то да ли ће уговор бити састављен у компјутеру пружаоца услуга и да ли ће бити до-

[6] Chissick M., Kelman A., *Electronic Commerce-Law and Practise, 3-rd edition,* Sweet & Maxwell, London, 2002, стр.83

[7] видети: Члан 11, тачка 1 Е-Директиве 2000/31; такође: Члан 13. став 1. Закона о електронској трговини: „Прималац услуге приликом наручивања електронским путем дужан је да од пружаоца услуге затражи да достави потврду о пријему наруџбине са посебном електронском поруком, без одлагања и електронским путем"

ступан; техничке мере за идентификацију и исправљање улазних грешака пре подношења понуде, као и језик понуђен за закључивање уговора.

У наставку, члан 10. тачка 3 обавезује пружаоце услуга да омогуће доступност и јавност свих услова и садржаја уговора, како би их заинтересована лица могла репродуковати и складиштити у својим базама података односно трговци морају дозволити приступ и објављивање свих уговорних одредби, елемената и садржаја, пре него што се постигне споразум воља. Коначно, пружаоци услуга морају информисати заинтересоване стране о кодексима понашања којих се придржавају и о томе како се ти кодекси могу претраживати електронским путем. У сваком случају, Европска заједница промовише ову врсту саморегулације са очекивањем да ће допринети ефикасној примени Директиве[8].

Сматра се да се електронски уговори морају додатно оснажити како би се одржао високи ниво заштите права потрошача. Такође, мора се омогућити доступност општих података, у складу са чланом 5 Директиве, преко одговарајућих линкова који воде до одређених веб страница. Ови линкови морају бити лако доступни због приступачности информација потрошачима и олакшавања извршења наруџби путем ових веб страница. Иако ове одредбе доприносе заштити права потрошача, члан 10 (т.1) омогућава уговорним странама да се одрекну транспарентних обавеза у уговорима уз обострану сагласност уговорних страна. Даље, чланом 10. тачка 4, прописано је да се ове обавезе не примењују на уговоре закључене између појединаца путем електронске поште или сличног комуникационог система. У том случају постоји одређени степен флексибилности за оне уговорне односе у којима су преговарачке позиције страна избалансиране и где им слобода преговарања омогућава да те односе формирају према сопственим потребама.

Коначно, члан 11 се односи на наручивање робе и услуга директно на веб страници. Као што је раније утврђено, читав уговорни однос може се водити путем Интернета, на веб локацији трговца. Прво купац бира или прегледа производ или услугу, затим попуњава стандардни образац са својим личним подацима и подацима о кредитној картици, и на крају верификује и шаље те податке једноставним кликом на веб страници. Ово посљедње може имати различите правне импликације у различитим државама чланицама и оставља простор за спор око места и времена закључивања уговора на даљину електронским путем. Тако, одређени правни системи утврђују да је то тренутак када понудилац прими поруку

[8] Lopez-Tarruella A., *A European Community Regulatory Framework for Electronic Commerce,* Kluwer Law International, Common Market Law Rewiew 38, 2001, стр.1367

о прихватању понуде, коју је понуђени послао, док други правни системи за време закључења уговора сматрају тренутак када је понуђени послао поруку за прихватање понуде. Директива по овом питању не даје тачан одговор нити упутства, управо због немогућности његове унификације у различитим правним системима. Према томе, питање о времену када се сматра да је уговор закључен остаје подложно регулисању националних закона који се односе на е-трговину, па се стога регулисање овог правног питања може разликовати у зависности од ситуације.

Члан 11 садржи обавезу пружалаца услуга да обавесте примаоца о извршеној поруџбини без непотребног одлагања, а тиме је утврђено да се налог о поруџбини или сазнање о пријему сматрају примљеним и доступним у тренутку када им странке могу приступити, са својох локација и уређаја. Такво сазнање о пријему има облик онлајн потврде услуге коју је затражио прималац. У другим случајевима, потврда се може послати аутоматизовано, као аутоматска порука из е-поште, под претпоставком да би две уговорне стране требале имати приступ понуди чим стигне у компјутерски систем провајдера услуга. Иако савремена компјутерска технологија омогућава да се утврди да ли је пренос поруке обављен исправно и на време, ипак се могу појавити одређени проблеми. Тако, као што сам већ поменуо, прималац би могао бити спречен да, у извесном временском периоду, проверава е-пошту, односно да прими поруку. Ово је правно питање о којем државе чланице појединачно одлучују и регулишу, с обзиром на чињеницу да није регулисано Директивом.

Е-пошта има своје специфичности као начин комуникације и средство за стварање уговора. У тренутку када понудилац притисне дугме за слање поруке, губи се свака даља контрола над њом. Тако се електронска порука шаље и путује преко Интернета и преусмерава, путем система од неколико мрежа и сервера, све до тренутка када стигне на одредиште. Због тога је, због временске удаљености између слања поруке (која се сматра тренутком изјаве воље) и њеног доласка на крајње одредиште, прихватљиво да се као тренутак закључења уговора може и треба сматрати тренутак пријема или прихватања поруке[9]. Међутим, у сајбер простору порука може да се изгуби, оштети или једноставно одбије од стране система личне или корпоративне безбедности (Firewall), тако да неће доћи до примаоца, или ће можда стићи нечитка порука. У таквим случајевима, пошиљалац најчешће добија повратну поруку у којој га систем обавештава да порука није стигла на одредиште и да он може контактирати примаоца или поново по-

[9] Македонски Закон о електронској трговини нуди релативно широку формулацију по овом питању. Тако је у члану 14. став 2. наведено да ће се "понуда и прихватање понуде сматрати примљеним када су постале доступне странкама којима су упућене"

слати поруку. Македонски Закон о електронској трговини[10] (члан 14. став 1.) једноставно регулише питање тренутка закључења уговора, односно прихвата тренутак када ће „... понуђач примити електронску поруку која садржи изјаву примаоца да прихвата садржај уговора"[11].

Закључење електронског уговора поставља неколико важних дилема у погледу правног аспекта електронског трговања. Наиме, правни стручњаци указују на неколико проблема који би могли настати током електронских трансакција, а које законодавци морају имати на уму приликом регулисања и стандардизације ове области. Дакле, главно питање које се поставља у анализи електронског уговора је питање валидности таквог уговора, односно да ли је уговор закључен електронским путем валидан и да ли се на основу таквог одговора може тражити извршење обавеза? Уопштено, прихваћено је да се таква врста уговора сматра важећом, односно највећи број законодавства има савремене законе о електронској трговини, усклађене са међународним правним актима и правилима, који наводе да се електронском уговору не сме оспоравати пуноважност и валидност због дематеријализоване форме у којој је закључен, односно због одступања од традиционалне писане форме уговора, ако испуњава одређене услове који постоје у свету традиционалних писаних уговора[12]. Такав приступ овом питању, или тзв. Функционално еквивалентан приступ, заузела је Комисија УНЦИТРАЛ-а за међународно трговинско право. Наиме, стручњаци из ове комисије сматрају да би било радикално и неоправдано почети са процесом промена класичних начела уговорног права која су постојала пре појаве електронских трансакција, и да би успостављене принципе требало применити и на нове технологије и технике договарања, уз дозвољена неопходна прилагођавања. У том контексту, питање пуноважности и валидности електронских уговора решено је наведеним функционално еквивалентним приступом, уз одговарајућа прилагођавања сваком правном систему појединачно[13].

3. Закључак

У савременим друштвима, у условима развоја дигиталне економије, индустрија и услужне делатности су оријентисане ка достигнућима и предно-

[10] http://www.slvesnik.com.mk/Issues/32B42231FD9864439992FB072DC990FE.pdf#page=2, преглед 26.09.2021 г.

[11] исто и код: Van Esch R., *Electronic Contracting: The European Approach,* Les deuxiemes journees internationals du droit du commerce electronique, Litec, Paris, 2003, стр.30

[12] Le Tourneau, op.cit., стр.8

[13] Živković V., *Elektronska trgovina-Pravo Informacionih tehnologija*, Pravni fakutelt Univerzitet UNION, Službeni glasnik, Beograd, 2007, стр.132

стима које пружа информационо друштво. Међутим, без поверења у уговоре закључене електронским путем, нове економије неће моћи да остваре свој пуни потенцијал и заостајаће за могућностима које нуде нове технологије. Тако, треба повећати поверење у техничке могућности и валидност електронског уговора или пронаћи потпуно нови концепт за регулисање размене добара и услуга у новој дигиталној ери. У сваком случају, лакше је и прихватљивије створити техничка решења за правну валидност е-уговора, од суштинског редефинисања правних уговорних механизама који вековима успешно делују. С друге стране, правни систем створен још за време Римског царства није био припремљен и није нудио озбиљну основу за увођење нових начина комуникације и закључивање уговора. Ова тема изазива озбиљне дилеме и велика је провокација за савремену науку у покушају успостављања савремених правних стандарда и инструмената који ће регулисати нове начине трговања и преговарања, уз поштовање правне традиције и утврђених правних правила уговорног права.

Литература

Le Tourneau Philippe, *La Notion de Contrat Electronique,* Les deuxiemes journees internationals du droit du commerce electronique, Litex, Paris, 2003

Коевски Горан, *Европската правна рамка за електронска трговија,* Деловно право бр.16/2006, Здружение на правниците од стопанството, Скопје, 2006

Chissick Michael, Kelman Alistair, *Electronic Commerce-Law and Practise, 3-rd edition,* Sweet & Maxwell, London, 2002

Lopez-Tarruella Aurelio, *A European Community Regulatory Framework for Electronic Commerce,* Kluwer Law International, Common Market Law Rewiew 38, 2001

Van Esch Rick, *Electronic Contracting: The European Approach,* Les deuxiemes journees internationals du droit du commerce electronique, Litec, Paris, 2003

Živković Vesna, *Elektronska trgovina-Pravo Informacionih tehnologija*, Pravni fakultet Univerzitet UNION, Službeni glasnik, Beograd, 2007.

Igor Kambovski, PhD,
Full Professor,
Faculty of Law - University "Goce Delchev", Shtip
Republic of North Macedonia

E-CONTRACT – CONCLUSION AND VALIDITY

Summary

The electronic contract is an agreement concluded at a distance by electronic means of communication, with the use of information technologies. However, electronic means are used not only for concluding the contract, but also for agreeing on its content and elements, or for influencing its performance and its execution. As with the traditional contract, it occurs at the moment of accepting the offer, or at the moment of reaching the agreement of the wills of the two contracting parties. In order to legally regulate the conclusion of the contract by way of exchange of electronic documents, it is necessary to determine: whether the conclusion of agreements in this way can be subsumed under the already existing distinction of conclusion of contracts inter absentes and inter praesentes, or becomes an assembly for a new type of conclusion; and whether and when the use of electronic documents satisfies the legal and agreed written (ad solemnitatem or ad probationem) form. The main question that arises in the analysis of the electronic contract is the question of the validity, ie whether the agreement concluded by electronic means is valid and whether on the basis of such an answer can be sought execution liability. The speed and dynamics of the development of information technologies and their increasing use by the participants in the trade transactions within E-Commerce indicate the fact that the electronic conctract in the near future will "prevail" over the formal written contract due to a number of advantages.

Keywords: *Electronic contract, conclusion, validity.*

Др Драган Јовашевић*[1]*,
Редовни професор,
Правни факултет Универзитета у Нишу,
Србија

UDK: 343.533:004

РАЧУНАРСКА ПРЕВАРА (КРИВИЧНА ОДГОВОРНОСТ И КАЖЊИВОСТ У МЕЂУНАРОДНОМ И НАЦИОНАЛНОМ ПРАВУ)[2]

Апстракт: *На бази усвојених међународних докумената универзалног и регионалног каратера највећи број држава, па тако и Република Србија, у свом националном законодавству познају више рачунарских (компјутерских) кривичних дела којима се штите различите дигиталне базе података. За учиниоце ових специфичних кривичних дела прописана је кривична одговорност и кажњивост физичких и правних лица. Поред специфичних рачунарских кривичних дела, у савременим условима и бројна стара класична кривична дела (крађа, превара, фалсификовање) добијају нову димензију са већим степеном тежине и опасности када се врше употребом рачунара или рачунарских система. Будући да се ради о криминалитету где најчешће нема временске и просторне повезаности учиниоца и његове радње извршења и проузроковане последице, односно оштећеног лица, то савремена законодавства познају и посебне доказне радње у поступку откривања и доказивања ових кривичних дела. Управо о појму и карактеристикама рачунарске преваре као облику рачунарског криминалитета у међународном и националном кривичном праву говори овај рад.*

Кључне речи*: рачунарски криминалитет, превара, закон, кривично дело, одговорност, кривична санкција.*

---

[1] jovas@prafak.ni.ac.rs

[2] Рад је настао као резултат финансирања од стране Министарства просвете, науке и технолошког развоја РС према уговору број 451-03-9/2021-14/200120.

1. Уводна разматрања

Усвајањем Закона о изменама и допунама Кривичног закона Републике Србије[3] априла 2003. године на бази прихваћених међународних стандарда у систем домаћег кривичног права је по први пут уведено више рачунарских (компјутерских) кривичних дела, те су одређена правила о кривичној одговорности и кажњавању њихових учинилаца. Наиме, у новоуведеној глави 16А. Кривичног закона предвиђена су кривична дела против безбедности рачунарских података. На тај начин се и наша држава прикључила низу савремених држава које се на различите начине (у првом реду системом кривичних санкција) покушавају ефикасно, законито и квалитетно супротставити различитим облицима и видовима злоупотребе рачунара у циљу остварења противправне имовинске користи за себе или друго физичко или правно лице, односно у циљу наношења (имовинске) штете другом лицу или ради повреде права другог лица.

После законодавне реформе 2005. године донет је Кривични законик Републике Србије[4] који у глави двадесет седмој под називом: „Кривична дела против безбедности рачунарских података'' прописује бројна рачунарска кривична дела.

2. Кривичноправна заштита рачунарских података

Због постојања различитих облика и видова испољавања злоупотребе рачунара у свакодневним животним ситуацијама домаће кривично законодавство прописује више рачунарских кривичних дела које назива „кривична дела против безбедности рачунарских података''. Но, сва та поједина кривична дела поред бројних различитости, имају и низ специфичних карактеристика које су им заједничке. Рачунар, у сваком случају, представља једну од најзначајнијих и најреволуционарнијих тековина развоја техничко-технолошке цивилизације на крају 20.века. Но, поред бројних предности које собом носи и огромне користи за човечанство, рачунар је убрзо постао и средство за разне злоупотребе од стране несавесних појединаца, група, па и читавих организација. Тако настаје рачунарски криминалитет као посебан и специфичан облик савременог криминалитета по структури, особеностима, облицима испољавања, карактеристикама учиниоца, начину и средствима извршења итд. (Ђорђевић, 2011:181-182).

[3] Службени гласник РС, 39/03.

[4] Службени гласник РС, 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94 /16 и 35/19.

Овај вид криминалитета још увек не представља заокружену феноменолошку категорију, те га је немогуће дефинисати јединственим и прецизним појмовним одређењем. Рачунарски криминалитет је само општа форма кроз коју се испољавају различити облици криминалне делатности уз помоћ или посредством рачунара. Наиме, то је криминалитет који је управљен против безбедности рачунарских (информатичких, компјутерских) система у целини или његових појединих делова на различите начине и различитим средствима у намери да се себи или другом физичком или правном лицу прибави противправна имовинска корист или другоме нанесе каква, најчешће, имовинска штета.

2.1. Објект рачунарских кривичних дела

Објект заштите код рачунарских кривичних дела јесте безбедност рачунарских (компјутерских) података и система, односно рачунарске мреже. Иако је данас уобичајено да се ова кривична дела обухватају појмом „компјутерски'' криминалитет[5], наш је законодавац за њих ипак употребио термин „рачунарски'' криминалитет. Но, поред овог назива за кривична дела систематизована на овом месту, домаће законодавство употребљава и појам „високотехнолошки'' криминал[6]. Под овим се појмом подразумева вршење кривичних дела код којих се као објекат или као средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, рачунарски системи, као и њихови производи у материјалном или електронском облику (Јовашевић, 2017:239-240).

При томе је сам законодавац у члану 112. Кривичног законика одредио појам и карактеристике објекта напада код ових кривичних дела. То су: а) рачунарски податак, б) рачунарска мрежа, в) рачунарски програм, г) рачунарски вирус, д) рачунар и ђ) рачунарски систем. Тако је рачунарски податак свако представљање чињеница, информација или концепта у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију (члан 112. став 17. КЗ). Рачунарска мрежа представља скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући податке (члан 112. став 18. КЗ). Као рачунарски

[5] Овај појам користе: Кривични законик Северне Македоније после новеле Кривичног законика (Службен весник на РМ, 19/04) и Кривични законик Републике Српске (Службени гласник РС, 64/17).

[6] Појам, карактеристике, органи кривичног гоњења и поступак за кривична дела високотехнолошког криминала уређени су одредбама Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала (Службени гласник РС, 61/05).

програм сматра се уређени скуп наредби који служи за управљање радом рачунара, као и за решавање одређеног задатка помоћу рачунара (члан 112. став 19. КЗ). Рачунарски вирус је рачунарски програм или други скуп наредби који је унет у рачунар или рачунарску мрежу, који је направљен да сам себе умножава и делује на друге програме или податке у рачунару или рачунарској мрежи додавањем тог програма или скупа наредби једном или више рачунарских програма или података (члан 112. став 20. КЗ). Рачунар је сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке (члан 112. став 33. КЗ). И коначно, рачунарски систем је сваки уређај или група међусобно повезаних или зависних уређаја од којих један или више њих, на основу програма врши аутоматску обраду података (члан 112. став 34. КЗ).

2.2. Појам рачунарских кривичних дела

Компјутер (рачунар) представља једну од најзначајнијих и најреволуционарнијих тековина техничко-технолошког развоја на крају 20. века. Но, поред бројних и различитих предности које рачунар носи са собом и огромне користи за човечанство, он је убрзо постао и средство злоупотребе од стране несавесних појединаца или група. Тако настаје рачунарски криминалитет као посебан и специфичан облик савременог криминалитета. Захваљујући огромној моћи рачунара у меморисању и брзој обради великог броја података, аутоматизовани информациони системи постају све бројнији и незамењиви пратилац целокупног људског и друштвеног живота физичких и правних лица.

Различите форме примене рачунара у свим областима живота, привреде, јавне управе и других друштвених делатности нису остале незапажене од стране несавесних и злонамерних појединаца или група који не бирајући средства и начине покушавају да прибаве за себе или другог противправну имовинску корист или да другоме нанесу какву, најчешће, имовинску штету. Тако рачунар постаје средство, оруђе за извршење бројних кривичних дела. За различите облике и видове злоупотребе рачунара у теорији се употребљавају и различити називи као што су: злоупотреба рачунара (*computer abuse*), деликти уз помоћ рачунара (*crime by computer*), компјутерска превара (*computer fraud*), информатички криминалитет, рачунарски криминалитет, сајбер криминалитет, техно криминалитет итд.

Иако се у правној теорији (Стојановић, Делић, 2013:257-258) могу уочити различита одређења појма рачунарског криминалитета, мишљења смо да се под овим појмом подразумева свеукупност различитих облика, видова и форми испољавања противправних понашања физичких или правних

лица управљених против безбедности рачунарских, информационих и компјутерских система у целини или њихових појединих делова на различите начине и различитим средствима у намери да се себи или другом прибави корист (имовинске или неимовинске природе) или да се другоме нанесе штета.

Из овако одређеног појма рачунарског криминалитета произилазе његове основне карактеристике. То су: а) објект заштите је безбедност рачунарских података или информационог система у целини или његовог појединог дела (сегмента), б) посебан, специфичан карактер и природа противправних делатности појединаца, в) посебна знања и специјализација на страни учиниоца ових кривичних дела која искључује могућност да се свако, било које лице нађе у овој улози, г) посебан начин и средство предузимања радње извршења – уз помоћ или употребом (злоупотребом) рачунара и д) намера учиниоца као субјективни елеменат у време предузимања радње која се огледа у намери прибављања за себе или другог користи или наношења штете другом физичком или правном лицу.

Рачунарски криминалитет карактерише велика динамика и изузетна шароликост појавних облика, форми и видова испољавања. То је и разумљиво јер се ради о новој технологији са великим могућностима примене у широкој сфери људске, друштвене и привредне делатности, те су и могућности злоупотребе рачунара сваки дан све веће. Поред нових појавних облика раније, већ познатих кривичних дела која под утицајем злоупотребе компјутера мењају традиционални, класични начин и модус испољавања (крађа, превара, фалсификовање исправа), јављају се и нови облици противправног и кажњивог понашања који не познају границе између држава (прављење рачунарског вируса). Штетне последице рачунарских кривичних дела су велике и испољавају се у наступању имовинске штете за физичка или правна лица (понекад и за целу државу), у губитку пословног угледа, губитку поверења у сигурност и истинитост рачунарског пословања и уопште рачунарских података, опасности од злоупотребе по слободе и права човека и грађана на разне начине, одавање личне, пословне и других видова тајни и сл. (Turković et al., 2013:345).

2.3. Остали елементи рачунарских кривичних дела

У теорији кривичног права се у област рачунарског криминалитета сврставају различити облици противправног, недозвољеног понашања као што су: а) рачунарска превара, б) финансијске крађе, преваре, утаје и злоупотребе, в) крађа добара, г) фалсификовање података и исправа, д) вандализам, ђ) саботажа, е) хакерисање, ж) рачунарска шпијунажа и з) крађа

времена. Велике практичне могућности које пружа савремена високо софистицирана рачунарска и информатичка технологија са собом носе и опасност од ширења и масовне употребе електронског прислушкивања, крађе пословних и других тајни, као и различитих облика интелектуалне својине, затим озбиљног нарушавања приватности и угрожавања људских слобода и права, као и личног интегритета, а у последње време је присутна и реална опасност од таласа различитих облика терористичког деловања (тзв. „техно'' или „сајбер'' тероризам).

Извршиоци рачунарских кривичних дела представљају специфичну категорију лица. Ради се, углавном, о неделинквентним и социјално прилагодљивим, ненасилним личностима. Они за вршење кривичних дела путем рачунара морају да поседују одређена специјална, стручна и практична знања и вештине у домену информатичке и рачунарске технике и технологије. Поред тога, ради се о лицима којима су оваква техничка средства (рачунари) доступна у физичком смислу.

Ова се кривична дела врше прикривено, често без видљиве просторне и временски блиске повезаности између учиниоца дела и оштећеног (пасивног субјекта). У пракси постоји већа или мања временска разлика између предузете радње извршења кривичног дела и тренутка наступања његове последице. Ова се дела тешко откривају, а још теже доказују, дуго времена остају практично неоткривена, све док оштећени не претрпи штету у домену информатичких и рачунарских података или система. Ради се о криминалитету који брзо и лако мења форме и облике испољавања, границе међу државама, као и врсту оштећеног (Pavišić, Grozdanić, Veić, 2007:559-560).

У погледу кривице, ова се дела врше искључиво са умишљајем.

Кривични законик Републике Србије у глави двадесет седмој под називом: „Кривична дела против безбедности рачунарских података'' предвиђа следећа рачунарска кривична дела: а) оштећење рачунарских података и програма, б) рачунарска саботажа, в) прављење и уношење рачунарских вируса, г) рачунарска превара, д) неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података, ђ) спречавање и ограничавање приступа јавној рачунарској мрежи, е) неовлашћено коришћење рачунара или рачунарске мреже и ж) прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података.

3. Европски стандарди заштите рачунарских система

Савет Европе је доношењем Конвенције о виокотехнолошком (кибернетичком, рачунарском, сајбер) криминалу - ETC 185 од 23. новембра 2001. године[7] поставио основе јединственог европског система кривичног права у области неопходне сарадње држава чланица на сузбијању различитих облика и видова рачунарског криминалитета (укључујући и рачунарску превару). При томе је сама Конвенција (чл. 2-13.) прописала више кривичних дела која су управљена против тајности, целовитости и доступности рачунарских података и система. На овај начин су постављене основе за поједина национална законодавства да прецизније одреде обележја и карактеристике појединих рачунарских кривичних дела, њихове основне, лакше или теже облике, те да пропишу кривичне санкције за њихове учиниоце (физичка или правна лица). Уз ову Конвенцију је усвојен и Допунски протокол о криминализовању аката расистичке и ксенофобичне природе која су учињена посредством рачунарских система. Протокол у чл. 3-7. прописује кривичну одговорност и кажњивост за злоупотребу рачунара у вршењу кривичних дела из расистичких и ксенофобичних побуда (мотива).

Имајући у виду утврђене обавезе за државе чланице Савета Европе, било је логично очекивати да ће и у кривичном законодавству Србије уследити, прво, на законодавном плану, па потом и у пракси ефикасна, квалитетна и законита борба са рачунарским криминалитетом и њиховим извршиоцима (Pavišić, 2006:261-263).

У основи Конвенције о високотехнолошком криминалу као обавезујућем међународном документу који је донет од стране најзначајније и најмасовније европске регионалне организације налази се више претходно донетих препорука као што су: а) Препорука број Р (85) 10 о практичној примени Европске конвенције о узајамној помоћи у кривичним предметима у погледу пружања међународне кривичноправне помоћи при пресретању комуникација, б) Препорука број Р (88) 2 о пиратству на пољу ауторских и сродних права, в) Препрорука број Р (87) 15 која прописује употребу личних података у области делатности полиције, г) Препорука број Р (95) 4 о заштити личних података на подручју телекомуникационих услуга са посебним освртом на улогу телефоније, д) Препорука број Р (89) 9 о рачунарском криминалу која даје смернице националним органима у погледу дефинисања појединих рачунарских кривичних дела и ђ) Препорука број Р (95) 13 о проблемима кривично процесог права који су везани за информатичку технологију.

[7] Службени гласник РС, 19/09.

Конвенција о високотехнолошком криминалу предвиђа низ правних средстава, мера и поступака који су нужни ради одвраћања лица од радњи које су усмерене против тајности, целовитости и доступности рачунарских, система, мрежа и рачунарских података, као и за одвраћање од њихове злоупотребе у било ком виду (Шкулић, 2020:117-119). На тај начин се олакашава откривање, истраживање и кривични прогон тих дела и њихових учинилаца на домаћем и међународном нивоу и осигурава ефикасна и брза међународна сарадња. У члану 1. Конвенција је дефинисала основне појмове рачунарског (кибернетичког, сајбер) криминалитета као што су: а) рачунарски систем, б) рачунарски податак, в) давалац услуга и г) подаци о саобраћају. На овај начин је дато упутство националном законодавцу да у овом смеру обезбеди ефикасну, квалитетну и закониту заштиту ових вредности као објеката кривичноправне заштите.

Дакле, члан 1.Конвенције у поглављу првом под називом: „Употреба термина” даје појмове везане за рачунарски криминалитет. Тако рачунарски систем означава сваки уређај или групу међусобно повезаних или зависних уређаја, од којих један или више њих, на основу програма, врши аутоматску обраду података. Рачунарски податак означава свако представљање чињеница, информација или концепата у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију. Појам давалац услуге означава: а) сваки јавни или приватни субјект који корисницима своје услуге пружа могућност комуницирања преко рачунарског система и б) сваки други субјект који обрађује или чува рачунарске податке у име такве комуникационе услуге или корисника такве услуге. Коначно, податак о саобраћају означава сваки рачунарски податак који се односи на комуникацију преко рачунарског система, произведену од рачунарског система који је део ланца комуникације, а у којој су садржани подаци о пореклу, одредишту, путањи, времену, датуму, величини, трајању или врсти предметне услуге.

4. Рачунарска превара као кривично дело

4.1. Рачунарска превара у међународном кривичном праву

У другом поглављу Конвенције под називом: „Казнено материјално право” у више одредби су дати појам и карактеристике појединих кривичних дела које треба инкриминисати у националним правним системима држава чланица Савета Европе. То су:

1) кривична дела против тајности, целовитости и доступности рачунарских података и система (чл. 2-6.): а) незаконти приступ, б) незаконито пресретање, в) ометање података и г) ометање система и злоупотреба уређаја,

2) рачунарска кривична дела (чл.7-8.): а) рачунарско фалсификовање и б) рачунарска превара,

3) кривична дела у вези са садржајем (члан 9) - кривична дела везана за дечју порнографију и

4) кривична дела повреде ауторских и сродних права (члан 10.).

Међу овим кривичним делима, од значаја за тему нашега рада, јесу следеће одредбе садржане у одељку другом под називом: "Дела у вези са рачунарима". То су два кривична дела: а) фалсификовање у вези са рачунарима (члан 7.) и б) превара у вези са рачунарима (члан 8.).

„Фалсификовање у вези са рачунарима" представља кривично дело из члана 7. Европске конвенције. Оно се састоји у уношењу, мењању, брисању или прикривању рачунарских података које за последицу има неверодостојност података, с циљем да се они сматрају веродостојним и да се са њима у правном саобраћају поступа као да су веродостојни, без обзира да ли су ти подаци директно читљиви и разумљиви, када је тп учињено са намером и противправно. При томе поједине државе могу да као елеменат овог дела предвиде постојање намере за обману другог лица или сличне нечасне намере.

Ово кривично дело чине следећи конститутивни елементи:

а) објект напада је рачунарски податак,

б) радња извршења је алтернативно прописана као: 1) уношење, 2) мењање, 3) брисање и 4) прикривање рачунарских података,

в) последица дела је угрожавање безбедности рачунарских података у виду наступања неверодостојности (неистинитиости) рачунарских података,

г) радња извршења се предузима са одређеним циљем. Тај циљ мора да постоји код учиниоца у време извршења дела, али он не мора бити остварен у сваком конкретном случају. Тако учинилац предузима радњу извршења са циљем да се рачунарски подаци сматрају веродостојним (тачним, истинитим, тако да одговарају објективној стварности) и да се са њима у правном саобраћају поступа као да су

веродостојни, без обзира да ли су ти подаци директно читљиви и разумљиви,

д) учинилац поступа са умишљајем (намером) као обликом кривице и

е) радња извршења се предузима на одређени начин – противправно, кршењем постојећих прописа.

Поједине државе могу да као елеменат овог дела предвиде постојање намере за обману другог лица (довођење у заблуду – погрешну или непотпуну представу, свест или одржавање у заблуди другог лица) или сличне нечасне (неморалне, дифамне) намере, што би указивало на директан умишљај као облик кривице учиниоца.

Друго кривично дело из члана 8. Конвенције носи назив: „Превара у вези са рачунарима". Ово се кривично дело састоји у уношењу, мењању, брисању или прикривању рачунарских података или у ометању рада рачунарског система, са преварном или нечасном намером да се неовлашћено прибави противправна имовинска корист за себе или другога чиме се другом лицу нанесе имовинска штета када је учињено са намером и противправно.

Из оваквом решења садржаног у Конвенцији Савета Европе произилази да кривично дело: „Преваре у вези са рачунарима" представља само посебан, специјални облик преваре као класичног имовинског кривичног дела.

Објект заштите је двојако одређен. То су: а) безбедност рачунарских података и б) имовина (покретна или непокретна) другог физичког или правног лица.

Као објект напада код овог дела јављају се: а) рачунарски податак и б) рачунарски систем.

Радњу извршења чине следеће алтернативно одређене делатности. То су (Мрвић, 2005:324): а) уношење – уписивање новог до тада непостојећег податка, б) мењање – промена облика или садржине већ унетог податка, в) брисање – физичко уклањање податка са места на коме се до тада налазио и г) прикривање – премештање податка са места на коме се налазио и склањање на друго непознато, скривено место. Све наведене радње се предузимају у односи на рачунарски податак. Коначно, као радња извршења овог дела се јавља и ометање рада рачунарског система. То је делатност чињења или нечињења којом се привремено или делимично отежава или усложава ефикасно, квалитетно и благовремено функционисање рачунарског система.

За постојање овог кривичног дела је потребно да је радња извршења у било ком од алтернативно предвиђених облика испољавања предузета:

а) са одређеном намером. То је преварна или нечасна намера да се на овај начин неовлашћено прибави противправна имовинска корист за себе или друго (физичко или правно) лице. Ова намера указује на директан умишљај као облик кривице учиниоца. Она мора да постоји на страни учиниоца дела управо у време предузимања радње извршења, али она не мора да буде остварена у сваком конкретном случају и

б) на посебан, специфичан начин – противправно, кршењем постојећих (законских или подзаконских) правила понашања.

Последица овог рачунарског кривичног дела се јавља у виду повреде. То је наступање за друго физичко или правно лице имовинске штете чија се висина утврђује као фактичко питање према тржишним условима у време извршења дела. Дакле, овде се ради о класичној последици имовинских кривичних дела у виду смањења постојеће имовине или спречавања њеног увећања.

Од посебног значаја за правну квалификацију дела јесу и одредбе Конвенције које изричито захтевају од држава чланица да се пропише кривична одговорност и кажњавање за покушај рачунарских кривичних дела, као и за поједине облике саучесништва у виду подстрекавања и помагања. Поред тога, Конвенција, поред одговорности физичких лица, за ова кривична дела предвиђа и кривичну одговорност правних лица. Покушај, помагање или подстрекавање на извршење рачунарских кривичних дела су кажњиви сходно одредбама члана 11.петог одељка, под условом ако су ове радње предузете са умишљајем (намером) учиниоцица.

Но, поред физичког лица, према Конвенцији Савета Европе (члан 12.), за рачунарска кривична дела, одговарају и правна лица. Наиме, правна лица се сматрају одговорним за рачунарска кривична дела која је у њихову корист извршило било које физичко лице, делујући као појединац или као члан органа правног лица, ако има руководећу улогу у правном лицу, на основу: а) овлашћења да заступа правно лице, б) овлашћења да доноси одлуке у име правног лица и в) овлашћења да врши контролу унутар правног лица. Но, правна лица су одговорна за рачунарска кривична дела и када је непостојање надзора или контроле од стране физичког лица које има руководећу улогу у правном лицу или физичког лица као члана органа правног лица омогућило (олакшало, потпомогло) извршење рачунарског кривичног дела које је извршило физичко лице у корист тог правног лица, на основу овлашћења правног лица.

4.2. Рачунарска превара у кривичном праву Србије

Све наведене европске стандарде је позитивно кривично законодавство Србије у потпуности имплементирало у свој правни систем обезбеђујући врсту и меру казне за поједина кривична дела, као и формирајући посебне органе у оквиру полиције, јавног тужилаштва и Вишег суда у Београду за борбу против високотехнолошког криминала где спадају наведена рачунарска кривична дела.

„Рачунарска превара" представља кривично дело из члана 301. Кривичног законика Србије. Дело се састоји у уношењу нетачног податка, пропуштању уношења тачног податка или на други начин прикривању или лажном приказивању податка чиме се утиче на резултат електронске обраде и преноса података у намери да се себи или другом прибави противправна имовинска корист и тиме проузрокује имовинска штета другом лицу. Ово је посебан, специјални облик имовинског кривичног дела преваре, које карактерише посебан, специфичан начин, односно средство извршења – рачунар (Ђорђевић, Ђорђевић, 2021:193).

Објект заштите овог дела је одређен као безбедност рачунарских система од уношења нетачних, неистинитих података и поверење у ове системе.

Радња извршења се састоји из две алтернативно предвиђене делатности. То су: а) прикривање и б) лажно приказивање рачунарског податка.

Прикривање је неуношење неког податка или потпуно или делимично пропуштање да се уопште или у одређеном року, на одређени начин унесе неки податак од стране лица које је обавезно да исти унесе у рачунар или рачунарску межу. Може се радити о било каквом податку.

Лажно приказивање рачунарског податка постоји када се у рачунарској мрежи приказује, објављује, уноси или користи неистинити податак (било да је у потпуности или делимично неистинит, лажан, тако да не одговара објективној стварности).

Обе делатности морају бити предузете у односу на податак који је по свом значају, природи, карактеру, времену уношења или начину употребе такав да је подобан да утиче на резултат (ток и поступак) електронске обраде и преноса података у рачунарском систему. Било која од ових делатности у смислу кривичног дела мора бити предузета на законом одређени начин: а) уношењем – уписивањем до тада непостојећег, нетачног (неистинитог, лажног у целини или делимично) податка, б) пропуштањем да се унесе, неуношењем, неуписивањем тачног податка (који је истинит, који одговара објективној стварности) в) на било који други начин (Ђорђевић, Коларић, 2020:196-197).

Све алтернативне, законом прописане, делатности у смислу радње извршења овог кривичног дела морају бити предузете у одређеној намери – намери да учинилац за себе или друго (физичко или правно) лице прибави противправну имовинску корист. Та намера мора да постоји на страни учиниоца у време предузимања радње, али она у конкретном случају не мора бити и остварена.

Последица дела се јавља у виду повреде која се огледа у проузроковању имовинске штете за друго физичко или правно лице. Може се радити о штети у било ком износу или обиму, која се огледа, манифестује на нечијој имовини у смислу њеног умањења или спречавања њеног увећања. Овако наступела штета треба да се налази у узрочно-последичној вези са предузетом радњом извршења, без обзира да ли је оштећени (жртва) власник или само корисник рачунарске мреже.

Извршилац дела рачунарске преваре може да буде свако лице, а у погледу кривице је потребан директни умишљај који квалификује наведена намера.

За основно дело је алтернатисно прописана новчана казна или казна затвора до три године.

Лакши, привилеговани облик овог дела (став 4.) постоји када је учинилац предузео радњу извршења – прикривање или лажно приказивање неког, било ког, података у рачунару или рачунарској мрежи на законом предвиђени начин са намером да се другоме нанесе штета, дакле, да се друго физичко или правно лице оштети. Малициозна намера учиниоца да се другоме нанесе имовинска или неимовинска штета у било ком износу или обиму (без обзира да ли неко прибавља имовинску корист или не) представља привилегујућу околност за коју је закон алтернативно прописао новчану казну или казну затвора до шест месеци.

Кривично дело из члана 301. КЗ има два тежа, квалификована облика испољавања, зависно од обима, интензитета и тежине проузроковане последице услед предузете радње извршења (Ђорђевић, 2011:181).

Први тежи облик дела (став 2.), за који је прописана казна затвора у трајању од једне до осам година, постоји ако је услед предузете радње извршења основног дела прибављена имовинска корист (за учиниоца или за друго физичко или правно лице) у износу преко 450.000 динара. Висина прибављене имовинске користи, која се утврђује према тржишним условима у време извршења дела као фактичко питање, представља квалификаторну околност. Ова тежа последица се мора налазити у узрочно-последичној вези са предузетом радњом извршења.

Други тежи облик дела (став 3.) постоји ако је предузетом радњом извршења учинилац за себе или другога прибавио противправну имовинску корист у износу преко 1.500.000 динара. Ово дело такође квалификује висина прибављене имовинске користи за учиниоца или друго лице, односно висина проузроковане имовинске штете за друго лице која наступа услед предузете радње извршења. За ово је дело прописана казна затвора у трајању од две до десет година.

4.3. Рачунарска превара у упоредном кривичном праву

Од држава у региону, које су настале издвајањем из СФР Југославије, Кривични законик Словеније[8], за разлику од осталих закона, не познаје рачунарска кривична дела као самосталне инкриминације, па ни дело рачунарске преваре.

Казнени закон Хрватске[9] у глави двадесетпетој: „Кривична дела против рачунарских система, програма и података" у члану 271.предвиђа кривично дело: „Рачунарска превара". Дело се састоји у уносу, измени, брисању, оштећењу, чињењу неупотребљивим или недоступним рачунарских података или у ометању рада рачунарског система чиме се проузрокује штета другоме са циљем да се себи или другоме прибави протуправна имовинска корист (Turković et al., 2013:345-346).

Објект заштите је безбедност рачунарских система.

Објект напада је двојако одређен као: а) рачунарски податак. То је у смислу члана 87.тачка 18. КЗ свако исказивање чињеница, информација или замисли у облику прикладном за обраду у рачунарском систему и б) рачунарски систем. Према члану 87.тачка 17. КЗ рачунарски систем је свака направа или скупина међусобно спојених или повезаних направа, од којих једна или више њих на основи програма аутоматски обрађују податке, као и рачунарски подаци који су у њега спремљени, обрађени, учитани или пренесени за сврхе његовог рада, коришћења, заштите и одржавања.

Радњу извршења овог кривичног дела чине следеће алтернативно предвиђене делатности. То су: а) унос, б) измена, в) брисање, г) оштећење, д) чињење неупотребљивим и ђ) чињење недоступним, под условом да се ове радње предузимају у односу на рачунарски податак. Но, радња извршења се може јавити и као ометање (отежавање у већој или мањој мери, краће или дуже време) рада рачунарског система.

[8] Uradni list RS, 55/08, 66/08, 39/09, 91/11, 55/14, 6/16, 38/16, 27/17, 23/20, 91/20 i 95/21.

[9] Narodne novine RH, 125/11, 144/12, 56/15, 61/15, 101/17, 118/18 i 126/19.

За постојање овог кривичног дела је потребно да је радња извршења предузета: а) са одређеним циљем, без обзира да ли је тај циљ у конкретном случају остварен. То је циљ да се учиниоцу или другом (физичком или правном) лицу прибави противправна имовинска корист и б) тако да проузрокује последицу повреде у виду штете (најчешће имовинске) другом физичком или правном лицу.

Извршилац дела може бити свако лице, а у погледу кривице потребан је директан умишљај који карактерише намера (циљ) учиниоца.

За основно дело је прописана казна затвора у трајању од шест месеци до пет година. Уз казну се обавезно изриче мера безбедности одузимања предмета, при чему се рачунарски подаци који су настали извршењем дела обавезно уништавају.

Тежи облик дела (став 2.) постоји ако је предузетом радњом извршења основног дела прибављена (за учиниоца или друго лице) знатна имовинска корист или је другоме проузрокована знатна штета. Када постоји „знатна" имовинска корист или „знатна" штета, представља фактичко питање које суд решава, као фактичко питање, према тржишним условима у време извршења дела, у сваком конкретном случају. За ово дело је прописана казна затвора у трајању од једне до осам година.

Кривични законик Црне Горе[10] у глави двадесетосмој: „Кривична дела против безбедности рачунарских података" у члану 352. предвиђа кривично дело: „Рачунарска превара". Дело се састоји у уношењу, измени, брисању, пропуштању уношења тачног податка или у прикривању или лажном приказивању на други начин рачунарског податка или у извршењу било каквог ометања рада рачунарског система чиме се утиче на резултат електронске обраде, преноса података и функционисање рачунарског система у намери да се себи или другом прибави противправна имовинска корист и тиме другом проузрокује имовинска штета.

Објект заштите је безбедност рачунарских података и функционисање рачунарског система. Рачунарским системом се у смислу члана 142.тачка 19. КЗ сматра сваки уређај или група међусобно повезаних или условљених уређаја, од којих један или више њих, у зависности од програма, врши аутоматску обраду података.

Објект напада је рачунарски податак. Рачунарским податком се према члану 142.тачка 20. КЗ сматра свако излагање чињеница, података или концепата у облику који је погодан за обраду у рачунарском систему, укључујући ту и програме помоћу којих рачунарски систем врши своје функције.

[10] Službeni list CG, 70/03, 13/04, 47/06, 40/08, 25/10, 32/11, 64/11, 40/13, 56/13, 42/15, 58/15, 44/17, 49/18 i 3/20.

Радњу извршења чини више алтернативно прописаних делатности. То су: а) уношење, б) измена, в) брисање, г) пропуштање уношења тачног податка, д) прикривање (прећуткивање) и ђ) лажно (неистинито) приказивање на други начин. Ове се делатности предузимају у односу на рачунарски податак. Поред тога, као радња извршења се сматра и било какво ометање (отежавање, усложавање) рада рачунарског система.

Циљ је овако предузетих делатности да се утиче на резултат електронске обраде или преноса података и на функционисање рачунарског система. Радња извршења се такође предузима у одређеној намери. То је намера да се себи или другом лицу прибави противправна имовинска корист. Ова намера постоји на страни учиниоца у време извршења дела, она утиче на формирање облика кривице као директан умишљај учиниоца, али она не мора да буде остварена у сваком конкретном случају. Последица дела се јавља као наступање повреде у виду проузроковања, наношења имовинске штете неком другом физичком или правном лицу.

Учинилац дела може бити свако лице, а у погледу кривице потребан је директан умишљај који карактерише намера учиниоца.

За ово дело је прописана казна затвора у трајању од шест месеци до пет година.

Зависно од висине и обима проузроковане последице, односно висине прибављене имовинске користи услед предузете радње извршења учиниоца (а тиме и висине проузроковане имовинске штете неком лицу), разликују се два тежа облика испољавања. То су: а) први тежи облик дела (став 2.) који постоји ако је основним делом прибављена имовинска корист која прелази износ од 3.000 еура, за што је прописана казна затвора у трајању од две до десет година и б) други тежи облик дела (став 3.) који постоји ако је предузетом радњом извршења прибављена имовинска корист која прелази износ од 30.000 еура. За ово дело је прописана казна затвора у трајању од две до дванаест година.

Лакши облик дела (став 4.), за који је алтернативно прописана новчана казна или казна затвора до две године, постоји ако је основно дело учињено из малициозне намере или како Законик каже: „само у намери да се друго лице оштети”, без обзира да ли је ова штета наступила у конкретном случају.

Кривични законик Северне Македоније[11] у глави двадесеттрећој: „Кривична дела против имовине” у члану 251-6.предвиђа кривично дело: „Ра-

[11] Службен весник на РМ, 37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 87/07, 7/08, 139/08, 114/09, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14,

чунарска превара". Дело чини лице које са намером да прибави за себе или за другога противправну имовинску корист изазива лажан резултат електронске обраде и преноса података уношењем у рачунар или информациони систем лажних података, неуписивањем или изменом истинитих података, брисањем или прикривањем рачунарских података, фалсификовањем електронског потписа или на други начин.

Објект заштите је безбедност система електронске обраде и преноса података.

Објект напада је рачунарски податак (који може бити истинит или неистинит).

Радња извршења је изазивање (проузроковање) лажног (потпуно или делимично неистинитог) резултата електронске обраде и преноса рачунарских података. Ова се радња извршења предузима: а) на одређени начин: 1) уношењем у рачунар или информациони систем лажних података, 2) неуписивањем или изменом истинитих података, 3) брисањем или прикривањем података, 4) фалсификовањем (кривотворењем, преиначењем) електронског потписа или 5) на други начин и б) са одређеном намером - намером да се прибави за себе или за другога противправна имовинска корист, без обзира да ли је она заиста остварена.

Извршилац дела може бити свако лице физичко или правно лице, а у погледу кривице потребан је такође директан умишљај у чијој се основи налази наведена намера учиниоца.

За ово дело је прописана казна затвора до три године. Према изричитој законској одредби (став 7.) покушај овог дела је кажњив. Ако се правно лице нађе као учинилац овог дела (став 8.), тада је прописана новчана казна. Уз казну се учиниоцу дела обавезно изриче мера безбедности одузимања предмета (став 9.) – посебних уређаја, алата, рачунарских програма или података којима је дело извршено.

Поред основног облика, дело има два тежа облика испољавања зависно од обима и интензитета последице. Први тежи облик дела (став 2.) постоји ако је извршењем радње учинилац стекао већу имовинску корист. За ово дело је прописана казна затвора у трајању од три месеца до пет година. Други тежи облик дела (став 3.) постоји ако је на овај начин учинилац стекао значајну имовинску корист, у ком случају се може казнити затвором у трајању од једне до десет година. Када постоји „већа", а када „значајна" имовинска корист представља фактичко питање које суд решава у сваком конкретном случају на бази тржишних услова.

28/14, 41/14, 115/14, 132/14, 160/14, 199/14, 196/15, 226/15, 169/16, 97/17, 170/17 i 248/18.

Поред тога, рачунарска превара се јавља и у два лакша облика испољавања. Први лакши облик дела (став 4.) постоји ако је радња извршења предузета само са намером да се другоме нанесе штета, без обзира да ли је до ње дошло. За ово дело је прописана новчана казна или казна затвора до једне године. Ако је пак услед овако предузете радње извршења у малициозној намери учиниоца проузрокована већа штета (став 5.), тада је прописана казна затвора у трајању од три месеца до три године.

Други лакши облик дела (став 6.) инкриминише припремне радње за извршење рачунарске преваре. Према законском решењу ово дело се састоји у неовлашћеној (противправној) производњи, набављању, продаји, држању или чињењу доступним другом лицу посебног уређаја, рачунарског програма или података који су намењени за извршење рачунарске преваре. За ово дело је прописана новчана казна или казна затвора до једне године.

У Босни и Херцеговини су у примени три кривична закона који познају рачунарска кривична дела уопште као самосталне инкриминације, па тако и рачунарску превару.

Кривични закон Федерације Босне и Херцеговине[12] у глави тридесетдругој: „Кривична дела против система електронске обраде података" у члану 395. предвиђа кривично дело: „Рачунарска превара". Дело се састоји у неовлашћеном уносу, оштећењу, измени или прикривању рачунарског податка или програма или утицању на исход електронске обраде података на други начин са циљем да се себи или другоме прибави противправна имовинска корист и тиме се другом лицу проузрокује имовинска штета.

Објект заштите је законито, ефикасно, квалитетно, уредно и благовремено функционисање система електронске обраде рачунарских података.

Објект напада је двојако одређен као: а) рачунарски податак или програм и б) електронски систем обраде података.

Радњу извршења чине следеће алтернативно предвиђене делатности. Оне се зависно од објекта напада јављају као (Petrović, Jovašević, Ferhatović, 2016: 434): 1) радње управљене на рачунарски податак или програм. Овде спадају: а) унос (уписивање), б) оштећење, в) измена и г) прикривање рачунарског податка или програма и 2) радње управљене на електронску обраду података - утицање (чињењем или нечињењем) на исход електронске обраде података на други начин.

[12] Službene novine Federacije BiH, 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14 i 75/17.

За постојање дела је потребно да се радња извршења у било ком виду испољавања предузима: а) са одређеним циљем – са циљем да се себи или другоме прибави противправна имовинска корист, б) са проузрокованом последицом у виду имовинске штете у било ком износу која наступа за било које физичко или правно лице и в) на одређени начин – неовлашћено, дакле, противправно.

Извршилац дела може бити свако лице, а у погледу кривице потребан је директан умишљај захваљујући постојању законом прописане намере на страни учиниоца у време извршења дела.

За основно дело је прописана казна затвора у трајању од шест месеци до пет година.

Дело има два тежа облика испољавања. Први тежи облик дела (став 2.) постоји ако је радњом извршења основног дела учинилац за себе или за другога прибавио имовинску корист која прелази 10.000 КМ. За ово дело је прописана казна затвора у трајању од две до десет година. Најтежи облик дела (став 3.), за који је прописана казна затвора у трајању од две до дванаест година, постоји ако је извршењем дела прибављена имовинска корист која прелази 50.000 КМ. Дакле, у оба тежа случаја квалификаторну околност представља висина проузроковане имовинске штете, јер то, заправо, представља, с друге стране, прибављену имовинску корист за учиниоца или за неко друго физичко или правно лице.

Лакши облик дела (став 4.) постоји ако је дело учињено само са циљем да се друго лице оштети, без обзира да ли је таква штета уопште наступила. За ово дело је алтернативно прописана новчана казна или казна затвора до три године.

На идентичан начин и Кривични закон Брчко дистрикта Босне и Херцеговине[13] у глави тридесетдругој: „Кривична дела против система електроничке обраде података" у члану 389.предвиђа кривично дело: „Рачунарска превара" у основном, два тежа и једном лакшем облику испољавања у идентичном законском опису и са истим прописаним казнама.

На другачији начин Кривични законик Републике Српске[14] у глави тридесетдругој: „Кривична дела против безбедности компјутерских података" у члану 410. предвиђа кривично дело: „Компјутерска превара". Ово се дело састоји у уносу нетачног податка, пропуштању уношења тачног податка или прикривању или лажном приказивању податка на други начин чиме се утиче на резултат електронске обраде и преноса података у намери

[13] Službeni glasnik Brčko Distrikta BiH, 19/20.

[14] Службени гласник РС, 64/17, 104/18 i 15/21.

да се себи или другоме прибави противправна имовинска корист и тиме другом проузрокује имовинска штета.

Ово дело карактеришу следећи конститутивни елементи бића: а) објект заштите – систем електронске обраде и преноса података, б) објект напада је рачунарски (компјутерски) податак, који може бити истинит (тачан) или неистинит (нетачан), в) радњу извршења чине следеће делатности. То су: 1) унос, уписивање нетачног (потпуно или делимично неистинитог) податка, 2) пропуштање уписивања (нечињење, неуписивање) тачног (истинитог) податка, 3) прикривање (склањање, чињење недоступним) податка и 4) лажно (неистинито) приказивање, саопштавање података на други начин, г) радња извршења се предузима у односу на податак који је подобан (по природи, садржини, значају, времену) да се утиче на резултат електронске обраде и преноса података, д) радња извршења се предузима са одређеном намером - у намери учиниоца да себи или другом (физичком или правном) лицу прибави противправну имовинску корист, без обзира да ли је ова намера остварена у конкретном случају и ђ) последица дела која наступа услед предузете радње извршења се јавља у виду проузроковања другом (физичком или правном) лицу имовинске штете.

Извршилац дела може бити свако лице, а у погледу кривице потребан је директан умишљај који карактерише наведена намера учиниоца.

За основно дело је прописана (блажа казна него у КЗ Федерације БИХ или КЗ Брчко дистрикта БИХ) и то алтернативно новчана казна или казна затвора до три године.

И овај Законик познаје два тежа облика испољавања овог кривичног дела, али су квалификаторне околности – висина проузроковане имовинске штете – одређене на другачији начин него у КЗ Федерације БИХ и КЗ Брчко дистрикта БИХ. Први тежи облик дела карактерише прибављена имовинска корист која прелази износ од 10.000 КМ услед предузете радње извршења. За ово дело је прописана казна затвора у трајању од једне до осам година. Други тежи облик дела, за који је прописана казна затвора у трајању од две до десет година, постоји ако је извршењем дела прибављена имовинска корист која прелази износ од 30.000 КМ.

Коначно, лакши, привилеговани облик дела (став 4.) постоји ако је било која од наведених радњи извршења основног дела предузета само (једино, искључиво) у намери да се друго лице оштети. За ово дело је алтернативно прописана новчана казна или казна затвора до шест месеци.

5. Закључак

Рачунарски криминалитет, било класични, било организовани полако, али сигурно заузима своје место у обиму, динамици и структури савременог криминалитета уопште, а посебно као облик имовинског криминалитета. Уочавајући опасности од злоупотребе рачунара и савремене технологије која је повезана са рачунарским системима међународна заједница је реаговала доношењем одређених међународних докумената – посебно Конвенције Савета Европе о високотехнолошком криминалу из 2001. године. На њеним основима су европска кривична законодавства успоставила систем кривичне одговорности и кажњавања за рачунарска кривична дела. Следећи ове тенденције Србија 2003.године први пут у свој правни систем уноси рачунарска кривична дела. Сличне тенденције показују и друга законодавства у региону.

Међу рачунарским кривичним делима се издваја рачунарска превара као посебан облик имовинског кривичног дела преваре која се у овом случају врши на специфичан начин – уз помоћ и употребу рачунарских програма или података са циљем да се омете процес електронске обраде података. У свим овим случајевима превару као кривично дело квалификује директан умишљај учиниоца који се заснива на намери учиниоца да за себе или другога прибави имовинску (или другу материјалну, најчешће противправну) корист или његовој намери да другоме нанесе штету.

Зависно од висине прибављене користи, односно проузроковане имовинске штете другоме, јављају се и тежи квалификовани облици дела за која је прописано пооштрено кажњавање. Уз казну затвора, прописане су најчешће новчане казне, као и обавезно изрицање мере безбедности одузимања предмета (рачунарских уређаја, програма или података) којима је ово дело извршено или која су намењена за његово извршење. Поред тога, поједина регионална законодавства (Северна Македонија) изричито прописују кажњивост за припремање извршења кривичног дела рачунарске преваре.

Литература

Ђорђевић, Ђ., (2011). *Кривично право. Посебни део.* Београд: Криминалистичко-полицијски универзитет.

Ђорђевић, Ђ., Коларић, Д. (2020). *Кривично право. Посебни део.* Београд: Криминалистичко-полицијски универзитет.

Ђорђевић, М., Ђорђевић, Ђ. (2021). *Кривично право.* Београд: Пројурис.

Јовашевић, Д. (2017). *Кривично право. Посебни део.* Београд: Досије.

Мрвић Петровић, Н. (2005). *Кривично право* .Београд: Службени гласник.

Narodne novine RH, 125/11, 144/12, 56/15, 61/15, 101/17, 118/18 i 126/19.

Pavišić, B. (2006). *Kazneno pravo Vijeća Evrope*. Zagreb: Tehnička knjiga.

Pavišić, B., Grozdanić, V., Veić, P. (2007). *Komentar Kaznenog zakona*. Zagreb: Narodne novine.

Petrović, B., Jovašević, D., Ferhatović, A. (2016). *Krivično pravo 2*. Sarajevo: Pravni fakultet.

Службен весник на РМ, 37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 87/07, 7/08, 139/08, 114/09, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 41/14, 115/14, 132/14, 160/14, 199/14, 196/15, 226/15, 169/16, 97/17, 170/17 і 248/18.

Службен весник на РМ, 19/04.

Službene novine Federacije BiH, 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14 i 75/17.

Službeni glasnik Brčko Distrikta BiH, 19/20.

Службени гласник РС, 39/03.

Службени гласник РС, 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 и 35/19.

Службени гласник РС, 61/05.

Службени гласник РС, 19/09.

Службени гласник РС, 64/17, 104/18 і 15/21.

Službeni list CG, 70/03, 13/04, 47/06, 40/08, 25/10, 32/11, 64/11, 40/13, 56/13, 42/15, 58/15, 44/17, 49/18 і 3/20.

Стојановић, З., Делић, Н. (2013). *Кривично право*. *Посебни део.* Београд: Правни факултет.

Turković, K., et al. (2013). *Komentar Kaznenog zakona.* Zagreb: Narodne novine.

Uradni list RS, 55/08, 66/08, 39/09, 91/11, 55/14, 6/16, 38/16, 27/17, 23/20, 91/20 і 95/21.

Шкулић, М. (2020). *Међународно кривично право*. Београд: Правни факултет.

Dragan Jovašević L.L.D.,
Full professor,
Faculty of Law University of Niš,
Serbia

COMPUTER FRAUD

(criminal responsibility and criminality in international and national law)

Summary

On the basis of adopted international documents of universal and regional character, the largest number of countries, including the Republic of Serbia, in their national legislation know more computer (computer) crimes that protect various digital databases. The perpetrators of these specific criminal offenses are prescribed criminal liability and punishability of natural and legal persons. In addition to specific computer crimes, in modern conditions, many old classic crimes (theft, fraud, forgery) gain a new dimension with a greater degree of severity and danger when committed using computers or computer systems. Since this is a crime where there is usually no temporal and spatial connection between the perpetrator and his act of execution and the caused consequences, ie the injured person, modern legislation also knows special evidentiary actions in the procedure of detecting and proving these crimes. This paper talks about the concept and characteristics of computer fraud as a form of computer crime in international and national criminal law.

Keywords: *computer crime, fraud, law, crime, liability, criminal sanction.*

Dr Enis Omerović,
Docent,
Prince Sultan University, College of Law,
Riyadh, Saudi Arabia
Damir Imamović, MA iur.,
Državni službenik u Zeničko-dobojskom kantonu,
Zenica, Bosna i Hercegovina

UDK: 343.533::004

ALTERNATIVNI PRISTUPI I PRIJEDLOZI ZA RJEŠAVANJE JURISDIKCIJSKIH SUKOBA UZROKOVANIH SAJBER KRIMINALOM

Apstrakt*: Cilj rada bio je pronaći i predstaviti adekvatan pristup za rješavanje jurisdikcijskih sukoba uzrokovanih sajber kriminalom. Teritorijalna karakteristika sajber kriminala manifestira se u odsustvu postojanja granica unutar sajber prostora, odnosno činjenici da je sajber krivično djelo počinjeno unutar nadležnosti različitih država, tako da ne postoji jedinstveni pravni okvir za uređenje svih sajber krivičnih djela. Proces digitalizacije, odnosno stalno i dinamičko kretanje podataka preko različitih servera ili računarskih oblaka smještenih u više jurisdikcija, ukazuje na određena pravna ograničenja u primjeni načela teritorijalnosti u sajber prostoru. Zbog te nefunkcionalne karakteristike teritorijalne jurisdikcije, u radu se nastoji ukazati na važnost utvrđivanja osnova jurisdikcije u procesuiranju sajber krivičnih djela kroz predstavljanje različitih paradigmi ili pristupa, kao dopune teritorijalnog načela u rješavanju jurisdikcijskih sukoba. Naime, prikazan je značaj ulaganja pravnih napora u eventualnom približavanju i rješavanju jurisdikcijskog sukoba u smislu primjene najadekvatnijeg načela nadležnosti od domaćih sudova u svakom konkretnom slučaju. Ta rješavanja bi vjerovatno išla u smjeru usklađivanja i preinaka međunarodnih akata, kao i u smjeru harmonizacije državnih propisa koja uređuju sankcioniranje određenih sajber krivičnih djela. Također, postojanje međunarodnog krivičnog suda ili tribunala s nadležnošću za slučajeve sajber terorizma, i drugih ozbiljnih sajber krivičnih djela, uz primjenu novih jurisdikcijskih teorija, omogućili bi rješavanje problema i otklanjanje poteškoća u pogledu zasnivanja nadležnosti za sajber krivična djela.*

Ključne riječi: *jurisdikcija, sajber kriminal, teritorijalna nadležnost, harmonizacija, univerzalna jurisdikcija.*

The issue of crime committed on the internet ('cybercrime') is not a straightforward one in as much as, since the internet is a network which is by definition universal, the location of such crime, be it the causal event or the loss sustained, is particularly difficult to determine.

(Advocate General at the Court of Justice of the European Union, Melchior Wathele)

1. Uvodne postavke

Širenje globalne informacijske infrastrukture rezultiralo je pojavom velikih mogućnosti za počinjenjem raznih vrsta krivičnih djela sajber kriminala. Činjenica je da živimo u digitalnom dobu i da je digitalna tehnologija prodrla u sva područja društvenog života. Raspon krivičnih djela koji se podržava tehnologijom konstantno se širi, i kao funkcija tehnoloških promjena i u smislu društvene interakcije s novim tehnologijama. (Urbas, Choo, 2008: 5). Sajber kriminal počev od međunarodnog hakiranja, industrijske špijunaže do sajber terorizma postaje sve prisutnija prijetnja sigurnosti na globalnom nivou.

Transnacionalni kriminal je pojam koji se u Ujedinjenim nacijama upotrebljava još od 1974., a 1994. na nivou te međunarodne organizacije prihvaćen je i pojam transnacionalnog kriminala kao pojave krivičnih djela koja se u izvršenju ili sprječavanju, odnosno ublažavanju posljedica, direktno ili indirektno, reflektiraju na više od jedne zemlje. (Degan, Pavišić, Beširević, 2011: 99). Savremeni transnacionalni organizirani kriminal koristi se prednostima globalizacije, slobodne trgovine i naglog razvoja novih tehnologija za izvršenje različitih krivičnih djela. (Šačić, 2004: 124). Shodno tome, sajber krivična djela danas predstavljaju značajno područje savremenog transnacionalnog kriminala.

Počinitelji sajber krivičnih djela koriste odsustvo postojanja granica u visokotehnološkom svijetu, a samim tim i nedostatke u vidu prekograničnih ograničenja. Koriste jurisdikcijsku nemogućnost državnih organa za provođenje zakona kao nedostatak i vid prepreke da djeluju izvan svoje jurisdikcije, odnosno preko državnih granica. U sajber svijetu nema tačno određenih teritorija ili granica zbog česte međunarodne dimenzije. Sve to ukazuje da je sajber kriminal tipičan transnacionalni kriminal koji predstavlja izazov u pogledu primjene krivičnog prava za transnacionalna sajber krivična djela s obzirom na stepen zahtjevnosti po pitanju određivanja jurisdikcije.

Tako će se država koja želi procesuirati sajber krivična djela počinjena od strane osoba koje se nalaze na teritoriji druge države vjerovatno naći u određenim poteškoćama. Stoga se mnoga pitanja i dileme javljaju u pogledu jurisdikcije za kompjuterska krivična djela. Nadasve, tu je i pitanje šta ako se šteta prouzročena samim činom počinitelja odrazi i na druge države, koja će država u tom slučaju biti nadležna za podizanje optužnice protiv počinitelja sajber krivičnog djela? Šta ako počinjeno djelo nije označeno kao krivično djelo u državi radnje, ali se smatra krivičnim djelom u zemlji gdje se posljedice štete manifestiraju? Šta bi trebalo biti osnova za traženje nadležnosti zbog sajber krivičnog djela, da li to treba biti državljanstvo osobe koja je počinila djelo ili država njegovog boravišta, ili, pak, teritorij na kojem je krivično djelo počinjeno?

Također, dodatnu otežavajuću okolnost pri utvrđivanju jurisdikcije za sajber krivična djela predstavlja i „*računarstvo u oblaku*" (*cloud computing*), i to zbog svoje distribuirane specifičnosti. Ono podrazumijeva da se podaci - a time i elektronski dokazi – manje čuvaju na određenom uređaju ili u zatvorenim mrežama, ali se zato distribuiraju preko različitih usluga-servisa, pružatelja usluga, lokacija i, često, različitih jurisdikcija. (Kleijssen, Perri, 2017: 155). Koliko se čvrsto pojam regulatorne moći, teritorijalnosti i državnosti isprepliću kroz koncept jurisdikcije najbolje se oslikava kroz riječi Manna: „Međunarodna nadležnost je aspekt ili sastojak ili posljedica suvereniteta (ili teritorijalnosti ili načela neintervencije - razlika je samo terminološka)". (Mann, 1984: 20).

Rasprave po pitanju jurisdikcije za sajber kriminal trenutno pokazuju da postoje velika ograničenja u pogledu primjene načela teritorijalnosti u virtualnom sajber prostoru, zbog stalnog i dinamičkog kretanja podataka preko različitih poslužitelja-servera smještenih u više jurisdikcija, zbog čega se dovodi u pitanje teritorijalna dogma u digitalnom dobu.

U dolasku do određenih naučnih spoznaja, u radu se koristimo pravnodogmatskom metodom, odnosno metodama analize i sinteze, ali i elementima induktivne i deduktivne metode. Rad je postavljen na način da nam predočava i teoretski i praktični presjek stanja u jednoj oblasti s kritičkim osvrtom na temeljni predmet istraživanja, postojeće međunarodnopravno uređenje i analizu prakse država i odgovarajućih međunarodnih institucija, a sve s ciljem propitivanja adekvatnosti i učinkovitosti sadašnjega učenja o jurisdikcijskim načelima za sajber krivična djela, te o potrebi svojevrsnih alternativnih pristupa i prijedloga kako bi se na cjelovit način tretirala ova oblast u praksi.

2. Međunarodna i transnacionalna[1] arbitraža

Sajber kriminal je složen globalni problem jer u elektronski povezanom svijetu efekti svake date radnje mogu se odmah odraziti negdje drugo, a da nisu geografski povezani. (Berman, 2012: 5).

Međunarodno pravo nudi potencijalno korisne smjernice za rješavanje pravnog problema jurisdikcije za pojedina sajber krivična djela, gdje se neki međunarodni ugovori o ljudskim pravima mogu odnositi na elemente sajber kriminala. Naprimjer, pravo na privatnost, priznato u međunarodnim dokumentima o zaštiti ljudskih prava, poput Univerzalne deklaracije o ljudskim pravima[2] ili Međunarodnog pakta o građanskim i političkim pravima[3], koji se mogu primijeniti i na sajber kriminal, kako bi se spriječio nezakonit pristup privatnim podacima drugih ljudi, dok pravo na slobodu izražavanja i slobodu informiranja u tim dokumentima argumentirano zabranjuje ometanje pristupa web stranicama medija.

Prijedlozi za rješavanje jurisdikcijskih sukoba uzrokovanih sajber kriminalom kao harmonizacija državnih zakona shodno međunarodnim standardima i eventualna primjena univerzalnog načela uz mogućnost međunarodne i transnacionalne arbitraže mogu biti jedan od funkcionalnih načina rješavanja problema nadležnosti za krivično gonjenje počinitelja sajber krivičnih djela. Naime, dugo postoji potreba za pronalaženjem adekvatnog odgovora na sajber kriminal, ali malo je bilo slaganja oko toga koji je pravni okvir najprikladniji za rješavanje jurisdikcijskih sukoba uzrokovanih sajber krivičnim djelima. Trenutna nemogućnost pronalaženja odgovarajućeg pravnog okvira upućuje na to da ne postoji pravni okvir koji bi u potpunosti mogao pravilno regulirati sva transnacionalna sajber krivična djela, a samim tim i pravno pitanje jurisdikcije.

---

[1] „Arbitraža je moguća i između bilo koja dva subjekta, npr. između dviju pravnih osoba iz različitih država ili između neke države i inozemne pravne osobe (npr. banke ili petrolejske kompanije). U ovomu potonjem slučaju nije riječ o međunarodnoj nego o tzv. transnacionalnoj arbitraži." (Degan, 2011: 717). Transnacionalna arbitraža slična je domaćim parnicama, ali umjesto da se održi pred domaćim sudom, to se odvija pred sudijama poznatim kao arbitri na međunarodnoj razini. To je ona arbitraža koja za predmet ima sporove iz međunarodnih poslovnih odnosa, a naročito ako: 1) stranke u vrijeme zaključenja sporazuma o arbitraži imaju poslovna sjedišta u različitim državama; 2) se izvan države u kojoj stranke imaju svoja poslovna sjedišta nalazi mjesto: a) arbitraže, ako je određeno u sporazumu o arbitraži ili na osnovu njega, ili b) u kome treba da se izvrši bitan dio obaveza iz poslovnog odnosa ili mjesto s kojim je predmet spora najuže povezan; 3) su se stranke izričito sporazumjele da je predmet sporazuma o arbitraži vezan za više država.

[2] Univerzalna deklaracija o ljudskim pravima, član 12., usvojena Rezolucijom Generalne skupštine Ujedinjenih nacija 10. decembra 1948.

[3] Međunarodni pakt o građanskim i političkim pravima, član 17., usvojen Rezolucijom 2200A (XXI) Generalne skupštine 16. decembra 1966. Stupio na snagu 23. marta 1976., u saglasnosti s članom 49.

Međutim, oslanjajući se na postojeće modele međunarodnog rješavanja sporova, jedno od mogućih rješenja problema reguliranja transnacionalnih sajber krivičnih djela je i putem međunarodne arbitraže. (Đorđević, 2020). Stoga i između država u ovome pogledu može doći do nastanka međunarodnoga spora. Takvo što bi se zbilo u situaciji da jedna država ne želi procesuirati počinitelje transnacionalnoga sajber krivičnoga djela, koja zasniva svoju nadležnost temeljem subjektivnog teritorijalnog načela (u kojoj državi je radnja djela započeta), a ne želi ga ni izručiti drugoj državi, koja zasniva svoju nadležnost temeljem objektivnog teritorijalnog načela (u kojoj državi je radnja dovršena ili je u njoj ostvarena protupravna posljedica). Zapravo, ovdje bi se radilo o povredi načela *aut dedere aut judicare* (obaveza procesuiranja počinitelja ili njihova izručenja). Dakle, ovakav bi se međunarodni spor mogao rješavati putem međunarodne arbitraže ili izabranoga sudovanja, koja za cilj ima rješavanje sporova između država od strane arbitara po vlastitome izboru. Države se tako prilikom odabira arbitraže, umjesto sudskoga postupka, odlučuju za tzv. privatni postupak rješavanja međunarodnoga spora.

Jednako tako, mogao bi se zamisliti određeni specijalizirani arbitražni sud (tribunal) za rješavanje sajber sporova, koji bi mogao biti vezan ili bi se svojim duhom mogao naslanjati na Konvenciju Ujedinjenih nacija o priznavanju i izvršavanju stranih arbitražnih presuda iz 1958., tzv. New York (Njujoršku) konvenciju. Međunarodna unija za telekomunikacije (ITU)[4] kao specijalizirana agencija Ujedinjenih nacija za informacijske i komunikacijske tehnologije (ICT), predstavlja jedno od mogućih rješenja unutar kojega bi arbitražno tijelo za transnacionalna sajber kriviča djela moglo funkcionirati. (Perloff-Giles, 2018: 213). ITU, u tome smislu, može predložiti potencijalne arbitre s relevantnom stručnošću ili izravno imenovati članove arbitražnoga tribunala, od iskusnih generalnih stručnjaka za rješavanje sporova do visoko specijaliziranih praktičara i stručnjaka koji pokrivaju cijeli pravni i tehnički spektar kada je u pitanju digitalna odnosno informacijska i komunikacijska tehnologija.

Također, transnacionalna arbitraža se može koristiti i za pozivanje privatnih aktera u sporu na odgovornost, s obzirom da se danas komercijalna arbitraža rukovodi, između ostaloga, na osnovu Njujorške konvencije.[5] To se najbolje oslikava u drugom i trećem članu odnosnog međunarodnog ugovora. Član 2. stav 1.

[4] ITU je osnovana 1865. radi razvijanja tehničkih standarda koji će omogučiti olakšavanje međunarodne povezanosti u komunikacijskim mrežama, kao i poboljšati pristup informacijskim i komunikacijskim tehnologijama slabo razvijenim državama širom svijeta. [Electronic version]. Retrieved 9 June 2021, from https://www.itu.int/en/about/Pages/default.aspx.

[5] Konvencija o priznanju i izvršenju inostranih arbitražnih odluka. [Electronic version]. Retrieved 10 June 2021, from https://www.newyorkconvention.org/11165/web/files/original/1/5/15467.pdf.

tako propisuje da „Svaka država ugovornica priznaje pismeni ugovor kojim se stranke obavezuju da stave u nadležnost arbitraži sve sporove ili neke od sporova koji nastanu ili bi mogli nastati između njih po određenom pravnom odnosu, ugovornom ili neugovornom, koji se odnosi na pitanje koje je podobno za rješavanje arbitražnim putem".[6] Član 3. nadalje predviđa da će „Svaka strana ugovornica priznati važnost arbitražne odluke i odobriće izvršenje te odluke shodno pravilima postupka koji važe na teritoriji na kojoj se poziva na odluku, pod uslovima utvrđenim u sljedećim članovima. Za priznanje i izvršenje arbitražnih odluka na koje se primjenjuje ova konvencija ne mogu se nametnuti osjetno stroži uslovi niti znatno veći sudski troškovi od onih koji se zahtijevaju za priznanje ili izvršenje domaćih arbitražnih odluka".[7]

Otuda bi se široko usvojeni sistem Njujorške konvencije u smislu građanske odgovornosti za transnacionalne protupravnosti mogao bi se iskoristiti i za promicanje odgovornosti za transnacionalna sajber krivična djela. (Perloff-Giles, 2017: 43). Softverske kompanije i pružatelji internetskih usluga mogli bi zahtijevati, u sklopu svojih uslova pružanja usluge, da sporovi u vezi sa sajber napadima budu predmet arbitraže. (Perloff-Giles, 2018: 212). To se može zamisliti na način da bi sajber imovina napadača mogla biti zaplijenjena gdje god se nalazila, dosezajući prag kompenzacije u vidu obeštećenja, odnosno novčane kompenzacije, čime bi se jednostavno finansijski pokušalo kazniti počinitelje sajber kriminala. No, da li arbitraža u svojoj srži ima za cilj krivičnu osudu?

Naravno, ono što transnacionalnu i međunarodnu arbitražu čini privlačnima za njihove sudionike čini ih primamljivima i za sajber kriminalce, budući da i transnacionalna i međunarodna arbitraža obično uključuju više sudionika u različitim jurisdikcijama, poput stranaka, advokata, arbitražnih institucija, arbitara i stručnjaka. (Cohen, Morril, 2019). Sudionici su digitalno međusobno ovisni, jer proces obično uključuje skupljanje i prijenos velikih skupova podataka, gdje svako može biti „slaba karika" u zaštiti sigurnosti podijeljenih informacija, odnosno osjetljivih komercijalnih i osobnih podataka. (Cohen, Morril, 2019). Zbog toga, jedan od izazova o kojem se raspravlja na međunarodnom nivou je i jačanje sajber sigurnosti u transnacionalnoj i međunarodnoj arbitraži. Prevladavanjem toga i drugih izazova pri uspostavljanju ova dva oblika arbitraže takvo što bi moglo pružiti kvalitetnu polaznu osnovu u eventualnom rješavanju problema zasnivanja jurisdikcije za sajber krivična djela.

[6] Član 2. Konvencije o priznanju i izvršenju inostranih arbitražnih odluka.

[7] Član 3. Konvencije.

3. Univerzalna jurisdikcija

Načelo univerzalne jurisdikcije dopušta državi da obavlja svoju krivičnonopravnu jurisdikciju, a time i da primjenjuje s njom tradicionalno povezano svoje materijalno krivično pravo na činjenično stanje koje se nije dogodilo na njenom teritoriju, i koje ne dotiče njene neposredne državne interese te u kojem ne sudjeluju njeni državljani, ni kao žrtve ni kao počinitelji. (Munivrana, 2006: 194). Ukratko, prema načelu univerzalnosti država prisvaja nadležnost da sudi nekoj osobi koja se našla na njenoj državnoj teritoriji, bez obzira na njeno državljanstvo, i to za djela koja je učinila bilo gdje u inostranstvu, pa čak ako žrtva zločina nije njen državljanin. (Degan, Pavišić, Beširević, 2011: 114). Temeljna ideja je potreba da se osigura da nijedno krivično djelo ne prođe nekažnjeno, odnosno da se države zajednički bore protiv nekažnjivosti (*impunity*), protiv izvršenja najtežih međunarodnih zločina, a sve kako bi se zaštitili interesi cijele međunarodne zajednice. Međutim, načelo univerzalnosti se ne odnosi na kažnjavanje običnih krivičnih djela, nego samo međunarodnih zločina prema općem međunarodnom pravu ili onih iz osnovnih međunarodnih konvencija. S obzirom na tu činjenicu, univerzalna nadležnost, primjenjiva na krivična djela piratstva, nudi jedno rješenje problema zasnivanja teritorijalne nadležnosti kada je u pitanju krivična odgovornost. (Kontorovich, 2003: 184). Piratstvo je klasičan primjer međunarodnoga zločina koje je još od 17. stoljeća obuhvaćeno univerzalnom jurisdikcijom u međunarodnom običajnom pravu (Scharf, Newton, Sterio, 2015: 58). Dok se sajber kriminal uspoređuje s tradicionalnim piratstvom (Cesare, 2010: 501) analogija bi se trebala zaustaviti na osnovnoj činjenici samog prekoračenja granica. Shodno tome, i sajber kriminalci, kao i pirati, koji se smatraju *hostis humani generis* ili neprijateljem čovječanstva (Luban, 2018: 122) mogu biti procesuirani gdje god da se nađu, budući da se sajber prostor može smatrati modernim „otvorenim morem", a transnacionalna sajber krivična djela kao ekvivalent piratskim neselektivnim djelima razbojništva. (Rho, 2007: 709).

Kao što piratstvo ugrožava međunarodnu trgovinu, tako bi i teža sajber krivična djela koja na sličan način prijete međunarodnoj trgovini mogla podlijegati univerzalnoj nadležnosti, naprimjer, kada DDoS napadi (Natarajan, 2019: 64) onemoguće pristup glavnim komercijalnim web stranicama, ili kada *ransomware* napadi (Natarajan, 2019: 64) prijete uništavanju evidencije međunarodnih korporacija i datoteka. (Perloff-Giles, 2017: 64). U 2018. mjesečno je prijavljeno više od 400.000 DDoS napada, a ukupni godišnji broj DDoS napada dostići će 14,5 miliona već 2022. (Jugović Spajić, 2019). Već godinama je *ransomware* glavna briga stručnjaka za sajber sigurnost, budući da i dalje sve više kompanija plaća otkupninu usljed napada ove vrste. Tako je evropska brodska kompanija *Maersk* postala žrtvom napada *ransomware*-a u junu 2017., kada se infekcija proširila njihovom globalnom mrežom i tako utjecala na brodsku otpremu kroz 76 luka,

koštajući ih oko 300 miliona dolara. (Zaharia, 2021). Napadi na kompanije sada čine 81% svih napada *ransomware*-a (Jugović Spajić, 2019), dok se očekuje da će *ransomware* koštati 6 triliona dolara godišnje do 2021. (Zaharia, 2021).

Kako smo naveli, države kod ograničenoga broja teških međunarodnih krivičnih djela (genocid, zločini protiv čovječnosti, ratni zločini, zločini protiv mira, mučenje, piratstvo) mogu zasnovati svoju nadležnost temeljem univerzalnoga načela, bez obzira na lokaciju djela, državljanstvo počinitelja ili žrtve, ili bilo kojega drugoga zaštićenog interesa države. (Brenner, Koops, 2004: 28). Nadalje, Kraljevina Nizozemska, naprimjer, prisvaja nadležnost za krivična djela, poput napada na kralja i krivotvorenje[8], dok sajber krivična djela ne spadaju u klauzulu o univerzalnoj nadležnosti. Međutim, neke države su zakonski usvojile univerzalnu nadležnost i za određene kategorije sajber kriminala, poput distribucije slika seksualnoga zlostavljanja djece. Tako Kraljevina Belgija[9] i Savezna Republika Njemačka[10] prisvajaju univerzalnu nadležnost za određeni sajber kriminal, kao što je dječja pornografija, gdje se njeno širenje može procesuirati na osnovu univerzalne jurisdikcije. (Leslie, 2014: 302). Vlada Sjedinjenih Američkih Država, prema članu 404. Zakona o vanjskim odnosima SAD-a iz 1987., oslanja se na pojam univerzalne nadležnosti kada je u pitanju određivanje i propisivanje kazne za određena krivična djela koja je zajednica nacija priznala općim interesom, poput piratstva, uzimanja talaca, trgovine ljudima, napada ili otmice odnosno sabotaže zrakoplova, genocida, mučenja, ratnih zločina, i određenih terorističkih djela, čak i ako ne postoji nijedna osnova nadležnosti navedena u članu 402.[11]

Osnovni argument protiv univerzalne jurisdikcije je tvrdnja da ona predstavlja miješanje u unutrašnje stvari drugih država, čime se narušava suverenitet, što omogućava zloupotrebu tog načela u političke svrhe i tokom međudržavnih sukoba. (Wible, 2002: 265). S obzirom da u različitim državama vladaju različiti pravni sistemi, otuda postoje i različita pravila i okolnosti vođenja istražnih i

[8] Član 4. Nizozemskog krivičnog zakona - *Wetboek van Strafrecht* (Dutch CC). [Electronic version]. Retrieved 23 June 2021, from http://www.wetboek-online.nl/wet/Wetboek%20van%20Strafrecht.html.

[9] Član 10. stav (1) *Wet houdende de voorafgaande titel van het Wetboek van Strafvordering* (Belgijski krivični zakon iz 2012).

[10] Odjeljak 6(6) i 184(b) Strafgesetzbuch (Njemački krivični zakon iz 1998).

[11] Godine 1987. Američki pravni institut objavio je prepravljeni član tri Zakona o vanjskim odnosima. Odjeljci 402-404. obuhvatili su međunarodno običajno pravo koje uređuje nadležnost propisivanja. [Electronic version]. Retrieved 24 June 2021, from http://www.qil-qdi.org/jurisdictional-reasonableness-under-customary-international-law-the-approach-of-the-restatement-fourth-of-us-foreign-relations-law/. Primjer: Sjedinjene Američke Države protiv Yousefa, 327 F.3d 56, 99-100 (2003), u kojem predmetu je okružni sud utvrdio univerzalnu nadležnost nad terorističkim aktivnostima.

dokaznih radnji, ispitivanja ili zaštite svjedoka, kao i pitanja suđenja u odsustvu okrivljenoga (anglosaksonsko i kontinentalno pravo). (Mladenović, 2012: 481).

Međutim, Prinstonska načela o univerzalnoj jurisdikciji (Program in Law and Public Affairs, 2001) približavaju dva suprotstavljena koncepta tako što primjenu univerzalne jurisdikcije načelno uslovljavaju prisutvom optuženog, ali istovremeno dopuštaju izuzetak da se zatraži izručenje osobe optužene ili osuđene za međunarodni zločin, pri čemu država koja traži izručenje mora da dokaže postojanje osnovane sumnje da je tražena osoba počinila krivično djelo, kao i da će suđenje i izvršenje sankcije biti ostvareno u skladu s međunarodno priznatim standardima zaštite ljudskih prava.[12]

Univerzalna nadležnost je vjerovatno potrebna, ne samo u predmetima međunarodnih zločina *stricto sensu*, već i nad transnacionalnim krivičnim djelima s obzirom na njihovu raširenost i veliku štetu koju uzrokuju (Obokata 2010: 208), budući da univerzalna jurisdikcija u velikoj mjeri predstavlja najefikasniji metod za odvraćanje i prevenciju međunarodnih zločina povećanjem vjerovatnoće gonjenja i kažnjavanja počinilaca. (Bassiouni, 2001: 153). Smatra se da bi očekivanje „suštinskoga usklađivanja" transnacionalnih krivičnih djela poput kompjuterskoga odnosno sajber kriminala, moglo rezultirati „organskim rastom univerzalne jurisdikcije". (Cockayne, 2005: 514). Izazov u primjeni univerzalne nadležnosti u sajber kontekstu je definiranje obima prijetnji na koje se univerzalna nadležnost može primijeniti. Obim mora biti dovoljno specificiran kako bi se krivična djela koja podliježu univerzalnoj nadležnosti mogla tačno odrediti, čime bi sud koji je ovlašten da vodi postupke protiv sajber počinitelja mogao izreći kaznu za sajber krivična djela počinjena bilo gdje u svijetu.

4. Osnivanje Međunarodnog krivičnog suda za sajber krivična djela

Mogućnost o kojoj se dugo raspravlja po pitanju progona počinilaca sajber kriminala je proširivanje nadležnosti Međunarodnog krivičnog suda (ICC) koji nema stvarnu nadležnost nad sajber kriminalom ili stvaranje novog međunarodnog krivičnog suda (tribunala) sa specijaliziranom nadležnošću za sajber krivična djela. Rimski statut utvrđuje nadležnost Međunarodnog krivičnog suda, i to nad četiri vrste međunarodnih zločina: genocidom, zločinima protiv čovječnosti, ratnim zločinima i zločinom agresije[13]. Kada se razmatra da li sajber napadi

[12] Načelo 1. tačka 3. Prinstonska načela o univerzalnoj jurisdikciji. [Electronic version]. Retrieved 25 June 2021, from https://lapa.princeton.edu/hosteddocs/unive_jur.pdf.

[13] Član 5. Zakona o potvrđivanju Rimskog statuta Međunarodnoga krivičnog suda. [Electronic version]. Retrieved 28 June 2021, from https://narodne-novine.nn.hr/clanci/medunarodni/2001_04_5_42.html. Rome Statute of the International Criminal Court. Published by the International Criminal Court. (2011). [Electronic version]. Retrieved

mogu predstavljati skupinu zločina protiv mira (agresiju), može se vjerovatno valjano ustvrditi da se većina sajber napada ne podiže na razinu oružanoga napada. Međutim, postoji i „*cyber-warfare*"[14], izraz koji se pravilno koristi samo za označavanje male podskupine sajber napada koji doista predstavljaju oružane napade ili koji se događaju u kontekstu međunarodnoga ili nemeđunarodnoga oružanoga sukoba koji je u toku. (Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue, Spiegel, 2011: 22).

Trenutno, Rimski statut Međunarodnog krivičnog suda nudi koristan model za procesuiranje međunarodnih zločina u užem smislu, odnosno onih djela s velikim međunarodnim razornim učincima, dok još uvijek, po svemu sudeći, ne bi obuhvatio transnacionalna sajber krivična djela, osim ako bi se Rimski statut mogao izmijeniti i proširiti nadležnost Međunarodnog krivičnog suda i na djela sajber kriminala. (Perloff-Giles, 2017: 61).

Samim aktom proširivanja nadležnosti primjenom načela komplementarnosti na procesuiranje sajber krivičnih djela, a kojim se razgraničava jurisdikcija suda od jurisdikcije država (Konforta, Munivrana-Vajda, 2014: 27), kao jednog od najvažnijih načela kojim se uređuje rad Međunarodnog krivičnog suda, moglo bi se doprinijeti rješavanju jurisdikcijskih sukoba (sukoba nadležnosti između više država u pogledu procesuiranja sajber kriminala). Međunarodni krivični sud u tom slučaju djeluje kao jedan vid zaštitne mreže, odnosno ukoliko države ne ispunjavaju svoje obaveze prema međunarodnom pravu primjenom učinkovite krivične nadležnosti za zločine navedene u Rimskom statutu, slučajevi se otuda mogu pokrenuti u Den Haagu pred stalnim Međunarodnim krivičnim sudom. (Bergsmo, 2010: 308). U Republici Turskoj jurisdikcijsko je načelo komplementarnosti provedeno kako bi se izbjegli negativni sukobi nadležnosti nakon usvajanja Evropske konvencije o međunarodnoj važnosti krivičnih presuda[15] od 28. maja 1970., a koja je stupila na snagu 26. jula 1974. Međutim, prema najnovijim turskim državnim izvještajima, u području sajber kriminala pozitivni sukobi nadležnosti predstavljaju više problema nego negativni sukobi. (Klip, 2014). Kraljevina Nizozemska donosi posebne propise za rješavanje sukoba nadležnosti, u kojem području je zakonodavstvo usvojeno kako na nivou Evropske

28 June 2021, from https://www.icc-cpi.int/NR/rdonlyres/ADD16852-AEE9-4757-ABE7-9CDC7CF02886/283503/RomeStatutEng1.pdf.

[14] *Cyberwar* se također naziva *cyberwarfare* ili kibernetski rat, rat koji se vodi u i s kompjutera i mrežâ koje ih povezuju, a vode ga države ili njihovi opunomoćenici protiv drugih država. *Cyberwar* se obično vodi protiv vladinih i vojnih mreža radi ometanja, uništavanja ili uskraćivanja njihove upotrebe. [Electronic version]. Retrieved 01 July 2021, from https://www.britannica.com/topic/cyberwar.

[15] European Convention on the International Validity of Criminal Judgments. [Electronic version]. Retrieved 3 July 2021, from https://rm.coe.int/1680072d3b.

unije, tako i na državnom nivou. Republika Italija se poziva na član 22. stav 5. Konvencije o sajber kriminalu Vijeća Evrope (*Convention on Cybercrime*)[16], koji predviđa mogućnost konsultacije „kada više strana ugovornica zahtijeva zasnivanje nadležnosti u pogledu prekršaja predviđenih ovom Konvencijom, odnosne strane se dogovaraju, kada je to potrebno, u cilju odlučivanja oko toga koja je strana najbolja izvršiti potragu".[17]

Nacionalni izvještaji država Evropske unije upućuju na Agenciju Evropske unije za saradnju u krivičnom pravosuđu (*Eurojust*)[18], Okvirnu odluku Vijeća 2009/948/PUP o sprječavanju i rješavanju sporova o izvršavanju nadležnosti u krivičnim postupcima[19], a povremeno i na Evropsku konvenciju o prijenosu postupka u krivičnim stvarima[20] iz 1972. kao na mehanizme za rješavanje sukoba nadležnosti (spominje se i načelo *ne bis in idem*[21]).

Kada je u pitanju *Eurojust*, važno je osvrnuti se i na činjenicu da je na strateškom sastanku *Eurojust*-a o sajber kriminalu 20. novembra 2014. uspostavljena Evropska mreža sudskih sajber praktičara (*EJCN*), osnovana 2016., tokom nizozemskoga predsjedavanja Evropskom unijom, radi poticanja kontakata među stručnjacima koji su specijalizirani za suzbijanje izazova sajber kriminala, kriminala koji je omogućen putem sajbera i istraga u sajber prostoru, kao i radi

[16] Konvencija Vijeća Evrope o sajber kriminalu usvojena je u Budimpešti 23. novembra 2001., otuda Budimpeštanska konvencija o sajber kriminalu. Prvi je međunarodni ugovor u svijetu o krivičnim djelima počinjenim putem interneta i drugih računarskih mreža. [Electronic version]. Retrieved 03 July 2021, from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa401.

[17] Odjeljak 3, član 22. stav 5. Odluka o ratifikaciji Konvencije o kibernetičkom kriminalu, Odluka Parlamentarne skupštine Bosne i Hercegovine, br. 274/06 od 10. marta 2006., Službeni glasnik BiH – Međunarodni ugovori, br. 6/2006 pod naslovom „Konvencija o kibernetičkom kriminalu".

[18] Agencija Europske unije za suradnju u kaznenom pravosuđu (*Eurojust*). [Electronic version]. Retrieved 05 July 2021, from https://europa.eu/european-union/about-eu/agencies/eurojust_hr.

[19] Okvirna odluka Vijeća 2009/948/PUP o sprječavanju i rješavanju sporova o izvršavanju nadležnosti u krivičnim postupcima. [Electronic version]. Retrieved 05 July 2021, from https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32009F0948.

[20] Evropska konvencija o prijenosu postupka u krivičnim stvarima iz 1972. [Electronic version]. Retrieved 05 July 2021, from https://wapi.gov.me/download/06fe33ff-12f8-4bea-b5ee-924391cc3636?version=1.0.

[21] Načelo *ne bis in idem* utvrđeno je u članu 50. Povelje Evropske unije o temeljnim pravima: „Nikome se ne može ponovno suditi niti ga se može kazniti u kaznenom postupku za kazneno djelo za koje je već pravomoćno oslobođen ili osuđen u Uniji u skladu sa zakonom". [Electronic version]. Retrieved 05 July 2021, from https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:12016P/TXT&from=RO.

povećanja učinkovitosti istraga i krivičnog gonjenja.[22] Također, *Eurojust* je prvi put predložio i koncept digitalnog krivičnog pravosuđa Vijeću Evropske unije u decembru 2018., čiji je cilj bio stvaranje digitalne platforme na cijelom prostoru ove supranacionalne regionalne međunarodne organizacije, kako bi se *Eurojust*-u i široj evropskoj pravosudnoj zajednici omogućilo brzo i učinkovito komuniciranje i razmjena informacija u pogledu krivičnih predmeta i dokaza tokom kriminalističke istrage.[23]

Naime, postoje razni mogući scenariji odnosno brojni načini na koje se mogu implementirati nacionalni pristupi komplementarnosti, gdje materijalna i proceduralna pravila koja uređuju načelo komplementarnosti Međunarodnog krivičnog suda mogu poslužiti kao koristan model za definiranje i primjenu kriterija supsidijarnosti za univerzalnu nadležnost. (Bergsmo, 2010: 156). S druge strane, formiranje jedinstvenog međunarodnog krivičnog suda (tribunala) za sajber krivična djela agresije odvratilo bi počinioce od takvih radnji i osiguralo mjesto za progon, i u slučajevima gdje države inače često odbijaju procesuirati takva djela. (Stahl, 2011: 272). Kao prilog ideji o osnivanju međunarodnog krivičnog suda ili tribunala s nadležnošću za sajber krivična djela može se istaći i skoro osnivanje Međunarodnoga antikorupcijskoga suda (IACC), koji će popuniti međunarodnu prazninu u borbi protiv korupcije i ojačati demokraciju pružanjem nepristranog foruma koji bi trebao biti oslobođen od utjecaja korumpirane politike. (Escobar, 2021). Naime, na posebnoj sjednici o izazovima i mjerama za sprječavanje i borbu protiv korupcije i jačanje međunarodne saradnje, održanoj od 2. do 4. juna 2021. u sjedištu Ujedinjenih nacija u New Yorku, Opća je skupština usvojila političku Deklaraciju „Naša zajednička predanost učinkovitom rješavanju izazova i implementiranju mjera za sprječavanje i borbu protiv korupcije i jačanje međunarodne saradnje".[24]

Prepoznajući višestruke prijetnje korupcije, predsjednik Sjedinjenih Američkih Država Joe Biden izdao je početkom juna 2021. memorandum koji definira borbu protiv korupcije kao temeljni interes nacionalne sigurnosti Sjedinjenih Američkih Država. Više od stotinu svjetskih lidera potpisalo je navedenu Deklaraciju o obrazovanju Međunarodnog suda za borbu protiv korupcije (*IACC*), koji bi procesuirao osumnjičene visoke državne dužnosnike kada nacionalne vlade to ili ne mogu ili ne žele učiniti. (Escobar, 2021). Shodno tome, moglo bi se vrlo

[22] European Judicial Cybercrime Network. [Electronic version]. Retrieved 08 July 2021, from http://www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx.

[23] Digital Criminal Justice. [Electronic version]. Retrieved 08 July 2021, from http://www.eurojust.europa.eu/ Practitioners/digital-criminal-justice/Pages/Digital-criminal-justice.aspx.

[24] UNGASS. Special session of the General Assembly against corruption 2021. [Electronic version]. Retrieved 14 July 2021, from https://ungass2021.unodc.org/ungass2021/index.html.

razložno gledati u svjetlu formiranja međunarodnog krivičnog suda ili tribunala za sajber prostor odnosno sajber terorizam i druga teža sajber krivična djela, koja ugrožavaju državne institucije, nanose veliku ekonomsku štetu i opsturiraju komercijalno i edukativno-informativno korištenje interneta.

Ukoliko se na međunarodnom nivou države ne usaglase oko dodatnih odredbi ili članova koji se mogu inkorporirati u popis krivičnih djela iz nadležnosti Međunarodnog krivičnog suda (*ICC*), alternativno rješenje može biti osnivanje specijaliziranog Međunarodnog krivičnog suda (tribunala) za sajber prostor (*International Criminal Court (Tribunal) for Cyber Crime*). Prijedlog osnivanja Tribunala ili Međunarodnog krivičnog suda za sajber prostor (*ICTC*), koji bi se bavio najozbiljnijim sajber krivičnim djelima od globalnog značaja, detaljno je obrazložio međunarodni stručnjak za sajber kriminal i jedan od utemeljitelja globalnog usklađivanja pravnih normi o kompjuterskom kriminalu, sudac Stein Schjolberg.[25] Prema njegovom Nacrtu Ugovora Ujedinjenih nacija o Međunarodnom krivičnom sudu za sajber prostor, takav bi međunarodni sud imao nadležnost progoniti osobe odgovorne za najteža kršenja međunarodnog prava o sajber kriminalu, u skladu s odredbama nacrta Statuta Međunarodnog krivičnog suda za sajber prostor. (Schjolberg, 2014: 6).

Kao što je istaknuto u samom uvodu ovoga rada, „računarstvo u oblaku" (*cloud omputing*) odnosno krivična djela počinjena s protupravnim učinkom u više nadležnosti, otežavaju tradicionalni način istrage i krivičnoga progona. Stoga i prema Schjolbergu, za efikasne sudske postupke u ovom području neophodno je ustanoviti odgovarajući međunarodni sud. Također, sudija Stein se referira i na zaključak Marca Gercka (Gercke, 2011: 129-160), koji je u svom radu naveo razloge zašto Konvencija o sajber kriminalu Vijeća Evrope nije valjano uspjela na globalnom nivou. Prije svega, to su: (Schjolberg, 2020: 97)

- nedostatak involviranosti država u razvoju u proces izrade Nacrta;
- zahtjevniji postupak pristupanja (akcesije) u poređenju s konvencijama UN-a;
- nedostatak ažuriranja u skladu s trendovima i tendencijama;
- nedostatak propisa o elektronskim dokazima i odgovornosti pružatelja internetskih usluga (ISP);
- nedostatak terenskih ureda izvan Evrope;
- nedostatak podrške izgradnji kapaciteta koji je posebno relevantan za zemlje u razvoju.

[25] Biography of Stein Schjolberg. [Electronic version]. Retrieved 17 July 2021, from https://www.cybercrimelaw.net/biography.html.

Sve prethodno navedeno ukazuje na neophodnost postojanja međunarodnog krivičnog suda ili tribunala s nadležnošću za slučajeve sajber terorizma, i drugih ozbiljnih sajber krivičnih djela, koji bi omogućio rješavanje problema i otklanjanje poteškoća u pogledu zasnivanja nadležnosti za sajber krivična djela.

5. Harmonizacija državnih zakona o sajber kriminalu

Problem jurisdikcijskih sukoba uzrokovanih sajber kriminalom nagnalo je međunarodne organizacije na odluku da se pozovu na „promjenu paradigme", kako bi se omogućila primjena drugih načela nadležnosti kao i da bi se mogla istražiti i procesuirati krivična djela počinjena u visokotehnološkom svijetu. (Odjel za zaštitu podataka i sajber kriminal, 2012).

Takozvana promjena paradigme zahtijeva od pravosudnih vlasti da istražuju nove ideje, puteve i mehanizme za provođenje krivičnog zakonodavstva, kao i da se postojeći pravni mehanizmi uzajamne pomoći učine dinamičnijim i fleksibilnijim po pitanju rješavanja jurisdikcijskih sukoba. Problem prekogranične nadležnosti u pravnom procesuiranju sajber krivičnih djela potrebno je rješavati kroz načela i pravila međunarodnoga prava putem predlaganja određenih pravnih rješenja, i to usvajanjem odgovarajućih međunarodnopravnih instrumenata koji će doprinijeti učinkovitijem suzbijanju te vrste krivičnih djela na međunarodnom nivou. Ta rješenja bi vjerovatno išla u smjeru usklađivanja i preinaka međunarodnih akata, ali i u smjeru harmonizacije državnih propisa koja uređuju sankcioniranje određenih sajber krivičnih djela. Konvencija o sajber kriminalu Vijeća Evrope ima za cilj harmonizirati nacionalna zakonodavstva u domenu materijalnopravnih odredbi iz oblasti visokotehnološkog kriminala, uvođenjem odgovarajućih procesnih instrumenata radi boljeg procesuiranja ovih krivičnih djela i uspostavljanja brzih i efikasnih institucija i procedura međunarodne saradnje.[26]

Slijedom iznijetoga, potonja Konvencija i drugi međunarodni ugovori predstavljaju kvalitetnu polaznu osnovu u eventualnom približavanju nadležnosti država u odnosu na transnacionalni sajber kriminal. U širem smislu, usklađivanje je bitno iz dva razloga, prvi je eliminirati ili barem smanjiti učestalost „sigurnih utočišta" (dvostruka inkriminacija), dok je drugi razlog ključan za učinkovitu saradnju između agencija za provedbu zakona. (Clough, 2014: 701). To ne samo da pomaže u suzbijanju sajber kriminala i omogućava domaće krivične progone, već i olakšava saradnju s drugim državama tako što osigurava načelo dvostruke inkriminacije. (O' Flynn, 2014: 63).

[26] Budapest Convention and related standards. [Electronic version]. Retrieved 23 July 2021, from https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Neophodnost harmonizacije državnih zakona o sajber kriminalu valjalo bi posmatrati iz razloga što kod slučajeva istrage i gonjenja za kompjuterska krivična djela u situacijama istovremene nadležnosti nedostatak procesne usklađenosti krivičnopravnih sistema značajno negativno utječe na način i dužinu trajanja same istrage i progona počinitelja sajber krivičnih djela. Stoga bi se usklađivanje nacionalnih zakona trebalo percipirati kao važan segment za razvoj jedinstvenoga međunarodnoga krivičnopravnoga sistema, koji će omogućiti efikasno prikupljanje dokaza kroz međunarodnu saradnju u krivičnim stvarima, odnosno na nivou izvršenja, gdje bi se države trebale obavezati jedna drugoj da će pomagati pri prikupljanju podataka. (Perloff-Giles, 2017: 64). Tako se u petom stavu člana 22. Budimpeštanske konvencije[27] navodi da u slučaju da je počinjeno krivično djelo bilo usmjereno protiv više ugovornih strana, te su države stranke dužne međusobno se koordinirati i savjetovati, kako bi se osiguralo usklađivanje postupaka i na taj način osigurao uspješan proces suđenja.

Prijedlog da se usklađivanjem zakonâ među državama i promicanjem međunarodne saradnje na području provođenja zakona razvije jedinstven međunarodni krivičnopravni sistem za transnacionalna sajber krivična djela je još jedan od mogućih načina uspješnog rješavanja pitanja jurisdikcijskih sukoba koji nastaju usljed (po)činjenja sajber krivičnih djela. (Perloff-Giles, 2018: 215).

6. Alternativni pristupi kroz nove jurisdikcijske teorije

Sajber krivična djela imaju transnacionalni karakter, budući da uključuju više država u svome „pokretanju, počinjenju i izravnom ili neizravnom učinku" (*United Nations*, 1995), i predstavljaju globalni problem koji se može svrstati u ono što bivši Generalni sekretar Ujedinjenih nacija Kofi Annan naziva „problemima bez pasoša".[28]

Poteškoće u rješavanju jurisdikcijskih sukoba uzrokovanih sajber kriminalom odnosno pitanje ko je nadležan za procesuiranje sajber krivičnih djela dovodi do odlučivanja za jednostavnija rješenja poput toga da se nadležnost domaćega suda zasnuje temeljem državljanstva počinitelja (načelo aktivnoga persona-

[27] Kada više strana ugovornica zahtijeva zasnivanje nadležnosti u pogledu protupravnih čina predviđenih ovom Konvencijom, odnosne strane se dogovaraju, kada je to potrebno, koja je država najpozvanija zasnovati nadležnost. Odluka o ratifikaciji Konvencije o kibernetičkom kriminalu, Odluka Parlamentarne skupštine Bosne i Hercegovine, br. 274/06 od 10. marta 2006., Službeni glasnik BiH – Međunarodni ugovori, br. 6/2006 pod naslovom „Konvencija o kibernetičkom kriminalu".

[28] Environmental Threats Are Quintessential "Problems Without Passports", Secretary General Tells European Environment Ministers, *Press Release, Secretary General, U.N. Press Release* SG/SM/6609, 23 June 1998. [Electronic version]. Retrieved 25 July 2021, from https://www.un.org/press/en/1998/19980623.sgsm6609.html.

liteta). No, postoje mnoge praktične i teorijske prepreke u vezi toga. Također, kod primjene prava na računarstvo u oblaku postoji inkompatibilnost, budući da računarstvo u oblaku podrazumijeva smanjenje nivoa izravne kontrole, dok je zakonodavstvo Evropske unije u potpunosti usmjereno ka uspostavljanju kontrole podataka. (O'Keeffe, 2012: 1). Zbog toga postoji prepoznatljiv trend dopune teritorijalnosti s ekstrateritorijalnim načelima. Tako uočavamo širenje teritorijalne nadležnosti izvan geografske teritorije države u primjeru odgovora određenih zemalja u vezi s dječijom seks industrijom (*child sex industry*). (Wallace, Janeczko, Wylie, 2013: 112). Zapravo, širenje teritorijalne nadležnosti u kontekstu transnacionalnog sajber kriminala je danas nužno, jer i sveprisutna upotreba usluga u oblaku postavlja dodatne različite izazove u borbi protiv ovakve vrste krivičnih djela u kojoj osnovna načela teritorijalnosti domaćega suda, uspostavljena međunarodnim i unutrašnjim pravom, ne pružaju jasna rješenja.[29]

Suočeni s ovim izazovom, neki pravni stručnjaci su postali manje optimistični zaključujući da je sajber prostor „prostor koji se ne može kontrolirati" (Marmo, Chazal, 2016: 66), dok su pojedini pisci, pored isticanja preventivnih mjera sigurnosti, na prioritetno mjesto predlagali i neke nove jurisdikcijske teorije odnosno načine uspostavljanja učinkovite nadležnosti domaćega suda.

6.1. Teorija novog (sajber) suvereniteta

Trenutno ni međunarodno krivično pravo, a ni domaće krivično pravo, učinkovito ne reguliraju ili ne suzbijaju transnacionalna sajber krivična djela, s obzirom da su sistem nacionalnog prava i transnacionalni internet sami po sebi nepomirljivi, tako da se regulatori suočavaju s vrlo jednostavnim izborom, ili da učine zakon više transnacionalnim ili internetsku aktivnost manje transnacionalnom. (Kohl, 2007: 28). Prema teoriji novog suvereniteta ili sajber suvereniteta, sajber prostor je stvorio globalno civilno društvo koje ima svoj oblik organizacije, vrijednosti i pravila, i, shodno tome, treba da ima izdvojen i poseban sistem zakona primjenjivih na sajber prostor, razvijen na način da nadležnost nad kompjuterskim i sajber kriminalom ne ovisi o tradicionalnoj krivičnoj nadležnosti. (Xiaobing, Yongfeng, 2018: 795).

Jednako tako, postavlja se pitanje da li se suverenost može utvrditi u sajber prostoru koji, pored fizičke, ima i virtualnu komponentu, odnosno da li država može imati nadležnost nad objektima ili aktivnostima u virtualnom svijetu sajber prostora. Premisa da sajber prostor ima ateritorijalne karakteristike, dok, istovremeno, pojam teritorije nije nužno sastavni element suvereniteta gdje koncept suverenosti prvenstveno znači vlast i moć odnosno nije inherentno

[29] Jednako tako, v. nadležnost baziranu na „*effects principle*", koja je svoju primjenu naročito našla u antimonopolskom zakonodavstvu Sjedinjenih Američkih Država.

teritorijalna, dovodi do zaključka da države mogu vršiti svoju nadležnost jednostrano ili u saradnji s drugim državama, tj. da se suverenost može proširiti i na neteritorijalne entitete ili dimenziju. (Tsagourias, 2015: 21).

Naime, već sada pojedine države prakticiraju svoju viziju sajber suvereniteta nad „domaćim" internetom, poput npr. Narodne Republike Kine, gdje je dvije trećine svih korisnika interneta trenutno podvrgnuto određenom stepenu cenzure kritika usmjerenih prema vladi, vojsci ili vladajućim elitama. (Shackelford, 2020: 1335). Narodna Republika Kina kao jedan od lidera u digitalnom svijetu nastoji da na međunarodnom nivou povede rasprave o tome kako treba upravljati sajber prostorom, predlažući svoj koncept sajber suvereniteta. Tu svoju viziju globalnog upravljanja sajber prostorom, a posebno koncepta sajber suvereniteta, predstavili su u posebnom izvještaju Nacionalnoga biroa za azijska istraživanja, pod nazivom „Kineska vizija sajber suvereniteta i globalno upravljanje sajber prostorom". Ova država zajedno s Ruskom Federacijom smatraju da države moraju štititi i kontrolirati internet kako bi zaštitile svoj suverenitet, dok, s druge strane, Sjedinjene Američke Države i Evropska unija smatraju da se trebaju očuvati demokratske karakteristike, poput otvorenosti, brzine, fleksibilnosti i učinkovitosti samoga interneta. (Chertoff, 2014: 13).

S obzirom da sajber prostor ne može postati suveren, ali može biti podložan suverenosti (Tsagourias, 2015: 21), potrebno je, kada se razgovara o sajber suverenitetu, prihvatiti ili barem razmotriti razuman prijenos kontrole u doba globalizacije, digitalnih tehnologija i informacijskoga društva, gdje svaka država treba pažljivo odrediti i odlučiti koje elemente suvereniteta će zadržati, a koje može prenijeti i u kojoj mjeri (tzv. višedržavno upravljanje) (Yeli, 2017: 112).

6.2. Načelo minimalnog kontakta

Ukazivanje na nefunkcionalnu karakteristiku teritorijalne jurisdikcije, koja se posebno komplicira s pojavom sajber kriminala (Arnell, 2001: 958), sugerira da se „smanjeni značaj granica" i internacionalizacija kriminala mogu koristiti kao argument u korist fleksibilnije prekogranične primjene teritorijalnih načela ili univerzalne nadležnosti. (Hirst, 2003: 203). Shodno tom načinu razumijevanja ostvarivanja odnosno uspostavljanja nadležnosti kada su u pitanju sajber krivična djela, Sjedinjene Američke Države izdaju potjernice ili optužuju sajber kriminalce u odsutnosti na temelju raznih jurisdikcijskih načela. Neki slučajevi pokazuju raznolikost mehanizama za traženje teritorijalne nadležnosti domaćega suda u odnosnoj državi, od dostupnosti web stranice u toj državi, korištenju platnih usluga servisa koji su locirani na tome državnome području, spremanju podataka na američkim serverima, usmjerenost napada na američke korporacije ili računare. Međutim, načelo koje Sjedinjene Američke Države najčešće koriste

је начело минималноga контакта (Law College Chicago-Kent, 2021) према којем да би суд вршио кривичну надлежност над случајем, односно у предмету над окривљеним за кривично дјело које је починио, потребно је да постоје одређени минимални контакти између оптуженога и суда како би се испунили захтјеви прописаноga и правичноga поступка. (Xiaobing, Yongfeng, 2018: 795).

U svojoj knjizi „*Cyberthreats and the Decline of the Nation-State*" Susan W. Brenner navodi da sajber kriminalci obično prođu nekažnjeno u svojim kriminalnim radnjama, ukazujući na lakoću kojom ti počinitelji izvršavaju krivična djela. Upravo da bi se osiguralo da sajber kriminalci ne izbjegnu suočavanje s pravdom, Sjedinjene Američke Државе koriste načelo minimalnog kontakta. To im olakšava traženje izručenja od drugih država, čak i u situacijama kada se nadležnost domaćega američкoga suda gradi na mnogo nestabilnijim osnovama. Naime, najčešći izrazi u američkim optužnicama odnose se na počinjenu štetu „u Sjedinjenim Državama i drugim mjestima", i to je za Sjedinjene Američке Државе dovoljno da se izručenje, temeljem njihove zamolnice, izvrši. (O' Flynn, 2014: 205). Tendenciju američkih sudova da održavaju integritet testa minimalnih kontakata u sajber prostoru, između ostalog, mnogi smatraju poštenim i razumnim načinom rješavanja pitanja zasnivanja nadležnosti koji se nastavlja prilagođavati novom polju sajber prostora. (Leigh, 2002: 95).

6.3. Teorija četvrtog (novog) međunarodnog prostora

Sajber prostor nema granica i ne potpada pod suverenitet ni jedne nacije. Zbog ove se činjenice sajber prostor identificira kao opće zajedničko dobro ili *res communis (omnium) (the common heritage of all humankind).* Darrel Menthe s Univerziteta Stanford u Sjedinjenim Američkim Državama predstavio je „četvrtu teoriju međunarodnoga prostora"[30], nakon Antarktika, svemira i otvorenoga mora. (Menthe, 1998: 70). Prema odnosnoj teoriji, sajber prostor bi trebao da postoji kao nova nadležnost, poput posebnih pravila međunarodnoga prava koja se primjenjuju na dijelove naše planete koji se nalaze izvan nacionalnih jurisdikcija država, otvorenoga mora, međunarodne zone dna mora i okeana, međunarodnoga zračnoga prostora, Antarktika i svemira, uspostavljajući na taj način nova pravila o nadležnosti koja se razlikuju od tradicionalnih. (Xiaobing, Yongfeng, 2018: 795).

Protivnici ove teorije smatraju da je to problematično iz razloga što pravni status, položaj i priroda sajber prostora prema međunarodnom pravu tek trebaju biti u potpunosti uspostavljeni i uređeni. (Ikeshima, 2018: 38). U današњem

[30] Radi sveobuhvatnoga pregleda, valjalo bi imati u vidu i pravni režim međunarodne zone dna mora i okeana, ali, jednako tako, ne gubiti iz vida ni međunarodni zračni prostor. Ako držimo ove prostore zasebnima, onda je sajber prostor zapravo šesti međunarodni prostor.

dobu, međunarodno pravo već identificira pet globalnih dobara, otvoreno more, međunarodnu zonu dna mora i okeana, međunarodni zračni prostor, Antarktik i svemir, kao zajedničke baštine čovječanstva, čiji prostori nisu *terra (res) nullius*, ali su *res extra commercium*. S obzirom na navedena globalna dobra, mišljenje je da bi sajber prostorom, kao novim međunarodnim prostorom, trebalo upravljati na osnovu zadanih pravila međunarodnoga prava koja su slična pravilima koja uređuju ostale međunarodne prostore. (Menthe, 1998: 85).

7. Zaključak

Internet stvara pravu svjetsku mrežu istodobnih jurisdikcijskih zahtjeva odnosno sukoba nadležnosti. Zato međunarodni akti i standardi za prekograničnu borbu protiv kompjuterskog kriminala, posebno Konvencija o sajber kriminalu Vijeća Evrope, kao i međunarodne organizacije koje doprinose harmonizaciji nacionalnih zakonodavstava, ukazuju na značaj ulaganja pravnih napora u eventualnom približavanju i rješavanju teškoća adekvatnoga zasnivanja nadležnosti za djela sajber kriminala. Prije svega, važno je riješiti pitanje prvenstva, a jedan od načina rješavanja problema zasnivanja nadležnosti nad predmetnim djelima je i koncept usklađivanja međunarodnih akata i harmonizacija državnih zakona za određena sajber transnacionalna krivična djela. Jasno je da prema međunarodnom krivičnom pravu postoje značajni izazovi u procesuiranju počinitelja transnacionalnih sajber krivičnih djela. Zbog toga prijedlozi za razvoj normi međunarodnoga prava u pogledu (obavezne) razmjene informacija i podataka te inkorporiranje međunarodnopravnih načela iz ove oblasti u domaće pravo sugeriraju kako međunarodno krivično pravo može promicati odgovornost na način da bi države morale žrtvovati određeni stepen svoga suvereniteta kao preduslov za efikasnije procesuiranje transnacionalnih sajber krivičnih djela. Naime, i antiteritorijalni aspekt računarstva u oblaku, koji zbog svoje nelokalizirane karakteristike predstavlja dodatnu otežavajuću okolnost pri utvrđivanju jurisdikcije za čćinjena sajber krivična djela, ukazuje na nužnost ostvarivanja saradnje između internet servis provajdera i pravosudnih institucija.

S obzirom na to, ali i na činjenicu kako se međunarodno krivično sudovanje još uvijek razvija, ne vidimo veću zapreku da se ustanovi novi međunarodni tribunal koji će biti stvarno nadležan za slučajeve sajber terorizma i drugih ozbiljnih sajber krivičnih djela. Držimo da bi se, da postoji takav sud ili tribunal, mogla poslati snažna poruka međunarodnoj internetskoj zajednici da sajber krivična djela neće proći nekažnjeno. U virtualnom, sajber prostoru odlike smanjenoga značaja državnih granica i prisutnost trendova internacionalizacije kriminala bi se ponajprije mogle koristiti kao argument u korist fleksibilnije prekogranične primjene teritorijalnih i drugih jurisdikcijskih načela ili, pak, primjene

nekog oblika univerzalne nadležnosti. Zbog te svojevrsne nefunkcionalne karakteristike teritorijalne jurisdikcije u kontekstu sajber kriminala, već sada postoji prepoznatljiva tendencija dopune teritorijalnosti s ekstrateritorijalnim načelima (elementima), gdje se predlažu i neke nove teorije nadležnosti. Stoga bi valjalo razmisliti i o adekvatnoj primjeni novih jurisdikcijskih teorija, poput teorije novog suvereniteta, teorije novog međunarodnog prostora, ali i teorije minimalnoga kontakta.

Literatura

Arnell, P. (2001). The Case For Nationality Based Jurisdiction. *International and Comparative Law Quarterly.* Volume 50. Issue 4. 955 – 962

Bergsmo, M. (2010). *Complementarity and the Exercise of Universal Jurisdiction for Core International Crimes*. Oslo: Torkel Opsahl Academic EPublisher and Peace Research Institute Oslo (PRIO). Publication Series (No.7)

Berman, P. S. (2012). *Global legal pluralism: A jurisprudence of law beyond borders*. Cambridge: Cambridge University Press

Brenner S. W., Koops, B. J., (2004). Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law.* 1. 1-44

Cesare, P. (2010). 'The Kelsen/Schmitt Controversy and the Evolving Relations between Constitutional and International Law". *Ratio Juris.* 23. 493-504

Cherif Bassiouni, M. (2001). Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice, *42 Virginia Journal of international Law 81.* 2001, 82-162

Chertoff, M. (2014). The Strategic Significance of the Internet Commons. *Strategic Studies Quarterly*. 10-16

Clough, J. (2014). A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation. *Monash University Law Review*. 40. 698-736

Cockayne, J. (2005). Review: "On the Cosmopolitanization of Criminal Jurisdiction". *Journal of International Criminal Justice*. 3(2).

Cohen, S., Morril, M.C. (2019). "TDM Special Issue "Cybersecurity in International Arbitration" - Introduction" TDM 3. [Electronic version]. Retrieved 13 June 2021, from www.transnational-dispute-management.com

Degan, V.Đ. (2011). *Međunarodno pravo*. Zagreb: Školska knjiga.

Degan, V.Đ., Pavišić, B., Beširević, V. (2011). *Međunarodno i transnacionalno krivično pravo*. Beograd: Pravni fakultet Univerziteta Union u Beogradu i Javno preduzeće Službeni glasnik

Đorđević, M. (2020). Arbitraža – pojam, karakteristike i vrste. [Electronic version]. Retrieved 03 June 2021, from http://www.ius.bg.ac.rs/prof/materijali/yormil/Arbitraza.pdf

Escobar, M. C. (2021). The Case for an International Anti-Corruption Court. [Electronic version]. Retrieved 13 July 2021, from https://www.americasquarterly.org/article/the-case-for-an-international-anti-corruption-court/

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2011). The Law of Cyber-Attack. *California Law Review*. 100. 1-72

Hirst, M. (2003). *Jurisdiction and the Ambit of the Criminal Law*, Oxford: Oxford University Press

Ikeshima, T. (2018). The Notion of Global Commons under International Law: Recent Uses and Limitations within a Security and Military Context, *Transcommunication*. Vol. 5-1. 37-46

Jugović Spajic, D. (2019). Cybercrime Statistics That Will Make You Change Your Password. [Electronic version]. Retrieved 17 June 2021, from https://kommandotech.com/%20statistics/cybercrime-statistics/

Kleijssen, J., Perri, P. (2017). Chapter 7 Cybercrime, Evidence and Territoriality: Issues and Options, *Netherlands Yearbook of International Law 2016.* (Netherlands Yearbook of International Law 47). 147-173

Klip, A. (2014). Section IV – International criminal law. Information society and penal law. [Electronic version]. Retrieved 03 July 2021, from https://www.cairn.info/article.php?ID_ARTICLE=RIDP_851_0381&contenu=article

Kohl, U. (2007). *Jurisdiction and the Internet, Regulatory Competence over Online Activity.* Cambridge: Cambridge University Press

Konforta, M., Munivrana-Vajda, M. (2014). Načelo komplementarnosti u praksi Međunarodnog kaznenog suda, *Zagrebačka pravna revija*, Vol. 3. No. 1. 9-27

Kontorovich, E. (2003). The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation. *Harvard International Law Journal. 45*. 183-238

Law College Chicago-Kent. *Project documentation*. An overview of the law of personal (adjudicatory) jurisdiction: The United States perspective. [Electronic version]. Retrieved 01 August 2021, from http://www.kentlaw.edu/cyberlaw/docs/rfc/usview.html

Leigh, G. T. (2002). Minimum Contacts in Cyberspace: The Classic Jurisdiction Analysis in a New Setting, *Journal of High Technology Law*, Vol. 1. No. 1. 85-100

Leslie, D. A. (2014). *Legal Principles for Combatting Cyberlaundering*, Basel: Springer International Publishing Switzerland

Luban, D. (2018). "The Enemy of All Humanity", *Netherlands Journal of Legal Philosophy*, 47(Vol. 2). 112-137

Mann, F. A. (1984). *The Doctrine of International Jurisdiction Revisited After Twenty Years*. Series: Recueil des cours, 186. Leiden: Martinus Nijhoff

Marmo, M., Chazal, N. (2016). *Transnational crime and criminala justice*. London: SAGE Publications Ltd

Menthe, D.C. (1998). Jurisdiction in Cyberspace: A Theory of International Spaces, *4 Mich. Telecomm. & Tech. L. Rev*. 69. 69-101. [Electronic version]. Retrieved 10 August 2021, from https://repository.law.umich.edu/mttlr/vol4/iss1/3.

Mladenović, D. (2012). *Međunarodni aspekt sajber ratovanja*. Beograd: Medija centar ''Odbrana'' Beograd

Munivrana, M. (2006). Universal jurisdiction. *Croatian Annual of Criminal Law and Practice.* 13(1). 189-235

Natarajan, M. (2019). *International and Transnational Crime and Justice*. 2nd edition. Cambridge: Cambridge University Press

O' Flynn, M. A. (2014). Harmonisation and Cybercrime Jurisdiction: Uneasy Bedfellows? An analysis of the jurisdictional trajectories of the Council of Europe's Cybercrime Convention. Doctoral thesis on School of Law Queen Mary, University of London

O'Keeffe, V. (2012). (Jurisdictional issues associated with a move to the Cloud. *Academia 3*. 1-8. [Electronic version]. Retrieved 27 July 2021, from

Obokata, T. (2010). *Transnational Organised Crime in International Law*, London: Hart Publishing

Odjel za zaštitu podataka i sajber kriminal. Global Project on Cybercrime. Cooperation against Cybercrime in 2012. Activities of the Council of Europe. Document prepared for information of the Cybercrime Convention Committee (T-CY). (2012)

Perloff-Giles, A. (2017). "Problem without a passport": Overcoming jurisdictional challenges for transnational cyber aggressions, *Yale Journal of International Law*. 1-68

Perloff-Giles, A. (2018). Transnational Cyber Offenses: Overcoming jurisdictional challenges. *Yale Journal of International Law.* Vol. 43. 191-227

Program in Law and Public Affairs and Woodrow Wilson School of Public and International Affairs, Princeton University, International Commission of Jurists, American Association for the International Commission of Jurists, Netherlands Institute of Human Rights, Urban Morgan Institute for Human Rights. *Princeton Project on Universal Jurisdiction.* (2001)

Rho, J. J. (2007). "Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute". *Chicago Journal of International Law*: Vol. 7: No. 2, Article 18. 695-718

Šačić, Z. (2000). International cooperation of the croatian ministry of the interior- forms, goals, features and noticed problems. *Croatian Annual of Criminal Law and Practice*, 7. (1/2000). 123-163

Scharf, M. P., Newton, M. A., Sterio, M. (2015). *Prosecuting Maritime Piracy: Domestic Solutions to International Crimes*. Cambridge: Cambridge University Press

Schjolberg, S. (2014). The third pillar for cyberspace: An international court or tribunal for cyberspace, 9th ed. [Electronic version]. Retrieved 18 July 2021, from http://www.cybercrimelaw.net/documents/140626 Draft_Treaty_text.pdf

Schjolberg, S. (2020). *The History of Cybercrime-Third Edition*. Norderstedt: Books on Demand Germany

Shackelford, S. J. (2020). The future of frontiers. *Lewis & Clark Law Review*. 1331-1384. Shackelford, S. J. (2020). *Governing New Frontiers in the Information Age: Toward Cyber Peace*. Cambridge: Cambridge University Press

Stahl, W. M. (2011). The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. *40 Ga. J. Int'L & Comp. L*. 248-272

Tsagourias, N. (2015). "The legal status of cyberspace". poglavlje 1. 13-29. U: *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing Limited.

United Nations. Ninth U.N. Congress on the Prevention of Crime & the Treatment of Offenders, *Interim Report by the Secretariat*. U.N. Doc. A/CONF.169/15/Add.1. 4 april (1995)

Urbas, G., Choo, K. K. (2008). Resource Materials on Technology-Enabled Crime. *Technical and Background Paper.* No. 28. 1-66

Wallace R., Janeczko F., Wylie K. (2013). *Nutshells. International Law*. London: Sweet&Maxwell.

Wible, B. (2002). De-Jeopardizing Justice: Domestic Prosecutions for International Crimes and the Need for Transnational Convergence, *Denver Journal of International Law & Policy*. Vol. 31. No. 2. 264-295

Xiaobing, L., Yongfeng, Q. (2018). Research on Criminal Jurisdiction of Computer cybercrime, *Procedia Computer Science 131*. 8th International Congress of Information and Communication Technology (ICICT). 793-799

Yeli, H. (2017). A Three-Perspective Theory of Cyber Sovereignty. *Prism: A Journal of the Center for Complex Operations. 7*. 109-115

Zaharia, A. (2021). 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends. [Electronic version]. Retrieved 17 June 2021, from https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

Doc. Enis Omerović, LL.D.,
Assistant Professor,
Faculty of Law, University of Zenica,
Bosnia and Herzegovina
Damir Imamović, LL.M.,
Civil servant of Zenica-Doboj Canton,
Zenica, Bosnia and Herzegovina

ALTERNATIVE APPROACHES AND PROPOSALS FOR RESOLVING JURISDICTIONAL CONFLICTS CAUSED BY CYBERCRIME

Summary

The aim of the paper was to find and present an adequate approach to resolving jurisdictional conflicts caused by cybercrime. The territorial characteristic of cybercrime is manifested in the absence of borders within cyberspace. Accordingly, the fact that cybercrime is committed within the jurisdiction of different states, there is no single legal framework for regulating all acts of cybercrime. The process of digitalization, i.e., the constant and dynamic movement of data through different servers or "clouds" located in multiple jurisdictions, indicates certain legal limitations in the application of the principle of territoriality in cyberspace. Due to this non-functional characteristic of territorial jurisdiction, the authors in the paper try to point out the importance of determining the basis of jurisdiction in the processing of cybercrime through the presentation of different paradigms and/or approaches, as a supplement to the territorial principle in resolving jurisdictional conflicts. Namely, in the paper the importance of investing legal efforts in the eventual approaching and resolving the conflict of jurisdiction in terms of applying the most adequate principle of jurisdiction by domestic courts in each specific case is shown. These solutions would probably go in the direction of harmonization and revision of international acts, as well as in the direction of harmonization of state regulations governing the sanctioning of certain cybercrimes. Also, the existence of an international criminal court or tribunal with jurisdiction over cases of cyber terrorism and other serious cybercrimes, with the application of new jurisdictional theories, would enable solving problems and eliminating difficulties for the establishment and application of an adequate principle of jurisdiction over cybercrimes.

Keywords: *jurisdiction, cybercrime, territorial jurisdiction, harmonization, universal jurisdiction.*

Др Душица Миладиновић-Стефановић*,*
Ванредни професор,
Правни факултет Универзитета у Нишу,
Србија

UDK: 004:343.6-053.6

*ИСКОРИШЋАВАЊЕ РАЧУНАРСКЕ МРЕЖЕ ИЛИ КОМУНИКАЦИЈЕ ДРУГИМ ТЕХНИЧКИМ СРЕДСТВИМА ЗА ИЗВРШЕЊЕ КРИВИЧНИХ ДЕЛА ПРОТИВ ПОЛНЕ СЛОБОДЕ ПРЕМА МАЛОЛЕТНОМ ЛИЦУ***

Апстракт: *Развој информационо-комуникационих технологија, њихова распрострањеност и широка доступност довели су до значајних промена у начину успостављања контакта и начину општења са другим људима. Поред несумњивих предности технологије, која нам је омогућила да „једним кликом", брзо и лако као никада раније, тренутно разменимо информације са неким на другом крају света и тиме савладамо огромну просторну удаљеност, појавиле су се и различите могућности њене злоупотребе, различити нови безбедносни изазови. Чини се да су тиме посебно угрожени малолетници који, без обзира на то што су рођени у „дигиталном свету" и што га некада много боље познају од одраслих, нису увек свесни ризика које он са собом носи. Иако они на различите начине могу бити виктимизирани у поменутом посредованом облику комуникације, истраживање у оквирима овога рада фокусирано је на тзв. online grooming, проналажење и припремање потенцијалне жртве за сексуалну злоупотребу. У том смислу, посебна пажња посвећена је анализи инкриминације искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу из члана 185б Кривичног законика Републике Србије, као правног одговора на наведену појаву. Да ли је она усклађена са захтевима постављеним у Конвенцији Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања, шта је показала досадашња судска пракса, какав је њен кримнално-политички значај и у ком правцу би се могао кретати њен развој de lege ferenda, основна су питања о којима се у овом раду расправља.*

* dusica@prafak.ni.ac.rs

** Рад представља резултат истраживања на пројекту „Одговорност у правном и друштвеном контексту", који финансира Правни факултет Универзитета у Нишу, у периоду од 2021. до 2025. године.

Кључне речи: *искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу, Кривични законик Републике Србије.*

1. Уводна разматрања или укратко о појму и карактеристикама тзв. *online grooming*-а

Етимолошки посматрано, термин *grooming*, потиче од глагола чије је основно значење тимарити, дотерати, извежбати и припремити (Benson, 1988: 292). Један од првих аутора који га је употребио у контексту криминалитета је *Ken Lanning*, да би означио понашање учиниоца какво се у неким случајевима јавља пре самог извршења сексуалног кривичног дела (више о томе у Burges, Hartman, 2018: 18), а које се раније погрешно називало завођењем жртве (*seduction*), услед чега се губила разлика између нормалног опхођења у сексуалним односима и сексуалне виктимизације (Berliner, 2018: 25). Наиме, ради се о томе да поједини учиниоци не извршавају сексуалне деликте искоришћавањем неке случајне погодне прилике, они се не понашају пасивно у ишчекивању, већ активно трагају за својом приликом, сами је проналазе и организују. У криминолошкој теорији данас постоје различите дефиниције *grooming*-а, при чему се често наводи да је то процес у којем одрасла особа припрема дете, али и особе из његовог окружења и објективне околности у циљу сексуалне злоупотребе детета[1] (Craven, Brown, Gilchrist, 2006: 297). У питању је посебна манипулативна стратегија или тактика, састављена од читавог низа међусобно повезаних корака, почевши од одабира потенцијалне жртве, успостављања комуникације са њом, како би се потом задобијањем њеног поверења, заиста и остварио физички контакт и прешло на извршење дела (Winters, Jeglic, 2017: 725-727). Емпиријска истраживања показују да ова појава уопште није за занемаривање, како скоро половина сексуалних делинквената који су дело учинили на штету детета примењује управо описани модус понашања (Winters, Jeglic, 2017: 724). Деца често не разумеју на прави начин ово дешавање, услед менталне и емотивне манипулације којој су изложена, она не доживљавају понашање *groomer*-а као недозвољено или патолошко, могу се осећати као његови саучесници, као искључиви кривци за евентуални нежељени развој догађаја, а могу га чак и оправдавати и бранити (Berliner, 2018: 25, Martellozzo, 2017: 122), што је сигурно један од разлога због којег се оно и не пријављује и остаје недовољно примећено. Укратко речено, суштина лежи у томе што овако „обрађена” деца некада наивно

[1] У овом делу излагања биће коришћен термин дете за особу која није пунолетна, како се то често чини у криминолошкој литератури.

верују да су у „добровољној емотивној вези" са *groomer*-ом, без свести да су заправо изманипулисана и злоупотребљена.

Док се овај процес раније морао одвијати *in persona*, уз све ризике који су са тиме повезани, експанзија информационо-комуникационих технологија омогућила је његово премештање у виртуелни свет, прерастање у тзв *online grooming*. Може се рећи да је поменутом дислокацијом он добио малигнију форму, и то из више разлога. Један од њих је анонимност сексуалних предатора, који се могу приближити детету коришћењем лажног идентитета, на пример изигравањем вршњака, што се по неким истраживачима дешава и трећини случајева (Winters, Kaylor, Jeglic, 2016: 3). Такође, деца данас нормалну и разумљиву потребу за социјализацијом у приличној мери задовољавају у *online* заједници, а не на „старомодан" *offline* начин, као генерације њихових родитеља, па да су лакше и у већем броју доступна за потенцијалне злоупотребе и то чак и за време док безбрижно седе у својим домовима. Тако су и класичне родитељске методе заштите од опасности „спољног света", остваривање ограничавањем и контролом изласка у исти, постале потпуно неделотворне, пошто је „спољни свет" посредством савремених технологија ушао у сваки дом. Поред тога, истраживања показују и да су деца слободнија и мање обазрива у *online* него у *tête-à-tête* комуникацији, више склона да поделе различите информације о себи него у реалном свету, што их додатно чини рањивим (Ezioni, 2020: 8, Martellozzo, 2017: 109). Не треба занемарити ни друге промене у друштвеном понашању деце, тј. све интензивније инсистирање на томе да буду (пре времена) независна и да имају право на поштовање приватности, које поистовећују са тиме да ни на који начин не буду надзирана и контролисана од стране родитеља. И неке опште околности, попут широке доступности савремених информационо-комуникационих технологија, презапослености и презаузетости родитеља, али често и њихове мање информатичке компетенције у односу на децу само погоршавају ситуацију. Што се осталих фактора ризика тиче, у теорији је примећено да су девојчице подложније опасности од *online* виктимизације, али су и спремније да је пријаве, док су дечаци више постиђени виктимизацијом, јер је сматрају атаком на мужевност, што их и одвраћа од пријављивања (више о различитим истраживањима о томе у Martellozzo, 2017: 115). Са друге стране, нема сагласности око тога који је узраст деце најугроженији, неки налази говоре о деци пре пубертета, неки о адолсецентима (детаљније у Martellozzo, 2017: 116-118, Winters, Kaylor, Jeglic, 2016: 4).

Како се *online grooming* јавља као припремна фаза за извршење неког сексуалног дела, у теорији је присутан став да се учиниоци који га практикују условно могу поделити у две групе, у зависности од тога за која дела се

врши припремање. Тако првој групи припадају они који своје сексуалне фантазије и потребе задовољавају *online*, а другој они чији је примарни циљ да се нађу са жртвом *offline,* тј. у реалном свету, и тако изврше сексуалну злоупотребу (више о различитим истраживањима на ту тему у Martellozzo, 2017: 111-113). Иако је сама појава *online grooming*-а, као релативно нова и мање проучена од класичних облика контактне сексуалне делинквенције, постоје и нека даља запажања о профилу учинилаца, по којима је типичан *groomer* белац мушког пола, тридесетих година, са вишим степеном полних девијација и проблемима у контроли понашања (Winters, Kaylor, Jeglic, 2016: 2 и 7), али се она из поменутих разлога морају узети са резервом.

Осим тога што *grooming* као последицу може имати извршење различитих кривичних дела, он може бити повезан и са дугорочним психичким последицама, попут ниског самопоуздања и самопоштовања, до депресије и покушаја самоубистава (Wood, Wheatcroft, 2020: 3-4).

2. Процена ризика виктимизације од online grooming-а у Републици Србији – доступност информационо-комуникационих технологија, навике малолетних лица приликом њиховог коришћења и родитељска контрола

Присутност рачунара и могућност приступа интернету у породичним домаћинаствима у Републици Србији су у константном порасту, тако да према званичним подацима за 2020. годину 74,3% домаћинстава поседује рачунар, а 81% и интернет прикључак (Републички завод за статистику, 2020: 10-12). Када се томе дода и широка распрострањеност употребе мобилних телефона (94,1% становника, Републички завод за статистику, 2020: 19) постаје јасно какве се комуникацијске перспективе тиме отварају, укључујући и различите могућности злоупотребе. Иако се и на основу опште статистике може добити некакав оквирни увид у потенцијалну изложеност малолетних лица ризицима, много су значајнији подаци који се односе на њих непосредно, на то у којој мери поседују уређаје за овакав вид комуникације, да ли их самостално користе или постоји нека контрола и надзор од стране родитеља и генерално каква су њихова интересовања и навике у дигиталном простору. Нажалост, код нас је до сада било мало емпиријских истраживања са тако постављеним предметом, а она малобројна су дошла до узнемирујућих резултата. Старије је спроведено 2012. године[2]

[2] Истраживање је обављено у оквиру пројекта „Зауставимо дигитално насиље" чији су носиоци Министарство просвете, науке и технолошког развоја и канцеларија УНИЦЕФ-а за Србију. Узорак је био састављен од ученика 17 основних и 17 средњих школа са територије Србије, који су подељени у три старосне групе: од 10 година

и оно је показало да међу популацијом деце која иду у основну школу њих 84% у четвртом разреду има свој мобилни телефон, у старијим разредима 94%, док међу средњошколцима заступљеност расте на чак 99%. Преко 90% ученика из узорка користи рачунар, а њих 60% има свој рачунар. Што се интернета тиче, међу испитаним ученицима само 17% полазника четвртог разреда га не користи, мада се у старијем узрасту то значајније мења, јер старији ученици основне школе у 6,5% не користе инетрнет, а средњошколци у само 3%. Занимљиве су и навике ученичке популације на интернету, јер се углавном ради о забави, при чему је најучесталија активност посећивање друштвених мрежа, која је за 69% старијих основаца и 81% средњошколаца свакодневна или скоро свакодневна активност, док се млађи у 95% посвећују игрању игрица на интернету. Истраживањем су мапирана и најчешћа ризична понашања на интернету – прихватање позива за пријатељство на друштвеним мрежама од стране непознатих особа (43% старијих основаца и 71% средњошколаца), као и комуницирање путем чета са непознатим особама (28% старијих основаца и 56% средњошколаца), а оно што посебно забрињава јесте и податак да су се испитаници, по сопственом признању, и састајали са лицима која су упознали преко интернета (6% основаца и 15% средњошколаца). Занимљиво је да се у случају појаве проблема испитивани ученици изјавили да би се пре обратили за помоћ вршњацима, него родитељима или наставницима, чије су дигиталне компетенције оценили као слабије од сопствених. Када се на све то дода да је око половине испитаних малолетних лица тврдило да имају неограничени приступ интернету (у односу на времене коришћења и врсту активности) и да од родитеља нису добили никакве инструкције о томе како да га користе, настаје јаснија слика о потенцијалној вулнерабилности ове популације за различите облике сајбер злоупотреба.

Друго истраживање које би требало поменути у овом контексту спроведено је 2016. године под окриљем УНИЦЕФ-а.[3] Узорак су овога пута чинили родитељи деце узраста од осам до седамнаест година, тако да су у фокус истраживања постављена питања, као што су: утврђивање степена њихове интернет писмености и компетентности, утврђивање степена свести о потенцијалним ризицима којима се њихова деца излажу приликом

(ученици четвртог разреда основне школе), од 12 до 14 година (од шестог до осмог разреда основне школе) и од 16 до 18 година (ученици од другог до четвртог разреда средње школе). Резултати истраживања су приказани према Попадић, Кузмановић, 2013: 9-11.

[3] У питању је део ширег пројекта „Global Kids Online" и „EU Kids Online" (у преводу Деца света на интернету и Деца Европе на интернету), више о томе на http://www.lse.ac.uk/media@lse/research/Global-Kids-Online.aspx и http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx, приступ 20.01.2021. године.

коришћења интернета, али и утврђивање мера које они предузимају у циљу сигурног коришћења интернета. Што се тиче присутности информационо-комуникационих технологија у домаћинствима у којима живе малолетна лица, у чак 83,3% постоје смарт телефони, односно уређаји који омогућавају мобилни приступ интернету, док је доступност класичног, статичног интернета још већа, како 90% оваквих домаћинстава располаже неким уређајем који то омогућава (УНИЦЕФ, 2016: 14-15). Директна изложеност малолетних лица информационо-комуникационим технологијама може се видети из података да 63% поседује свој смарт телефон или телефон са андроид платформама, 59% мобилни телефон, 54% свој компјутер (УНИЦЕФ, 2016: 17). Када се упореди са резултатима ранијег истраживања, приметно је мање присуство мобилних телефона и компјутера међу лицима поменуте старосне доби. Ово се може објаснити тиме да се претходно истраживање односило само на градску популацију, док је истраживање из 2016. године обухватило репрезентативан узорак, дакле и рурално и субурбано становништво. Са друге стране, ако се узме у обзир да смарт телефони садрже могућност мобилног приступа интернету, испада да је доступност интернета већа него што је била по резултатима претходног истраживања. Већина проводи више од сат времена дневно *online*, број сати расте са узрастом, а садржаји који привлаче пажњу деце, према мишљењу њихових родитеља, су претежно забавног карактера, попут играња игрица и комуникације на друштвеним мрежама, која постаје значајна преокупација деце, већ на узрасту од дванаест година, док се од четрнаесте до седамнаесте године ради се о свакодневној активности за 70% деце која имају приступ интернету (УНИЦЕФ, 2016: 21-23). Посебна пажња у оквирима овог истраживања посвећена је питању шта највише забрињава родитеље у вези са употребом интернета од стране деце, а овај сегмент истраживања открио је да се на врху листе налази управо бојазан од контакта са непознатим људима на друштвеним мрежама. Ради добијања прецизније слике у наставку је, посматрано очима родитеља, дат преглед опасности: успостављање контакта са непознатим људима (38,7%), излагање штетним садржајима (16,4%), малтретирање или узнемиравање преко интернета (13%), сексуално узнемиравање, сексуално злостављање и сексуално завођење (12,8%), крађа или злоупотреба личних података и информација (12,8%), излагање сексуалним или порнографским садржајима (12,4%), трговина децом и кријумчарење (7,8%), излагање штетним саветима и предлозима (7,6%), сусрети са лицима које су упознали преко интернета (4,7%), крађа новца (4,1%), навођење на наркотике, алохол, криминал (3,8%), лош утицај на здравље због некретања, кварења вида, стварања асоцијалности (3,1%), зависност од интернета (2,8%), лажни профили на друштвеним мрежама (1%), вршњачко насиље

(1%), вируси или хаковање (1%) и друго (5,8%, УНИЦЕФ, 2016: 30). Присутна је и традиционална визура, јер су родитељи женске деце много више били забринути због могућег контакта са непознатима и могућности сексуалне злоупотребе, него родитељи дечака (УНИЦЕФ, 2016: 31). Занимљиво је да су истраживачи утврдили да упркос томе што родитељи препознају потенцијалне ризике, истовремено оцењују и да њихова деца нису директно угрожена, при чему су више поуздања у том погледу показивали родитељи вишег нивоа образовања од родитеља који су мање образовани (УНИЦЕФ, 2016: 33-34). Надаље, предмет истраживања је представљало и учешће родитеља у интернет активностима детета, која је дистрибуирана на следећи начин: разговор са дететом о томе шта ради на интернету (93,2%), остајање у близини када дете користи интернет (75%), гледање шта дете ради, али без укључивања (70,9%), подстицање да само истражује и учи на интернету (62,7%), заједничке активности са дететом (52,6%, УНИЦЕФ, 2016: 34). Комуникација о интернет ризицима се интензивира око девете, а опада после петнаесте године, интензивнија је са децом женског пола и од стране родитеља који имају виши образовни ниво (УНИЦЕФ, 2016: 34). Занимљива је и самопроцена способности да помогну детету у случају проблема у дигиталном окружењу, тј. колико добро познају интернет и начине његовог коришћења: веома добро (17%), углавном (46,3%), не превише (31,2%), нимало (5,5%, УНИЦЕФ, 2016: 41). Међутим, када је требало навести конкретан облик контроле понашања деце на интернету, већина родитеља је навела најпростије могуће активности: праћење историје на уређају са којег дете приступа уређају, прегледање профила и контаката на друштвеним мрежама, прегледање порука на мобилном телефону, а мање инсталирање софтверских забрана и ограничења на интернет претраживачима на рачунару или мобилном уређају (32,2%) или уговор са провајдером о који ограничава време на интернету (18,2%, УНИЦЕФ, 2016: 42).

3. Кривично дело искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу – законодавство и пракса у Републици Србији

Кривично дело искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (чл. 185б Кривичног законика Републике Србије, у даљем тексту КЗРС)[4] постало је део нашег кривичноправног си-

[4] *Службени гласник РС, бр. 85/05, 88/05-испр., 107/05-испр., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 и 35/19*.

стема на основу ратификације Конвенције Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања (у даљем тексту Конвенција).[5] Међу осталим обавезама, наша земља је прихватила и да инкриминише одређена понашања (чл. 18-23 Конвенције), укључујући и тзв. наговарање деце у сексуалне сврхе (чл. 23 Конвенције).[6] У том смислу, било је потребно предвидети као кривично дело „предлог састанка који одрасло лице са намером упути, користећи информациону и комуникациону технологију, детету које још није досегло узраст наведен у примени члана 18 став 2,[7] ради извршења било ког дела одређеног у складу са чл. 18 став 1а или чланом 20 став 1а, против њега или ње, ако је тај предлог пропраћен и материјалним радњама које воде ка одржавању таквог састанка". Новоуведено дело је очигледно понело други назив у КЗРС, што се може оправдати тиме да превод термина *solicitation*, коришћеног у енглеском тексту Конвенције, као „наговарање" није баш најсрећније изабран, пошто он у домену сексуалне делинквенције означава нешто више од простог наговарања и представља намаљивање, па чак и салетање (указано у Стојановић, 2018: 600). Са друге стране, можда би се могло приговорити и да је изабрано „искоришћавање" превише неутрално и помало „безбојно" у овом контексту, да не одсликава суштину која се огледа у злоупотреби савремених средстава комуникације у циљу манипулације малолетним лицима, а не у некој уобичајној употреби, иако је несумњиво боље од термина наговарање.

У основном облику кривично дело из КЗРС чини лице које, у намери извршења одређених кривичних дела против полне слободе, користећи рачунарску мрежу или комуникацију другим техничким средствима, договори састанак са малолетником и појави се на договореном месту ради састанка. Како је дело сврстано у групу кривичних дела против полне слободе, полна слобода представља објекат заштите.

Радња кривичног дела искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу одређена је двоактно, тако да је за његово постојање неопходно да је извршилац договорио састанак са малолетником и да се појавио на договореном месту ради састанка. То значи да је за његово извршење потребно више услова, а не само то да је са малолетником постигнута сагласност око виђења, већ и да се учинилац

[5] *Службени гласник РС – Међународни уговори, бр. 1/10.*

[6] Више о другим инкриминацијама у Миладиновић-Стефановић, 2014: 568-570.

[7] Старосни узраст испод којег је забрањено бављење сексуалним активностима са дететом, при чему Конвенција под појмом дете подразумева лице млађе од 18 година (чл. 3).

физички појавио на уговореном месту, и то у циљу одржавања уговореног састанка. У супротном, уколико учинилац уопште није дошао на састанак, или се појавио али са неким другим циљем, на пример да би боље осмотрио малолетника, да би га фотографисао или направио видео снимак, или можда проверио да ли се он креће у пратњи старијих и слично, што није неосновано очекивати због предострожности и лукавости сексуалних предатора, дело ће остати у покушају.[8] Када се радња дела из КЗРС упореди са радњом из Конвенције, приметне су извесне неподударности. Наиме, Конвенција инсистира на томе да је предлог састанка пропраћен и „материјалним радњама које воде ка одржавању таквог састанка", што се не може у потпуности поистоветити са појављивањем на месту састанка. Појам „материјалних радњи" је очигледно шири. Чињеница је да долазак на место састанка може представљати материјалну радњу о којој се овде говори, али се њихов круг тиме не затвара. Шта ако је изнајмљен стан, резервисана хотелска соба или ако је предузета нека друга, у суштини, припремна активност са циљем одржавања истог? По Конвенцији би и наведено било кажњиво, али не и по КЗРС. То значи да је кажњива зона из Конвенције шира у односу на ону постављену домаћим законодавством, чиме се отвара проблем испуњавања међународних обавеза и усаглашености са Конвенцијом, али и проблем адекватне заштите малолетних лица.

Такође, у оквиру излагања о радњи требало би се осврнути и на извесно несагласје које постоји између ње и назива овог кривичног дела. Судећи само по називу „*искоришћавање* рачунарске мреже или комуникације другим техничким средствима" требало би да се ради о инкриминацији чија радња представља вишекратно деловање, деловање које се понавља. Међутим, такав закључак је погрешан, пошто радњу, управо супротно, чине једнократне активности – „*договори* састанак са малолетником" и „*појави* се на договореном месту ради састанка". Занимљиво је да се слична неподударност јавља и у Конвенцији између назива „наговарање" и радње „упути предлог". Иако би се назив могао усагласити са радњом, ово и није толико нужно, пошто је за постојање дела битна радња, тако да ће одговорност постојати уколико је само једном постигнута сагласност око састанка, уз додатни услов да се учинилац само једном појавио на договореном месту.

Од објективних елемената требало би поменути и коришћење одређеног средства, тј. рачунарске мреже или неког другог техничког средства за успостављање контакта са малолетником. Појам рачунарске мреже дат је аутентичним тумачењем – скуп међусобно повезаних рачунара односно рачунарских система, који комуницирају размењујући податке (чл.

[8] Требало би поменути да је покушај у овом случају кажњив, с обзиром на прописану казну (казна затвора од шест месеци до пет година и новчана казна).

112 ст. 18 КЗРС). Овде се поставља питање шта би се све могло сматрати другим техничким средством комуникације. Иако је комуникацију могуће остварити на веома различите начине, највероватније је у пракси очекивати телефон или мобилни телефон, по некима изузетно и радио, а мало вероватно нека друга средства (Стојановић, 2018: 601). То значи да је санкционисан само тзв. *online grooming*, али не и *grooming* остварен у непосредном контакту са жртвом, преко трећег лица као посредника или слањем класичне (неелектронске) поште, што је остало изван домета наше инкриминације. У овом домену законодавац је очигледно настојао да стриктно прати захтеве Конвенције, која се фокусирала само на овај најопаснији вид *grooming-a.*

Са друге стране, субјективни супстрат дела представља одређена намера – намера извршења одређених кривичних дела против полне слободе. Она мора да постоји у време извршења дела, а уколико би се десило да се састанак уговара са неком другом намером, која се не односи на вршење набројаних дела, тада кривично дело искоришћавање рачунарске мреже или комуникације другим техничким средствима не би постојало. Пошто представља елемент бића кривичног дела, намера мора бити и доказана, односно о њој се не може аутоматски доносити закључак на основу саме чињенице уговарања састанка и појављивања на истом. Готово да и не треба указивати на тешкоће које се могу појавити приликом доказивања намере, јер је потпуно јасно да је учинилац неће открити малолетнику, већ ће се позивати на неке друге, тобожње разлоге за састајање.

Раније је речено да се намера односи на извршење одређених дела против полне слободе, а прецизније ради се о следећим делима: силовање (чл. 178 ст. 4),[9] обљуба над немоћним лицем (чл. 179 ст. 3),[10] обљуба са дететом (чл. 180 ст. 1 и 2),[11] обљуба злоупотребом положаја (чл. 181 ст. 2 и 3),[12] недозвољене полне радње (чл. 182 ст. 1),[13] подвођење и омогућавање вр-

[9] Квалификовани облик учињен према детету.

[10] Исто.

[11] У основном облику и у квалификованом облику када је наступила тешка телесна повреда детета, када је дело за последицу имало трудноћу или када је извршено од више лица.

[12] Када је дело учинио наставник, васпитач, старалац, усвојилац, родитељ, очух, маћеха или друго лице које злоупотребљава свој положај или овлашћење за извршење обљубе или са њом изједначеног чина са малолетником који му је поверен ради учења, васпитања, старања или неге, односно када је дело учињено према детету.

[13] Извршене силом или претњом да ће се непосредно напасти на живот или тело тог или њему блиског лица; или претњом да ће се за то или њему блиско лице изнети нешто што може да шкоди његовој части и угледу или претњом другим тежим злом;

шења полног односа (чл. 183 ст. 2),[14] посредовање у вршењу проституције (чл. 184 ст. 3),[15] приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (чл. 185 ст. 2)[16] и навођење детета на присуствовање полним радњама (чл. 185а). У набрајању дела законодавац је очигледно начинио омашку, помињући посредовање у вршењу проституције из чл. 184 ст. 3 које уопште не постоји, иако ово дело има квалификовани облик уколико је учињено према малолетном лицу у ст. 2 (Стојановић, 2017: 601). Занимљиво је да од 2009. године до данас, мада је КЗРС у више наврата новелиран, ово никада није исправљено.

Говорећи о делима обухваћеним намером, требало би поменути да се заправо ради о свим инкриминацијама против полне слободе из КЗРС осим полног узнемиравања (чл. 182а). Како Конвенција наговарање деце у сексуалне сврхе доводи у везу само са сексуалним злостављањем (чл. 18 ст. 1а) и дечијом порнографијом (чл. 20 ст.1а), али не и са другим делима, евидентно је да је наш законодавац проширио листу дела обухваћених намером. Дакле, само искључење полног узнемиравања јесте у складу са Конвенцијом, док проширење у односу на остала дела (која не представљају пандан делима из чл. 18 ст. 1а и чл. 20 ст. 1а Конвенције) није било неопходно са аспекта испуњења међународних обавеза, мада се може оправдати потребом шире заштите малолетних лица. Принципијелно посматрано, када се већ определио да оде даље од оног што Конвенција тражи, поставља се питање зашто је на листу уврстио нека дела која су по прописаној казни лакша од полног узнемиравања, као што је случај са недозвољеним полним радњама, а изоставио само полно узнемиравање.[17]

или искоришћавањем душевног обољења, заосталог душевног развоја, друге душевне поремећености, немоћи или каквог другог стања лица услед којег оно није способно за отпор; или злоупотребом положаја у односу на лице које се према учиниоцу налази у стању какве подређености или зависности; или када дело чини наставник, васпитач, старалац, усвојилац, родитељ, очух, маћеха или друго лице које злоупотребљава свој положај или овлашћење за извршење обљубе или са њом изједначеног чина са малолетником који му је поверен ради учења, васпитања, старања или неге, односно када је дело учињено према детету.

[14] Ако се омогућава обљуба, са њом изједначен чин или нека друга полна радња према малолетном лицу.

[15] Овај став не постоји у КЗРС.

[16] Ако је малолетник искоришћен за производњу слика, аудио-визуелних или других предмета порнографске садржине или за порнографску представу.

[17] За недозвољене полне радње из чл. 182 ст. 1 прописана је новчана казна алтернативно са казном затвора до три године, док је за полно узнемиравање када је жртва малолетник предвиђена казна затвора од три месеца до три године.

Надаље, пажљива анализа побројаних дела открива да се она у знатној мери односе на квалификоване облике учињене према детету. То је нелогично, јер испада да извршилац основног облика дела из чл. 185б КЗРС договара састанак са *малолетником* у намери да према њему изврши неко од назначених дела против полне слободе, при чему је за постојање већине тих дела потребно да се у улози пасивног субјекта не појављује малолетник већ *дете*. Како ово реално није могуће, поставља се питање због чега се није технички боље поступило при набрајању дела. Мада није оправдање, чини се да забуна може да настане отуда што се појам дете не одређује исто у нашем праву и у Конвенцији. Док је по КЗРС дете лице које није навршило четрнаест година (чл. 112 ст. 8), по аутентичном тумачењу датом у Конвенцији у питању је свако лице млађе од осамнаест година (чл. 3). Тако се под дететом из Конвенције, када се преведе на језик нашег права, подразумева лице које није пунолетно. Истини за вољу, приликом дефинисања дела „наговарање деце у сексуалне сврхе" Конвенцијом је прецизирано да је пасивни субјект овог дела „дете које није досегло узраст наведен у примени члана 18 став 2", што значи старосни узраст од којег је дозвољено бављење сексуалним активностима са таквим лицем. Како се наш законодавац определио за четрнаест година као за просечно старосно доба у којем већина досеже полну зрелост, а стриктно пратећи оно што је наведено у Конвенцији, требало је прописати да дело постоји само ако се као пасивни субјект јавља лице које није навршило четрнаест година (Стојановић, 2017: 601), са којима постоји апсолутна забрана ступања у сексуалне односе.

Што се активног субјекта тиче, очигледно је на основу језичког тумачења да у КЗРС то може бити било које лице, пошто он ни на који начин није ближе одређен, ни по полу, ни по узрасту нити по било каквој другој карактеристици. Ту лежи још једна разлика у односу на Конвенцију, у којој је ово питање другачије решено. Превод Конвенције говори о „одраслом лицу" (оригинални енглески текст „adult"), док је у инкриминацији у КЗРС овај атрибут активног субјекта потпуно изостављен, чиме се изгубио и смисао који би ова инкриминација требало да има, а то је заштита малолетних лица која нису досегла одређени узраст од сексуалне злоупотребе пунолетних лица. То значи да, теоријски посматрано, ово дело код нас може да учини и малолетник према другом малолетнику. Нема сумње да су такве ситуације реално могуће и да се може пронаћи неко оправдање за реакцију и на малолетне учиниоце овог дела, посебно ако постоји значајнија разлика у душевној и телесној зрелости између њих и жртве. Међутим, у самој Конвенцији је наглашено да инкриминације немају за циљ уређивање сексуалних активности међу малолетницима које се одвијају уз обострани пристанак (чл. 18 ст. 3).

Поред основног, кривично дело из КЗРС има и тежи облик, који настаје ако је пасивни субјект дете. За основни облик прописана је кумулативно казна затвора од шест месеци до пет година и новчана казна, а за квалификовани казна затвора од једне до осам година.

Већ приликом његовог увођења, у домаћој теорији је изражена сумња да се ово дело неће често јављати у пракси (Лазаревић, 2011: 642). Десетогодишњи период, протекао од његовог увођења, сада је већ дао за право ауторима који су заузели поменути скептични став. Прецизније речено, у периоду од 2010. до 2019. године[18] донете су само четири осуђујуће пресуде за ово кривично дело (које се односе на пунолетне учиниоце, прим. аут.), тако да још увек недостаје емпиријски материјал за неку значајнију анализу, што се може видети из табеле која следи.

година	укупан број осуда	осуде за дела против полне слободе	осуде за дело из чл. 185б	санкције за дело из чл. 185б
2010.	21681	164	0	-
2011.	30807	190	0	-
2012.	31322	244	0	-
2013.	32241	236	0	-
2014.	35376	242	0	-
2015.	33189	174	1	кућни затвор
2016.	32525	204	1[19]	кућни затвор
2017.	31759	189	1	условна осуда
2018.	29750	188	1	кућни затвор
2019.	28112	251	0	-

Са друге стране, у посматраном периоду од 2010. до 2019. године, ниједан малолетник није осуђен за искоришћавање рачунарске мреже или комуникације другим техничким средствима, није забележена ниједна кривична пријава, мада би се и они, с обзиром на то како је дело нормативно уобличено код нас, могли појавити као извршиоци.[20]

[18] У време настанка рада (јануар 2021. године) још увек нису били прикупљени и обрађени подаци за 2020. годину (прим. аут.). Сви подаци потичу из билтена Републичког завода за статистику *Пунолетни учиниоци кривичних дела у Републици Србији – пријаве, оптужења, осуде*, за период од 2010. до 2019. године, преузетих са https://www.stat.gov.rs/oblasti/pravosudje/, приступ 20.01.2021.

[19] Осуда за покушано дело.

[20] На основу података из билтена Републичког завода за статистику *Малолетни учиниоци кривичних дела у Републици Србији – пријаве, оптужења, осуде*, за период од 2010. до 2019. године, преузетих са https://www.stat.gov.rs/oblasti/pravosudje/, приступ 20.01.2021.

Иако је већ наведена ограда да се ради о премалом броју пресуда да би се могли извлачити неки релевантнији закључци, у теоријском смислу могли би се понудити одређени одговори због чега је то тако. Наиме, различита истраживања о сексуалној злоупотреби малолетника код нас показују да је учинилац од раније познат малолетнику пре извршења дела, јер се ради о особама из његовог блиског круга, попут чланова породице, породичних пријатеља, или лица којима је поверен у циљу образовања и васпитања, тако да врбовање преко информационо-комуникационих технологија за већину учинилаца уопште и није неопходно да би успоставили контакт (Петковић, Ђорђевић, Балос, 2010: 312). Ова инкриминација сигурно има већи значај у оним срединама где преовлађује другачији тип учинилаца, тзв. опасни странац (*stranger danger*), који нужно мора да има и другачији приступ потенцијалним жртвама.

Друго могуће објашњење почива на претпоставци да се ради о делу са високом тамном бројком, тако да је оно реално много учесталије него што се то може видети из било које званичне статистике. У теорији је присутан став да је генерално веома тешко проценити стварне размере сексуалне злоупотребе малолетних лица. Постоји много разлога за то: механизам инфантилне амнезије, услед којег се потискују догађаји из раног детињства укључујући и могућу виктимизацију, ограничене могућности детета (посебно у млађем узрасту) да схвати праву природу сексуалних радњи, различите манипулативне технике учиниоца, почевши од тога да неприхватљиво понашање представља као игру, исказивање љубави, до развијања осећаја кривице због наводног провоцирања и саучествовања у чину, па чак и отвореног уцењивања и застрашивања жртве. Томе треба додати и да некада други чланови породице уместо помоћи и подршке реагују негирањем проблема, као и то да се неки видови сексуалне злоупотребе остварују без примене физичког насиља, чак и бесконтактно, те не остављају видљиве трагове и бивају потпуно нерегистровани. У једном новијем истраживању спроведеном код нас показало се да у Србији међу школском популацијом узраста од 10 до 18 година у сваком одељењу постоји њих четворо који су преживели неки облик сексуалног насиља, као и њих четворо који су изјавили да знају да се тако нешто догодило другоме (Прва национална студија о друштвеном проблему сексуалног злостављања деце у Републици Србији, 2015: 7). Посебно је поражавајуће то што је утврђено да је само у 7% случајева дошло до пријаве надлежним државним органима, као и то што је у процесу истраживања 62,1% злостављане деце одбило да било како означи учиниоца. Оно што би у овом контексту могло бити значајно јесте и податак о средини у којој се

одиграва злоупотреба, јер су испитаници на друго место ставили управо друштвене мреже (22%), одмах после куће као места дешавања (32%).[21]

Што се казнене политике тиче, може се констатовати да су се домаћи судови у свим случајевима опредељивали за неки вид алтернативног реаговања. Без увида у списе предмета веома је незахвално процењивати да ли је то оправдано или не. Међутим, с обзиром на услове постављене за изрицање кућног затвора[22] и условне осуде[23] могућа је компарација са казном прописаном у чл. 185б, која потврђује „правило" да се судови приликом изрицања казне углавном крећу у првој половини, па чак и првој трећини прописаног казненог распона (више у Миладиновић-Стефановић, 2014: 571).

Такође, општи статистички подаци не показују ни то да ли су коришћени и институти из Закона о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима.[24] У одређивању подручја примене овог Закона изричито је наведено и предметно дело (видети чл. 3), што значи да је у односу на њега искључена примена института ублажавања казне, условног отпуста и застарелост кривичног гоњења и извршења кривичних санкција (чл. 5), а обавезно је наступање одређених правних последица осуде (чл. 6).[25] Поред тога, по издржавању казне затвора обавезно је и спровођење посебних мера (чл. 7),[26] као и увођење

[21] Више о томе у Прва национална студија о друштвеном проблему сексуалног злостављања деце у Републици Србији, 2015: 8.

[22] Ако учиниоцу кривичног дела суд изрекне казну затвора до једне године он истовремено може одредити и да ће се она извршити тако што ће је осуђени издржати у просторијама у којима станује, ако с обзиром на личност учиниоца, његов ранији живот, држање после учињеног дела, степен кривице и друге околности под којима је дело учињено може очекивати да ће се на тај начин остварити сврха кажњавања (чл. 45 ст. 3 КЗРС).

[23] Условна осуда се може изрећи када је учиниоцу утврђена казна затвора у трајању мањем од две године (чл. 66 ст. 1), али се не може изрећи за кривична дела за која се може изрећи казна затвора у трајању од осам година или тежа казна (чл. 66 ст. 2 КЗРС), док је раније, тј. пре измена и допуна из 2019. године та граница била одређена на десет година (прим.аут.).

[24] *Службени гласник РС, бр. 32/13*.

[25] Престанак вршења јавне функције; престанак радног односа односно престанак вршења позива или занимања које се односи на рад са малолетним лицима; забрана стицања јавних функција и забрана заснивања радног односа односно обављања позива или занимања које се односи на рад са малолетним лицима.

[26] Обавезно јављање надлежном органу полиције и Управе за извршење кривичних санкција; забрана посећивања места на којима се окупљају малолетна лица (вртићи, школе и сл.); обавезно посећивање професионалних саветовалишта и установа;

учинилаца ових дела у посебну евиденцију (чл. 13).[27] Занимљиво је да се међу санкцијама и мерама предвиђеним у нашем законодавству не налази ниједна која би посебно погодила учиниоце који су злоупотребили савремене информационо-комуникационе технологије, какве су пристутне у компаративном праву.[28]

4. Закључне напомене

Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу представља значајну новину у нашем кривичном законодавству. Иако је унето извршавањем прихваћених међународних обавеза ово дело, како је показано, има и одређено криминално-политичко оправдање, што се не може рећи баш за све инкриминације које су истим путем „ушле" у наш правни систем. Сигурно је да искоришћавање као деликт запреке има смисла и да би требало да одигра своју улогу „бране" за вршење озбиљнијих, тежих дела против полне слободе. Претходна анализа је показала да оно до сада није „прорадило", тако да би се за праксу могла формулисати препорука да се у поступцима за остала дела против полне слободе више поведе рачуна о дешавањима пре извршења, о механизму припремања дела, не би ли се утврдило да ли постоје и елементи искоришћавања рачунарске мреже или комуникације другим техничким средствима. Доступност савремених технологија у овом домену, као и навике малолетних лица приликом њиховог коришћења, говоре у прилог тези да је дело вероватно много учесталије у стварности него што се то може видети из судске статистике. Са друге стране, постоје и препоруке за законодавца, како су уочене могућности за измене на различитим нивоима. Најслабије стране дела представљају радња извршења, коју треба редефинисати, јер је у нашем праву постављена уже у односу на Конвенцију, као и активни субјект, пошто би у том својству требало да се појављује само пунолетно лице. Пасивни субјект би, стриктно следећи Конвенцију, требало да буде лице које није навршило 14 година, мада је шире посматрано, због обавеза из Конвенције УН о правима детета[29] и из криминал-

обавезно обавештавање о промени пребивалишта, боравишта или радног места; и обавезно обавештавање о путу у иностранство. Детаљно о овим мерама у Миладиновић-Стефановић, 2013: 377-392.

[27] Више о томе у Миладиновић-Стефановић, 2014: 447-462.

[28] Попут мере забране приступа интернету. Више о томе у Cvitanić, Glavić, 2012: 891-916.

[29] Закон о ратификацији Конвенције Уједињених нација о правима детета, *Службени лист СФРЈ – Међународни уговори, бр. 15/90 и Службени лист СРЈ – Међународни уговори, бр. 4/96 и 2/97*.

но-политичких разлога потребно задржати постојеће решење. Надаље, листу дела обухваћених намером треба средити у номотехничком смислу, а посебно исправити омашку учињену у вези са посредовањем у вршењу проституције.

Литература

Benson M. (1988). *Englesko-srpskohrvatski rečnik, drugo, izmenjeno i dopunjeno izdanje*. Beograd: Prosveta

Berliner L. (2018). The Concept of Grooming and How It Can Help Victims. *Journal of Interpersonal Violence*. 33 (1). 24-27.

Burges A. W., Hartman C. R. (2018). On the Origin of Grooming. *Journal of Interpersonal Violence*. 33 (1). 17-23.

Ezioni L. (2020). The Crime of Grooming. *Child and Family Law Journal*. 8 (1). 1-18.

Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима. *Службени гласник РС*. Бр. 32/13.

Закон о потврђивању Конвенције Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања. *Службени гласник РС – Међународни уговори*. Бр. 1/10.

Закон о ратификацији Конвенције Уједињених нација о правима детета. *Службени лист СФРЈ – Међународни уговори.* Бр. 15/90*. Службени лист СРЈ – Међународни уговори.* Бр. 4/96 и 2/97.

Кривични законик Републике Србије. *Службени гласник РС*. Бр. 85/05, 88/05-испр., 107/05-испр., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 и 35/19.

Лазеревић Љ. (2011). *Коментар Кривичног законика, друго, измењено и допуњено издање*. Београд: Правни факултет Универзитета Унион

Martellozzo E. (2017). Online Sexual Grooming – Children as Victims of Online Abuse. *In Cybercrime and its Victims (eds. E. Martellozzo, E. A. Jane), pp. 108-128*. Routledge: Taylor&Frances

Миладиновић-Стефановић Д. (2014). Кривичноправна заштита малолетника од сексуалног искоришћавања и злостављања – европски стандарди и право Републике Србије. *Зборник радова Правног факултета у Нишу*. 68. 567-584.

Миладиновић-Стефановић Д. (2014). Одмеравање казне и прописани казнени распони у Кривичном законику Србије. *У Оптужење и други кривичноправни инструменти државне реакције на криминалитет, LIV редовно*

годишње саветовање удружења (ур. С. Бејатовић), стр. 557-574. Београд-Златибор: Српско удружење за кривичноправну теорију и праксу

Миладиновић-Стефановић Д. (2014). Посебна евиденција учинилаца кривичних дела против полне слободе према малолетним лицима. *У Усклађивање права Србије са правом ЕУ: тематски зборник (ур. М. Лазић), стр. 447-462*. Ниш: Правни факултет

Миладиновић-Стефановић Д. (2013). Посебне мере за спречавање кривичних дела против полне слободе према малолетним лицима. *У Заштита људских и мањинских права у европском правном простору: тематски зборник радова (ур. П. Димитријевић), стр. 377-393*. Ниш: Правни факултет

Петковић Н., Ђорђевић М., Балос В. (2010). Анализа ставова јавности у Србији према феномену сексуалне злоупотребе деце. *Темид*а. 4 (13). 61-82.

Попадић Д., Кузмановић Д. (2013). *Коришћење дигиталне технологије, ризици и заступљеност дигиталног насиља међу ученицима у Србији*. Београд: Министарство просвете, науке и технолошког развоја, УНИЦЕФ

Прва национална студија о друштвеном проблему сексуалног злостављања деце у Републици Србији. (2015). Београд: Инцест траума центар

Републички завод за статистику. (2020). *Употреба информационо-комуникационих технологија у Републици Србији, 2020*. Београд: Републички завод за статистику

Стојановић З. (2017). *Коментар Кривичног законика, шесто, измењено и допуњено издање*. Београд: Службени гласник

УНИЦЕФ. (2016). *Истраживање о нивоу свести о потенцијалним интернет ризицима и злоупотребама међу родитељима деце узраста од 8 до 17 година*. Београд, https://www.unicef.org/serbia/sites/unicef.org.serbia/files/2018-08/Istrazivanje_o_nivou_svesti_roditelja_o_rizicima_od_zloupotrebe_dece_na_internetu.pdf, приступ 27.01.2021.

http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx, приступ 20.01.2021.

https://www.stat.gov.rs/oblasti/pravosudje/, приступ 20.01.2021.

Craven S., Bowen S., Gilchrist E. (2006). Sexual Grooming of Children: Review of Literature and Theoretical Considerations. *Journal of Sexual Aggression*. 12 (3). 287-299.

Cvitanić L., Glavić I. (2012). Uz problematiku sigurnosne mjere zabrane pristupa internetu. *Hrvatski ljetopis za kazneno pravo i praksu*. 19 (2). 891-916.

Winters G. M., Jeglic E. L. (2017). Stages of Sexual Grooming: Recognizing Potentially Predatory Behaviors of Child Molseters. *Deviant Behavior*. 38 (6).724-733.

Winters G. M., Kaylor, L. E., Jeglic E. L. (2016). Sexual Offenders Contacting Children Onlline: An Examination of Transcripts of Sexual Grooming. *Journal of Sexual Aggression*. 1-15.

Wood A. C., Wheatcroft J. M. (2020). Young Adult Perceptions of Internet Communications and Grooming Concept. *Sage Open*. 10 (1). 1-12.

Dušica Miladinović-Stefanović, LL.D.,
Associate Professor,
Faculty of Law, University of Niš
Serbia

ABUSE OF COMPUTER NETWORKS OR OTHER TECHNICAL COMMUNICATION MEANS FOR COMMITTING SEX CRIMES AGAINST MINORS

Summary

The development of information and communication technologies (ICT), their prevalence and wide availability have led to significant changes in contacting and communicating with other people. In addition to the indisputable advantages of technology, which has enabled us to rapidly, easily and instantly exchange information with a person on the other side of the world and thus overcome huge spatial distances by a single "mouse-click", the use of technology has given rise to various abuses and new security challenges. As a vulnerable group, minors seem to be especially endangered. In spite of the fact that they were born in the "digital world" which they sometimes understand much better than adults, minors are not always aware of the risks lurking in the digital environment. Although minors can be victimized by using different means of communication, the research within this paper focuses on the so-called online grooming, which entails contacting and preparing a potential victim for sexual abuse. In that context, special attention is given to the analysis of the legal provision in Article 185b of the Criminal Code of the Republic of Serbia, on the abuse of computer networks or other technical communication means for committing sex offences against juveniles, which is a legal response to this phenomenon. In this paper, the author explores whether this provision is in compliance with the requirements set out in the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, with specific reference to Serbian judicial practice. The author discusses the significance of this provision in view of criminal policy and its prospective development de lege ferenda.

Keywords: *abuse of computer networks, technical communication means, sex crimes against minors, Serbian Criminal Code.*

Др Бојан Милисављевић
Редовни професор,
Правни факултет Универзитета у Београду,
Србија

UDK: 351.853:355.4
7.025:355.4

ЗАШТИТА КУЛТУРНИХ ДОБАРА У ОРУЖАНИМ СУКОБИМА

Апстракт*: Рад анализира заштиту различитих облика културних добара у време оружаних сукоба. Напочетку рада указује се на значај ове заштите, дефинише само културно добро и даје увод у смислу негативних примера уништења културних добара и развијања првих правила о забрани такве активности. Аутор излаже у раду да се свест о забрани таквих активности јавила јако давно, али да смо и у новије време сведоци уништавања културних добара. У чланку се анализира развој правне забране оштећења и уништења културних добара почев од унутрашњих прописа, преко Хашког права, па до Конвенције о заштити културних добара Уједињених нација.*

Аутор нарочито истиче значај рада међународне организације УНЕСКО, али и усвајање два допунска Протокола на поменуту конвенцију. Поред ових аката аутор истиче значај и дугих правних извора из ове области, како на универзалном, тако и на регионалном плану. На крају у раду се указује на неке основне мањкавости постојећег система заштите културних добара у потпуно измењеним околностима терористичких аката и унутрашњих сукоба и предлаже конкретне мере за унапређење њихове заштите у времену које нам предстоји. Нарочито се указује на потребу организовања међународне заједнице у погледу враћања украдених културних добара након оружаних сукоба и износе се позитивни примери из праксе у том погледу.

Кључне речи: *заштита културних добара, оружани сукоби, теорирстички акти.*

1. Уводна разматрања

Одувек су се постављали захтеви за посебном заштитом културних добара у време оружаних сукоба, било да се ради о покретним(слике, иконе, кипови...) или непокретним (грађевине, храмови...) културним добрима.

Културна добра су нарочито угрожена током оружаних сукоба и у сваком случају морају бити заштићена од уништавања, оштећења, као и продаје. Током ратова кроз историју често је долазило до намерног уништавања културних добара и културне баштине јер су вођени тотални ратови за уништење непријатеља, а често и окупације и анексије.[1] У таквим околностима непријатељ је желео да уништи све што подсећа на предходну власт или цивилизацију како би се наметнуо као нови суверен. Тако је 146 године п.н.е. дошло до потпуног уништења Картагине од стране римске војске, али и пљачке Херодотовог храма у Јерусалиму 70 године п.н.е.[2]

На жалост на овај начин долазило је до неповратног уништења културне баштине читаве цивилизације. Како је сазревала свест о потреби да се оружани сукоби ограниче тако је долазило и до развоја правила о потреби заштите културних добара. Временом се културна добра не везују само за државу одакле потичу већ се сматрају заједничком баштином читавог човечанства. Тако је још Вател стао у заштиту културних добара и значајних грађевина пишући да је допуштено уништење војних објеката, али да културне творевине никако није.[3] Прве правне трагове заштите културних добара налазимо у значајном Либеровом кодексу где се они штите кроз заштиту приватне имовине. Тако он предвиђа да имовина цркава, добротворних установа и музеја мора бити изузета из конфискације и поштована као и приватна имовина.[4] У наставку су приликом усвајања Хашких конвенција 1907. године у посебном Правилнику заштићена и културна добра на следећи начин: Приликом опсада и бомбардовања градова морају се предузети све мере да се поштеде, колико је то могуће, зграде посвећене верским обредима, уметности, науци и добротворним сврхама, историјски споменици, болнице под условом да нису у исто време употребљени у војне сврхе.[5] Дакле овде се не ради о апсолутној заштити културних добара него је она ограничена војном потребом, па уколико се користи у војне сврхе и доноси значајну корист нападачу онда могу бити уништени или оштећени. У наставку истог акта посебно је занимљива конструкција која је изведена: „Имовина општина, као и институција посвећених религији,

[1] За више погледати: Erika Techera, Protection of Cultural Heritage in Times of Armed Conflict: The International Legal Framework Revisited, MqJICEL (2007) Vol 4, Joshua E Kastenberg, USAF 'The Legal Regime for Protecting Cultural Property during Armed Conflict' (1997) 42 Air Force Law Review;

[2] J. Johnson, Under the new management; the obligation to protect cultural property during military occupation, Military law review, 190/191, 2006/2007, 115

[3] E. De Vattel, The Law of Nations, Philadelphia 1852, 294-295

[4] J. Johnson, op.cit., 119;

[5] Члан 27 Правилника о законима и обичајима рата на копну;

добротворним установама и образовању, уметности и науци, чак и када је државна, третираће се као приватна својина. Свако одузимање, уништавање или намерно оштећење институција овог карактера, историјских споменика, уметничких дела и науке, забрањено је и требало би да буду предмет правног поступка."[6] Интересантно је што се у овој норми успоставља фикција да је јавна имовина у ствари приватна да би се она боље заштитила и на тај начин изузела од правног режима државне имовине која у начелу може бити предмет присвајања или евентуално уништавања у току оружаних дејстава.

Између два светска рата појавила се потреба за регулисањем додатне заштите различитих објеката укључујући и културне објекте услед коришћења ваздухоплова у војне сврхе. Тако је формирана посебна Комисија правника на Вашингтонској конференцији 1922. године са задатком да припреми нацрт правила о ваздушном рату. У овом нацрту предвиђено је да бомбардовање из ваздуха може бити усмерено само на војне објекте, а да никако предмет бомбардовања не смеју бити насељена места, градови, села, стамбени објекти и културно – историјски споменици под условом да нису намењени за војне потребе.[7] Као један од важних корака у креирању посебних правни правила у погледу заштите културних добара може се навести нацрт правила које је настало у оквиру Друштва народа 1938. године под називом Конвенција о заштити историјских споменика и културних дела у време рата. Овај акт је остао само на нивоу нацрта јер је врло брзо дошло до отпочињања Другог светског рата у коме су се догодила најстрашнија уништења и оштећења културних добара на различитим континентима и неповратно наштетило светској културној баштини.

2. Заштита културних добара кроз идеју културног геноцида

Један од аутора који је веома допринео усвајању Конвенције о спречавању и кажњавању злочина геноцида Лемкин на веома леп начин објашњава због чега је уништавање културних добара по њему једнако тежак злочин као и сам злочин геноцида: „ ... уништавање уметничког дела било које нације мора се сматрати вандализмом усмереним против светске културе. Аутор (злочина) узрокује не само непосредне неопозиве губитке уништеног дела као имовину и као културу колективитета који је директно дотичан ...већ на тај начинпогађа и цело човечанство које доживљава губитак овим чином вандализма. У варварству, као и у вандализму, огледа се асоцијални и

[6] Члан 56 Правилника;

[7] Z. Vučinić, Međunarodnoratnoihumanitarnopravo,Javnopreduzeće "Službeniglasnik", Beograd 2006, 215;

деструктивни дух аутора. Овај дух је по дефиницији супротан култури и напретку човечанства. Враћа еволуцију идеја у суморни период средњег века. Таква дела шокирају савест читавог човечанства, док генеришу крајњу забринутост за будућност. Из свих ових разлога, дела вандализма и варварства морају се сматрати прекршајима против права свих народа."[8] Идеја о постојању културног геноцида касније је подржавана и од стране других аутора и има оправдану заступљеност у литератури. На жалост и поред тога, као и поред тешких искустава из праксе о уништавању културних добара током оружаних сукоба, у Конвенцију о спречавању и кажњавању злочина геноцида, није ушла таква инкриминација. Обзиром да су креатори конвенције желели да истакну тежину дела геноцида у односу на сва друга дела одлучено је да се задрже на забрани уништавања људских живота, док је културна баштина остала изван дефиниције геноцида. Позитивно – правна регулатива задржала се на психичком и биолошком уништењу групе као такве.[9]Ипак, да се овоме пришло другачије, то јест, онако како је то Лемкин предлагао вероватно би то имало утицаја да се током оружаних сукоба у мањој мери уништавају културна добра. Линија којом се требало поћи јесте да када се ради о уништењу групе као такве, наношење штете на културним добрима доприноси потпуном истребљењу и саме групе која је заштитни објект. Ипак правна правила у међународној заједници настају кроз призму политичких односа држава, па је изнет исправан закључак тим поводом: „борба око дефиниције геноцида не може бити адекватно схваћена без проучавања начина на који политика утиче и на правни и на историјски приказ геноцида."[10] Приликом рада на Конвенцији о спречавању и кажњавању злочина геноцида културни геноцид је ушао у први нацрт конвенције, али су државе приговарале и веома брзо је културни геноцид искључен из даљег рада на конвенцији.[11]

3. Заштита културних добара након Другог светског рата

На жалост остају за памћење негативани примери из Другог светског рата када је Адолф Хитлер основао специјалне јединице са задатком да плене

[8] Rafael Lemkin, Acts Constituting a General (Transnational) Danger Considered as Offences Against the Law of Nations (1933), *available at* http://www.preventgenocide.org/lemkin/madrid1933-english.htm

[9] W. Schabas, Genocide in International Law: The Crime of Crimes, Cambridge University Press, 2009, 271–272;

[10] LeoraBilsky Rachel Klagsbrun, The Return of Cultural Genocide?, European Journal of International Law, Volume 29, Issue 2, 2018, 375;

[11] Patty Gerstenblith, The Destruction of Cultural Heritage: A Crime Against Property or a Crime Against People?, Journal of Marshall Review of Intellectual Property Law, 2016, 343;

културну баштину на свим подручјима која су била окупирана од стране Немачке и организован је њихов транспорт у Немачку. Те јединице биле су под руководством Алфреда Розенберга. Према уредно вођеној евиденцији из Западне Европе заплењено је 21 903 уметничка дела, а у СССР је уништено 427 музеја, 1670 православних цркава, 237 католичких.[12] Нарочите штете на културним добрима нанете су услед масовне употребе ваздухоплова у војне сврхе током Другог светског рата и то како од стране сила осовине, тако и од стране савезника. Посебан проблем био је неселективност приликом бацања бомби са великих висина и уништавање читавих градских квартова укључујући и културна добра.

Обзиром на велика разарања која су се догодила током Другог светског рата убрзо по окончању приступило се раду на усвајању правних правила о заштити културних добара. Пре свега културна добра нису била предмет заштите кроз четири Женевске конвенције, јер се овом питању посветила посебна пажња. Један од оправданих разлога за то био је и чињеница да се Женевске конвенције односе на заштиту људских права током оружаних сукоба, а да је заштита културних добара више повезана са ограничењем вођења војних операција. Ипак у допунским Протоколима на Женевске конвенције од 1977. године који се односе како на међународне, тако и на немеђународне сукобе постоје одредбе о заштити историјских споменика, уметничких дела и религијских места, као и употребу такве имовине у војне сврхе. Такође Протокол један забрањује и репресалије према тим објектима.

Тако је 1954. године у Хагу усвојена Конвенција о заштити културних добара у време оружаних сукоба. Конвенција је рађена под окриљем УНЕСКА, а на основу нацрта који је израђено пред почетак Другог светског рата у систему Друштва народа. Ова конвенција је ступила на снагу 1956. године, када је достигла 5 ратификација што је и био услов према слову њеног текста.[13] Данас ова конвенција има 133 државе чланице, што представља велики број чланица међународне заједнице, а Република Србија је чланица од 2001. године након што је поднела сукцесорску изјаву којом приступа овој конвенцији.

На почетку се закључује да су културна добра заједничка баштина целокупног човечанства и да због тога мора бити заштићена. Гарантује се заштита културних добара како у рату, тако и у миру.

[12] J. Johnson, op.cit., 123;

[13] Више о конвенцији видети: Jan Hladik, The 1954 Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict and the Notion of Military Necessity,) 86(835) International Review of the Red Cross,1999;

У овој конвенцији културна добра дефинисана су као а) покретна или непокретна добра од велике важности за баштину народа, као што су споменици архитектуре, уметнички или историјски споменици, било верски или световни; археолошки локалитети; скупови грађевина који су као целине историјски или уметнички занимљиви; уметничка дела; рукописи, књиге и други уметнички, историјски или археолошки занимљиви предмети; научне збирке и важне збирке књига, архивског градива или репродукција горе дефинираних добара; б) зграде чија је главна и стварна намена очување или излагање културних добара дефинисаних у тачки а), као што су музеји, велике библиотеке, места чувања архивског градива те склоништа намењена склањању покретних културних добара дефинисаних у тачки а) у случају оружаног сукоба.[14]Одавде се може видети да се културна добра деле на покретна и непокретна, стим што она могу бити и у директној физичкој вези, али то и не морају да буду. Даље је предвиђено да су стране уговорнице дужне да се старају о таквим културним добрима, али да су време оружаних сукоба може да се одступи од тога уколико то захтева војна потреба. Ова одредба у великој мери штети очувању културтних добара јер омогућава оправдање за њихово уништење. У наставку се забрањује било каква крађа културних добара, оштећења или репресалија.[15] Државе се даље обавезују да воде уредне евиденције културних добара, као и да у случају сукоба не организују војне јединице у њиховој близини. Предвиђа се и одређивање зона безбедности у околини културних локалитета. Конвенцијом су предвиђене и обавезе окупатора да штити културна добра на териоторији коју је окупирао. Сва културна добра морају бити јасно обележена да би се према њима поштовале потребне мере. Конвенција предвиђа и културна добра под специјалном заштитом која имају нарочити третман. Као један од учесталих приговора овој конвенцији наводи се непостојање механизма контроле и надзора над применом њених одредаба. Овај акт наводи како би требало поступати са њима, али не и шта се догађа у случају непоштовања одредаба. Протокол 1 штити посебно покретна културна добра која се могу изнети са окупиране територије. Предвиђено је да се културна добра обележавају плаво – белим штитом и као таква распознају приликом спровођења војних операција.

На међународном плану се води регистар културних добара и организује надзор и контрола од стране УНЕСКА. Ова организација има статус специјализоване агенције Уједињених нација и задатак да обезбеди очување и заштиту светског уметничког наслеђа и споменика историје и науке.[16]Тако

[14] Члан 1 Конвенције;

[15] Члан 4;

[16] Члан 1. Статута УНЕСКА;

се улога ове организације може пратити кроз неколицину сукоба где је или надзирала примену конвенције током сукоба, или давала препоруке о потреби да се појача брига у вези заштитом културних добара током оружаних сукоба.[17]

На ову конвенцију усвојена су и два допунска протокола, такође под окриљем УНЕСКа, где се првим спречава држава која је окупирала територију да угрожава културна добра, као и да уколико је дошло до изношења културних добара исте врати. Проколом 2 из 1999. године уводи се термин добара од највеће важности за човечанство и уводи се посебан регистар за та добра. На овај начин се уводи међународни надзор и контрола заштите таквих добара. Поред ове опште конвенције и поменутих протокола културна добра су заштићена и у следећим правним изворима: Конвенција о мерама забране и спречавању недозвољеног увоза, извоза и преноса власништва културних добра из 1970., Конвенција о заштити светске културне и природне баштине из 1972., Европске конвенције о заштити археолошке баштине из 1992., Конвенција о заштити подводне културне баштине из 2001., Конвенција о заштити нематеријалног културног наслеђа из 2003. године. Конвенција о културној разноликости из 2005. године.

Конвенција о заштити светске културне и природне баштине на следећи начин дефинише културна добра: - споменици, намењени као „архитектонска дела, дела монументалне скулптуре и слике, елементи или структуре археолошке природе, натписи, пећински станови и комбинације обележја, који су од изузетне универзалне вредности са становишта историје, уметности или науке ";

- локалитети, укључујући „дела човека или комбинована дела природе и човека, и подручја која укључују археолошка налазишта која имају изузетну универзалну вредност са историјске, естетске, етнолошке или антрополошке тачке гледишта";

- групе зграда, односно „групе одвојених или повезаних зграда које су због своје архитектуре, хомогености или места у пејзажу од изузетне универзалне вредности са становишта историје, уметности или науке".[18]

Поред наведених правних инструмената мора се нагласити да су културна добра заштићена и кроз Статут којим је основан Стални међународни кривични суд. Тако је предвиђено као ратни злочин следеће: „Намерно усмеравање напада на верске, образовне, уметничке или научне објекте

[17] O'Keefe R, The Protection of Cultural Property in Armed Conflict, Universityof Cambridge, 2008, 172 – 173;

[18] Конвенција о заштити светске културне и природне баштине, члан 1;

или објекте који се користе у добротворне сврхе, историјске споменике, болнице и места где се сакупљају болесни и рањени, под условом да то нису војни циљеви."[19] Овакво дефинисање злочина је у суштини континуитет са регулисањем заштите културних добара у Хашкој конвенцији из 1907. године и ограничава заштиту начелом војне потребе. Такав приступ је помало разочаравајући јер може да доведе до оправдања да се оштете или униште културна добра током оружаних сукоба. Прилично је поражавајуће и то што је након једног века уништења великог броја културних добара Римски статут на овакав начин дефинисао овај ратни злочин јер је употреба војне потребе веома често потенцијално оправдање за оштећење или уништење културних добара.

Током оружаних сукоба било је и позитивних примера када су војни команданти водили рачуна о заштити културног наслеђа. У шпанском грађанском рату (1936 – 1939) један републикански командант, у борбама око Мадрида, одлучио се за ризичнију ратну операцију само зато да не би дошло до оштећења или уништења музеја Прадо и његовог културног блага.[20]

4. Новији примери из праксе и деловање Савета безбедности УН

Остаје на жалост забележено и да су Талибани уништили будине кипове старе 1700. године 2001. године који су били урезани у стени. Затим је Ал - каида 2006. године уништила џамију у Ал Аскари у Ираку стару преко хиљаду година. Неколико година касније уништили су древни град Тимбукту који је био уврштен у УНЕСКО попис светске културне баштине. Остају забележена најновија страшна уништења светске културне баштине када су припадници Исламске државе ушли у древне градове Палмиру, Мосул и Ниниву која је стара преко 6000 и под заштитом је УНЕСЦ – а. Просто невероватно делује да се 2015. године чине таква зверства усмерена према културној баштини целокупног човечанства, а снимци уништења морају да згрозе сваку особу на свету. Поред ових случајева у новије време и терористичке организације су започеле дејства према културним објектима што представља нарочиту опасност по њих. Тако су 2000. године изведени напади на катедралу у Стразбуру, на Ајфелов торањ 2002. године, на Базилику Светог Петра у Риму 2005. године

[19] Statute of the International Criminal Court, art. 8(2)(b)(ix) (applying to international armed conflict) and Article 8(2)(e)(iv)(applying to non-international armed conflict).

[20] Јелена Вилус, Правна заштита културних добара, Европски центар за мир и развој Универзитета за мир Уједињених нација, 2007, стр. 20;

и на зграду британског парламента 2005. године.[21] Након 1999. године и губљења непосредне јурисдикције над јужном покрајином Косово и Метохија дошло је до низа напада на верске објекте на овом подручју који имају далекосежне последице, а ово нарочито јер су неки од њих евидентирани као културна добра од посебног значаја на међународном плану, као на пример Високи Дечани од 2004. године.

Савет безбедности Уједињених нација је у више наврата у својим резолуцијама позивао на заштиту културних добара у неким од новијих сукоба. Тако је у случају Авганистана 1999. године Савет безбедности закључио следеће: „Савет безбедности потврђује своју снажну посвећеност суверенитету, независности, територијалном интегритету и националном јединству Авганистана и своје поштовање културног и историјског наслеђа Авганистана."[22] Веома слично овај орган огласио се и поводом ситуације у Ираку 2003. године.[23] Он је овом приликом, примењујући своја овлашћења према глави 7 Повеље, позвао све државе да предузму све потребне мере како би се омогућило враћање културних добара која су нестала са тачно утврђених локалитета из Ирака и позвао државе да спрече њихову трговину. Овакав приступ, иако представља деловање у оквиру овлашћења која има овај орган, у реалности не доводе до жељених резултата. На исти начин овај орган деловао је и у случају великих уништења и оштећења културних добара у Сирији 2015. године. Услед сукоба на територијама Сирије и Либана дошло је до крађе великог броја уметничких и културних дела па је прво Европска унија 2013. године забранила трговину сиријским уметничким делима, а затим две године касније и Савет безбедности у односу на уметнине из Сирије и Ирака.[24] Све државе су дужне да обезбеде у свом унутрашњем поретку примену одредаба ових резолуција путем усвајања одговарајућих аката и мера. Такође неопходна је и сарадња међународних организација у том контексту пре свих УНЕСКА и ИНТЕРПОЛА. Обзиром да су мировне мисије Уједињених нација ангажоване у великом броју подручја, а нарочито у подручјима у којима се још увек воде борбена дејства Генерални секретар ове организације је још 1999. године донео упутства по којима снаге морају да поступају у смислу поштовања норми међународног хуманитаног права. Тако је између осталог предвиђено да се забрањује снагама УН да нападају културна добра, да не користе њихову околину тако да се према њима може нанети штета или се могу уништити,

[21] Frey, B. S., Rohner, D., Protecting cultural monuments against terrorism, Defence and Peace Economics, Vol. 18(3), No. 2007, 246;

[22] Резолуција 1267 из 1999;

[23] Резолуција 1483 из 2003;

[24] Резолуција Савета безбедности број 2199 из 2015. године;

а предвиђена је и строга забрана пљачкања, крађа, њиховог одузимања или неког варварског чина према културним добрима[25].

У складу са резолуцијом Савета безбедности Аустралија је 2003. године усвојила Уредбу под називом Прописи у Ираку где је предвиђено да лица не смеју да преносе предмете културних добара која су на илегалан начин уклоњена уз места у Ираку (укључујући Ирачки национални музеј или Националну библиотеку Ирака) након усвајања резолуције 66, а лица која поседују или контролишу предмет таквих културних добара морају та добра што пре предати а) особљу УН, б) припаднику одбрамбених снага, в) представнику власти из резолуције 1483, г) представнику Ирачког националног музеја или Националне библиотеке Ирака, д) представнику места са којег је уклоњен или се основано сумња да је уклоњен или ђ) припаднику аустралијске савезне полиције или полицијске снаге државе или територије.[26] Овакво поступање Аустралије је вредно пажње и похвале и било би добро да овај пример следе и друге државе када имплеметирају одредбе резолуције Савета безбедности. Једино што делује неостваривo да се таква културна добра предају лицима која су представници културних институција из Ирака обзиром да ће се до њих из разумљивих разлога веома тешко доћи. Вероватно су она наведена да би се отклонила свака сумња у добру веру ове државе када поступа у конкретном случају.

Као један од веома позитивних примера бриге о заштити културног наслеђа након оружаних сукоба може се навести примерВелике Британије која је 2018. године вратила један део украденог културног наслеђа током инвазије на Ирак још из 2003. године, као и новији пример враћања 17000 јединица културног наслеђа из Ирака од стране САД – а 2021. године које су махом пре инвазије биле смештене у Ирачком националном музеју у Багдаду. Као једна од највреднијих културних знаменитости овом приликом је враћена глинена плоча са делом текста Епа о Гилгамешу.

Нови примери уништења или крађа културних добара показују све већу умешаност недржавних актера у ове недозвољене делатности који се свесно организују ради вршења нелегалне трговине културним добрима из разлога материјалне користи. Такве групе се организују и имају своје путеве за илегални транспорт и продају културних добара. Због те чињенице потребно је радити на што чвршћем повезивању држава на међународном плану, али и усвајања потребне регулативе у правним порецима

[25] Извори Међународног хуманитарног права, 2007, 343;

[26] Vincent Négri,Cultural heritage through the prism of resolution 2199 (2015) of the Security Council, Legal study on the protection of cultural heritage through the resolutions of the Security Council of the United Nations, 9;

држава. Поред тога све су чешћи примери терористичких аката према културним добрима, управо због вредности коју имају и значаја који остварују за конкретне државе и народе.

5. Закључна разматрања

Уништење, оштећење или крађа културних добара током оружаних сукоба представља велики изазов за међународну заједницу. Такви варварски чинови су неспојиви са модерном међународном заједницом, али ипак прате модерне оружане сукобе. Појавом аката тероризма и све веће илегалне трговине културним добрима овај проблем је још више закомликован. Због таквих нових трендова неопходна је другачија активност држава и међународне заједнице преко међународних организација. У раду су изнети неки позитивни примери понашања држава који могу бити модел за решавање овог сложеног проблема. Често је потребно дуго година након оружаних сукоба радити на проналажењу културних добара, а предуслов за то је њихов прецизан попис и праћење илегалних тржишта овим добрима.

Са друге стране мере које треба појачати и на којима треба да инсистира Савет безбедности Уједињних нација у сарадњи са организацијом УНЕСКО јесте поштовање зона безбедности на местима где се налазе културна добра. На овај начин ће се умањити могућност њихвоог уништавања. Поред тога треба инсистирати на упућивању независних мешовитих међународних комисија током и након оружаних сукоба које ће имати специјални задатак да контролишу заштиту културних добара током и након оружаних сукоба. Овакве активности могуће су и посредством мировних мисија Уједињених нација које су често задужене за успостављање и изградњу мира.

Bojan Milisavljević, PhD.,
Full Professor,
Faculty of Law, University of Belgrade,
Serbia

PROTECTION OF CULTURAL PROPERTY IN ARMED CONFLICTS

Summary

The paper analyzes the protection of different forms of cultural property during armed conflicts. At the beginning of the paper, the importance of this protection is pointed out, only the cultural good is defined and an introduction is given in terms of negative examples of destruction of cultural goods and the development of the first rules on the prohibition of such activity. The author states in the paper that the awareness of the ban on such activities appeared a long time ago, but that in recent times we have witnessed the destruction of cultural property. The article analyzes the development of the legal prohibition of damage and destruction of cultural property, starting from internal regulations, through the Hague Law, to the Convention on the Protection of Cultural Property of the United Nations.

The author especially emphasizes the importance of the work of the international organization UNESCO, but also the adoption of two additional Protocols to the mentioned convention. In addition to these acts, the author emphasizes the importance of long legal sources in this area, both at the universal and regional level. Finally, the paper points out some basic shortcomings of the existing system of protection of cultural goods in completely changed circumstances of terrorist acts and internal conflicts and proposes concrete measures to improve their protection in the time ahead. In particular, the need to organize the international community regarding the return of stolen cultural property after armed conflicts is pointed out, and positive examples from practice in this regard are given.

Keywords: *protection of cultural goods, armed conflicts, theoretical acts.*

Angel Ristov, PhD,
Associate Professor,
Faculty of Law Iustinuanus Primus,
University Ss.Cyril and Methodius in Skopje,
Republic of North Macedonia

UDK: 347.628.41(497.17)

EXTRAMARITAL UNION IN MACEDONIAN LAW: LEGAL BIGAMIA OR LEGAL GAP

Abstract: *The extramarital union in modern societies is becoming an increasingly accepted form of community life in which the family is founded. In modern societies, it is no longer a step towards marriage, but its alternative. Despite the tendency of increasing the number of children born out of wedlock, in a number of European legislations the extramarital union is still not legally regulated. In the legislations where the extramarital union is predicted, there are no single and unified solutions for it's regulation. In the paper, the author analyze the extramarital union in Macedonian and comparative family law, in order to point out the need for reforms in its regulation. The current legal solution that does not predict marital barriers as a condition for the validity of the extramarital union makes Macedonian family law a rare example in comparative law that is contrary to the morality of society and the principle of monogamy.*

Keywords: *extramarital partners, extramarital union, marital barriers, Civil Code.*

Introduction

The extramarital union is following the marriage as its faithful "shadow" throughout human history (Korać, 2019:228). The road to its legal recognition was difficult (Meulders Klein, 1998 :23). In some periods the extramarital union was tolerated, in others it was forbidden or ignored (Rubellin-Devichi, 1990:18; Kovaček Stanić, 2002: 119-120). In modern societies, despite the large representation of the extramarital union (Atkin, 2011:793), the words of Napoleon Bonaparte: - "Extramarital partners ignore the law, therefore the law ignores them" *(Les concubins ignore le loi, le loi les ignore)*; is still valid!

At the beginning of the second decade of the 21st century in many European legislations the extramarital union is still not legally regulated (Austria, Czech Republic, Estonia, Bulgaria, Georgia, Hungary, Latvia, Poland, Romania, Switzerland, Turkey, etc.) (Ruggeri et alt., 2019) In a number of countries, partners have the choice of whether to marry or enter into another type of legally regulated community. The number of countries that regulate, not only the heterosexual, but also the same-sex extramarital community (France, Belgium, Luxembourg, Slovenia) is small. In recent decades, the number of states that legally regulate same-sex communities in the form of registered partnerships and allow same-sex marriage is slowly increasing.[1]

The decisions of the European Court of Human Rights (ECHR) have a great influence on the legal recognition of same-sex extramarital affairs.[2] Based on them, the extramarital union received its legal protection under Article 8, which regulates the right to private and family life, [3] Article 12 on the right to marry, [4] and Article 14 on the prohibition of discrimination by the ECHR. [5] In the case law of the ECHR, Valianatos v. Greece (2013), in conjunction with Articles 14 and 8 of the Convention, is extremely important for the legal recognition of same-sex communities. In the text that follows, first the extramarital union will be analyzed through the prism of the Macedonian and Comparative Family Law, and at the end we will present the proposals for its arrangement de lege ferenda.

1. The extramarital union in Macedonian law

1.1. Generally for the extramarital union

In Macedonian family law, the extramarital union was not legally regulated until the adoption of the Family Law Act (FLA) in 1992. [6] Macedonian Family legislation is usually thirty years late in terms of all modern reforms! In the past, case law has filled the legal gap in the law (Hadzi Lega, 1994:216; Hadzi Vasilev, 1990: 224). Based on it, certain property rights were recognized to the extramarital partners (Hadzi Lega,1994:216). In recent decades, the attitude of

[1] Neatherland in 2000 was the first state in Europe that allowed sam sex marriage. Till 2020 16 states in Europe predicted the same sex marriage: Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Irish, Luxemburg, Malta, Norvege Portugal, Sweden, Spain and UK.

[2] See more on *www.echr.coe.int*

[3] See *Guide on Article 8 of the European Convention on Human Rights,* Council of Europe, 2020.

[4] See *Guide on Article 12 of the European Convention on Human Rights,* Council of Europe, 2020.

[5] See *Guide on Article 14 of the European Convention on Human Rights,* Council of Europe, 2020.

[6] "Official paper of Repblic of Macedonia" No. 80/92, 9/1996, 38/2004, 33/2006, 84/2008, 67/2010, 156/2010, 39/2012, 44/2012, 38/2014, 115/2014, 104/2015 and 150/2015.

the Macedonian society towards the extramarital union has changed and has become more liberal towards this issue. However, unlike the Western European and Scandinavian countries,[7] in Macedonian society as a basis for family relations dominates the marital community. Marriage is still the most desirable form of community life. This is due to traditional family values, the influence of religion and customs.

The basis for the legal recognition and regulation of the extramarital union in the Macedonian family law arose from the Constitution established in 1991. Article 40 paragraphs 1 and 2 stipulates that: "The Republic provides special care and protection of the family. Legal relations in marriage, family and extramarital union are regulated by law." Based on this provision, extramarital union was recognized as an equal basis for starting a family together with the marital union. However, the marital union, as a more permanent and stable community of life, retained its primacy as a privileged community, while the extramarital union was granted only certain rights. The attitude of the legislator towards the extramarital union is best indicated by the fact that it regulates it with only one norm. Apart from the Family Law Act, provisions governing the rights of extramarital partners are contained in the Law on Property and Other Real Rights,[8] the Law on Biomedically Assisted Reproduction[9] and other regulations governing conflicts of interest.

1.2. The term extramarital union

The legal definition of an extramarital union does not differ from its classical definition of a concubine under Roman law, as a community of life of a man and a woman who have not entered into a valid marriage (Puhan, 1973:189).

[7] An indicator of the increased number of extramarital union's is the increase the number of children born out of wedlock. On average in EU countries, the percentage of children born out of wedlock increased from 5.1% in 1960 to 8.8% in 1980, and in 2011 39.3%. There are large differences between European countries, so that in the countries of southern Europe the percentage of children born out of wedlock is relatively small, but in some other countries it is already more than 50%. The highest percentage of children born out of wedlock in 2012 was in Iceland (66.9%), Bulgaria (57.6%), Sweden (57.4%) and France (55.8%). In contrast, in southern Europe the rates of children born out of wedlock are much lower. In 2012, there were only 2.6% children born out of wedlock in Turkey, 7.6% in Greece, 15.4% in Croatia and 24.7% in Serbia. In Macedonia, the percentage of children born out of wedlock is far below the European average. In 2011, according to the State Statistical Office, only 11.5% of children in Macedonia were born out of wedlock. Over the years this number has increased. In 2019, the number of children born out of wedlock is 2454 or 13.4% of the total number of children born.

[8] "Official paper of Repblic of Macedonia" No. 18/01, 92/08, 139/09 and 35/10.

[9] "Official paper of Repblic of Macedonia" No. 37/08, 164/13, 149/14 and 192/15.

The legislator defines the extramarital union as: “A union of life of a man and a woman which is not established according to the provisions of this law (extramarital union) and which lasted at least one year, is equal to the marital union in terms of mutual support and property acquired during the duration of that community ”(Art. 13 FLA). This determination of the legislator is in accordance with the generally accepted view of domestic science according to which the extramarital union is a living union of a man and a woman who did not enter into a marriage based on the intention to be permanent and which does not differ much in content from the marital union (Hadzi Vasilev, 1990:223; Hadzi Lega, 1994: 215). Based on that, in our law only the heterosexual extramarital union is legally regulated. Same-sex extramarital community and registered same-sex partnerships are not legally regulated (Spirovic Trpenovska et alt., 2011:78).

Essential conditions for the validity of the extramarital union are: 1) existence of a community of life of persons of different sex and 2) duration of the community of at least one year. Although is not explicitly predicted in the law, for its recognition should take into account the overall relationship of the partners, their quality and the true intention to live together. This is because the occasional and short-lived relationship between a man and a woman does not have the character of an extramarital affair. In theory, even before the extramarital union was regulated, it was indisputable that marital barriers apply appropriately to extramarital partners (Hadzi Vasilev, 1990:223). However, in the FLA the legislator forgot to provide them in the legal provisions (Mickovik, Ristov, 2015: 188). This unintentional omission of the legislator on this issue has created dilemmas in theory and practice.

In the opinion of prof. Spirovic Trpenovska, despite the fact that marital obstacles are not explicitly provided as a condition for the validity of the extramarital union, they are applied by analogy and are valid for the extramarital union as well (Spirovic Trpenovska, 2007:294). The author of this text, in the past, referring to the provision of Article 8 paragraph 2 of the Constitution, according to which “everything that is not prohibited by the Constitution and laws is allowed” advocated the liberal opinion that until the legislator explicitly prohibits, it is allowed and possible one person to be both in a formal marital union and in an extramarital union. This is because most often in practice it is about the so-called “dead” marriages, which formally exist only on paper. The marital union does not actually exist at the expense of the actually established extramarital union in which the extramarital partners live, raise children, acquire property and enter into numerous property relations.

Different views in the science of family law have been reflected in case law. [10] In its initial decision, the Skopje Court of Appeals quashed the first-instance judgment, citing the analogy between the application and validity of marital barriers and the extramarital union, as a condition for its validity. Following the same verdict, with an in-depth explanation by the first instance court, in its repeated decision, the Court of Appeals in Skopje changed its initial position, stating that "the formal existence of the marital union, in conditions of real de facto existence of an extramarital union and the life of a man and a woman, longer than one year, cannot be an obstacle for the extramarital union to produce legal actions like the marital union".

After many years, the author of this text changed its original liberal position for the reason that everything that is not forbidden by the Constitution and laws does not have to be honest and fair! (Galev, Dabovic Anastasovska, 2018: 212-214). The legislator and the case law in regulating marital and family relations have forgotten about morality as an additional source of law! (Ristov, 2004:216) It is in marital and family relationships where morality has it greatest application. Many personal relationships in marriage and the family are not regulated by law but by moral norms. Therefore, morality must be taken into account. After a decade of its original view, the author believe that he was wrong in the liberal view of the issue, preferring the regulation of property relations that can be brought under the rules of civil law, rather than moral norms.

Morality in society should be a guide in the conscientious and honest conduct of individuals, especially in marital and family relationships. Therefore, legal norms should be based on morality and moral social values (Ruschev, 2016:176-180). In a conservative society such as the Macedonian one, in which the old traditional family values still dominate, it is contrary to the morality of the society for a person to be married and in an extramarital union at the same time. This view promotes bigamy in theory and case law, which is contrary to public order and morality. It can seriously shake the foundations of the family and the good relationships in it and have far-reaching and irreparable consequences for the children in the future. It can seriously grow into a pattern of behavior in the future. Therefore, the author believes that the current solution is a mistake of the legislator, who should correct it as soon as possible in the upcoming reforms of family law. For the validity of the extramarital union, there must be no marital obstacles between the extramarital partners! (Mickovik, Ristov, 2019:167). In addition, the general legal provisions must predict the morality of society. Until then, the courts should interpret the existing provisions on the validity of the extramarital union through the analogous application of marital barriers and

[10] See verdict of the Appeal Court in Skopje Gz. No. 1811/11 from 16.09.2011.

the morality of society, and resolve the relations between these persons with the rules of civil law (Mickovik, Ristov, 2015:65-66).

1.3. Formation of the extramarital union

Extramarital union differs from marriage in several aspects. The marriage is concluded in written and formal form (ad solemnitatem) before a competent state body. The extramarital union occurstakes place informally. For its occurrence, the consent of the free will of the extramarital partners to establish a community of life is sufficient. The participation of a competent state body, the participation of witnesses and other persons is not required. The reason for this is the accepted concept of unregistered extramarital union, due to which the formation of the extramarital union does not require any written statement, nor its registration before a competent state body or notary. For its occurrence, the beginning of the joint life between a man and a woman is enough. The exact moment of the formation of the extramarital union is known only to the extramarital partners, but not to the general public. Because the extramarital union is not registered and a document is not issued, a public document for it, most often when it terminates there is a need to prove its occurrence and duration, in order to provide judicial protection.

This concept produces legal uncertainty in property relations and the possibility of abuse. Therefore, in comparative law there is a very small number of countries that have accepted the concept of unregistered extramarital union (Croatia, Slovenia, Montenegro, Kosovo). Therefore, we consider it desirable for the legislator to reconsider its position on the existing concept of an unregistered extramarital union. In that sense, in order to ensure greater legal certainty, it should enable the extramarital partners who want to avoid possible difficulties in exercising their rights, to formalize their relationship with a two-sided statement that will be notarized and deposited with a notary public or with mutual agreement for cohabitation. The time for the realization of the rights from the extramarital union will be considered from the day of the notarization of the statement or the agreement with the notary public. The extramarital union could end with a unilateral or mutual statement of the partners that the extramarital union ends. Extramarital partners who do not want to register their extramarital affair will be exposed to more severe consequences in exercising their rights from the extramarital union in terms of proving the existence and duration of the extramarital union.

1.4. Legal effects of the extramarital union

In Macedonian family law, the extramarital union is not completely equal to the marital union, despite the fact that it performs the same functions. It is equal

to the marital union, in terms of the right of the extramarital partners to a part of the jointly acquired property and the right to alimony. This means that the Macedonian legislator has opted for a middle ground, equating the extramarital union with the marital union, but only in terms of certain legal consequences. In comparative law there are legislations that completely equate the extramarital affair with the marital union, including the right of inheritance (Slovenia, Sweden). However, as a result of conservative and traditional values, there are still legislations that do not attach any importance to the extramarital union.

Unlike spouses, in Macedonian law extramarital partners do not enjoy any rights from social, health and pension insurance. There is also a difference in the legal status of spouses and extramarital partners in relation to children. While the paternity of children born in wedlock is not established, extramarital paternity should be established in one of the ways predicted by law. According to the Family Law Act, the mother's spouse is considered the father of the child born during the duration of the marriage or within 300 days after the termination of the marriage (Article 50). The father of a child born out of wedlock is the person who will recognize the child as his own. In addition, paternity can be recognized before the registrar, the Center for Social Work and the court. Acknowledgment of paternity can also be made by will.

There are also differences regarding the entrustment of custody and upbringing of children in case of termination of the marital and extramarital union. While the court decides on entrusting the custody and upbringing of children during divorce, the Center for Social Work decides on for the children born out of wedock. This decision, in addition to being discriminatory, is also contrary to the UN Convention on the Rights of the Child, according to which there is always judicial control when deciding on the rights and interests of the child. As a result of this legal solution, the extramarital partners face great difficulties in establishing personal and direct contacts with the child after the termination of the extramarital union. That was the reason why our country lost the dispute before the ECHR in the case of Oluri v. Macedonia.

According to the Law on Biomedical Assisted Reproduction (BAR), the extramarital partners had the right to biomedically assisted fertilization. The right to use the BAR procedure have adult and legally capable men and women, who are capable of performing parental care and who are married or living in an extramarital union, as well as women who are not married or in an extramarital union, if the previous treatment is not successful (Art. 9). In this procedure, the extramarital partners prove their status before the competent authorities with a statement certified by a notary public so that they can exercise their right. This indicates the need to introduce the concept of a registered extramarital union, in order to avoid possible abuse of rights in practice.

2. The extramarital union in comparative law

The extramarital union was for the first time equated with marriage under the Russian Marriage, Family, and Guardianship Act of 1927, which allowed informal marriage (Kovaček Stanić, 2002:119) . Due to the catastrophic consequences, the actual marriage was dissolved in 1944. In European countries, extramarital affairs were not subject to legal regulation until the 1960s. In recent decades, as a result of transformations in marital and family relations, major changes have taken place in all European family law legislation. Part of those changes in certain legislations is the legal regulation of extramarital communities (Mickovik, Stojkova, 1999:99). The large increase in the number of extramarital affairs in all European countries is an indicator that in recent decades there have been major changes in the meaning, role and functions of marriage and the family (Mickovik, 2008:86). Is marriage as an institution in crisis due to the fact that the number of marriages is decreasing at the expense of increasing the number of divorces? (Mickovik, Shutova, 2020: 23-27) Individualism and the pursuit of happiness contribute to many men and omen no longer accepting the rigid framework of marriage and looking for other forms of realization of their intimate relationships.

The choice of extramarital union is a result of the free decision of the people, for whom the realization of happiness and personal satisfaction is a top priority. Due to this, in all European countries there is a tendency to reduce the number of marriages[11] and a large increase in the number of extramarital affairs and children born out of wedlock. In addition to the large increase in the number of extramarital affairs, their nature is changing in modern society. In the past, extramarital affairs were usually only the first step towards marriage, as most extramarital partners have been married for some time. In modern society, the essence of the extramarital union is changing and it is becoming a real alternative to marriage and its competition. In addition, society's attitude towards the extramarital union is changing and it, instead of being rejected as a deviant phenomenon, becomes an acceptable social phenomenon.

[11] The rate of marriages in European Union countries (which shows the number of marriages per 1,000 inhabitants) decreased from 6.75 in 1980 to 4.8 in 2008, so that in 2008 737,000 marriages were concluded in European countries less than in 1980. According to Eurostat, in 2012 the highest marriage rates were in Turkey (8), Lithuania (6.9), followed by Malta and Cyprus (6.7). The marriage rate in Macedonia in 2012 was among the highest in Europe (6.8 marriages per 1,000 inhabitants). The lowest rates of marriages in Europe in 2012 were in Bulgaria (2.9), Portugal (3.3) and Slovenia (3.4). At the same time, there is a tendency to increase the average age at the first marriage. Between 1980 and 2005, the average age at first marriage for men increased from 26 to 31.2 years, and for women from 23.3 to 29 years. In Macedonia in 2011 the average age at first marriage was 25.4 years for women and 28.3 years for men. In 2019, 13,814 marriages were concluded, while in 1990 they were divorced.

In the past, an extramarital affair was considered to be a union of two people of different sexes, which occurs and ceases to exist in an informal way, without fulfilling the form provided for the marriage. Lately, in many European countries, gender diversity is no longer required, but it is accepted that extramarital union can exist even when it comes to people of the same sex. The French Civil Code (C.civ), in the provisions of Article 515-8 stipulates that: together (in pairs) ". In that direction is the Spanish law in which certain regional rights by the same law regulate the extramarital affairs of partners of different and same sex, which are considered sui generis communities, outside the family law (Mignot,2001 :602-603). Catalonia passed the Law on Couples in Stable Communities in 1998 (Law 10/1998), while Aragon passed the Law on Stable Unmarried Couples in 1999 (Law 6/1999). In order to have legal consequences, the extramarital union must have certain characteristics, such as the permanence and stability of the relationship, or the birth of a joint child.

In European countries there are different models of legal regulation of the extramarital union. According to Kovacek-Stanic, the laws that regulate the extramarital union differ according to the manner of regulating their occurrence, according to the family legal actions of the extramarital union and according to its termination (Kovaček Stanić, 2002:120-121). Regarding the formation of the extramarital union, there are two models in the European legislation: according to the first model, the registration of the extramarital union is required for it to have legal effect, and according to the second model, which is accepted in the Republic of Macedonia, the extramarital union informal consent of two persons of different sex to live together in an extramarital union. Those countries that provide for the registration of an extramarital union differ in the form of the registration of the extramarital union. In some countries, such as France, there is a specific form for registering a cohabitation, which differs from the form provided for marriage. According to the French model, the registration of the extramarital union takes place in court. In other countries, such as the Netherlands, the registration of the extramarital union uses the form provided for the marriage, so here both the marriage and the extramarital union are concluded in the municipality before the registrar.

There are two basic concepts in European legislation regarding the legal regulation of extramarital communities. In some countries, a complete and comprehensive system of legal norms governing extramarital affairs is envisaged. This is the case in the legislatures of France, the Netherlands, Sweden, Belgium, as well as in the provinces of Catalonia and Aragon in Spain. In other European countries there is no such model of regulation of the extramarital union, but certain aspects of the extramarital life are regulated in special legal texts, such as the laws on social protection, labor relations and tax laws. In third countries, such as

the United Kingdom, Germany and Italy, the extramarital union is governed by an agreement between the extramarital partners (leaving together agreement).

European legislation also differs in terms of the material conditions that must be met in order for the extramarital union to have legal effect. Some countries provide for certain conditions to be met (most often it is required that there are no obstacles such as kinship, marriage, minority or incapacity for judgment, which are also provided for marriage), and in other countries such conditions are not provided. As stated earlier, in the Republic of Macedonia, certain conditions are not required to be met in order for the extramarital life that lasted more than one year to cause legal effect.

In certain European legislations the legal effect of the extramarital union is similar to the legal effect of the marriage, and it covers both the personal and property legal relations between the partners. Such is the situation in the Netherlands, where the law stipulates that there is an obligation between the extramarital partners for fidelity and helping, leading a life together, as well as a joint responsibility for the care and maintenance of the children. Slovenian law provides for the full equalization of spouses and extramarital partners in their personal and property relations (Novak, 2015: 117-119). In Slovenia, extramarital partners have an obligation to respect and help each other, have the right to independently choose a profession and occupation, as well as the right to decide amicably on a shared home and running a joint household, just like spouses. Contrary to such solutions, which practically equate the action of the extramarital union with the action produced by the marriage, in many legislations (Belgium, Sweden, Serbia, Croatia, Macedonia) only the property relations between the extramarital partners are legally regulated. Thus, for example, in the Republic of Macedonia it is envisaged that an extramarital union lasting more than one year is equated with marriage in terms of the division of property acquired during the duration of the extramarital life and in terms of the right to alimony between the partners. Unlike other legislation that provides norms for regulating property relations between extramarital partners, in Sweden and Norway only norms are regulated that regulate the legal status of the joint home, to which the provisions that apply to marriage apply, but are not regulate property relations between extramarital partners, nor is the right to alimony provided for extramarital partners.

In European countries there are also differences regarding the inheritance status of extramarital partners. In some countries, such as Sweden, Croatia, Montenegro and others, the law stipulates that under certain conditions, extramarital partners can appear as legal heirs. In Croatia, it is stipulated that extramarital partners have the right to inherit if the community has lasted for a long time

and if there were no marital obstacles between the extramarital partners, and a similar solution is provided in Montenegro. On the other hand, in many European countries, such as France, extramarital partners do not have the opportunity to inherit from each other according to the rules of legal inheritance. Such a solution is envisaged in the Republic of Macedonia.

Despite the tendency of increasing the number of illegitimate children in many European countries, the extramarital union is still not legally regulated. Napoleon Bonaparte's words about the legislator's ignorant attitude towards the extramarital union are still relevant. There is a long list of European countries that do not legally regulate the extramarital union: Austria, Belarus, Bulgaria, Cyprus, Czech Republic, Estonia, Georgia, Hungary, Latvia, Lithuania, Poland, Romania, Switzerland and Turkey, etc.(Ruggeri et alt., 2020:3). Whether the decisions of the European Court of Human Rights will have an impact on the legal recognition of the extramarital union in these countries, time will tell.

3. Instead of a conclusion - Extramarital union in Macedonian law de lege ferenda

Almost three decades have passed since the initial arrangement of the extramarital union until today. The provision that regulates the extramarital union, as well as most of the other provisions of the Law have not undergone significant legal changes. Reforms in the family law started in 2011 within the Project for drafting the Civil Code. Ten years of experience so far have shown that the legislator has not yet understood the meaning, importance and role of the Civil Code. The future will show whether the Civil Code will be adopted. Regarding the regulation of the extramarital union, science and practitioners agree that a more thorough regulation of the extramarital union and expansion of its rights is needed. In that sense, it is necessary to envisage marital obstacles as a condition for its validity and to introduce the possibility for registration of the extramarital union, in order to achieve greater legal certainty and enable the realization of other rights in the field of social, health and pension insurance. .

It is also necessary to provide for the proper application of the legal presumption for establishing marital paternity. On that basis, the father of the child born in an extramarital union will be considered the husband of the extramarital partner who gave birth to the child, provided that the extramarital union is registered before a notary public. Furthermore, it is necessary to provide a provision that regulates the performance of parental responsibilities after the termination of the extramarital union or to supplement the existing one that after the termination of the marriage and the extramarital union, the parents jointly and contractually perform the parental responsibilities. To provide for the jurisdic-

tion of the court, and not the Center for Social Work, as an administrative body, to decide which of the extramarital partners the child will be entrusted with care and upbringing. That the existing provisions are outdated, do not work in practice and are contrary to the Convention on the Rights of the Child was confirmed by the decision of the European Court of Human Rights in the case Oluri v. Macedonia. Therefore, it is necessary to make a reform in the regulation of parental responsibilities after the termination of the marital and extramarital union. There should be no difference in editing this issue.

Finally, we believe that the right to legal inheritance of extramarital partners should be provided, provided that the extramarital union lasted for a certain period of time determined by law and that there are no marital obstacles between the extramarital partners. If the extramarital union lasted at least five years until the moment of the testator's death, the extramarital partner would acquire the right to inheritance, analogous to the provisions for the spouse within the legal inheritance. In case there were joint children in the extramarital union, then the deadline should be shorter, ie the extramarital union should have lasted at least three years until the moment of the testator's death. Arguments for such a proposal are the equal position of the married with the illegitimate children, as well as the possibility of persons who have lived in a permanent community for more than five years with the testator to have the right to inherit under conditions provided by law.

In order to increase legal certainty, it is desirable for the legislator to enable the extramarital partners who want to avoid possible difficulties in proving the existence and duration of the extramarital union, to formalize their relationship with a two-sided statement that will be notarized or deposited with a notary or cohabitation agreement. The time that should expire in order for the rights of the extramarital union to be exercised will be considered from the day of certifying the statement with the notary public. Under this solution, extramarital partners who do not wish to register their extramarital affair will continue to enjoy the rights provided for extramarital partners, but will be exposed to the risk associated with proving the duration of the extramarital union.

Literature

Atkin Bill, (2011) "The Legal World of Unmarried Couples: Reflections on "De Facto Relationships" in recent New Zeland Legislation in VUWLR" Vol 39 issue 4.

Bailey M, (2011) "Poligamy and Unmarried Cohabation" Canada, *The International Survey of Family Law,* 2011 Edition, Jordan Publishing Limited, Bristol.

Борковски Е., Де Плесис П, (2004) *Римско право,* Просветно дело, Скопје.

Boulanger François, (1999) *Droit civil de la famille,* 3 édition, tom I, Aspects comparatives et internationaux, Economica, Paris.

CAE-IRENE-CNUE, (2019-2020) *Couples in Europe,* National Law of 33 European Countries, Edition.

Галев Гале, (2004) Местото, улогата и значењето на справедливоста во правото, *Зборник на трудови од Меѓународниот симпозиум Современото право, правната наука и Јустинијановата кодификација,* Том 2, Универзитет „Св. Кирил и Методиј" Скопје.

Галев Гале, Дабовиќ Анастасовска Јадранка, (2018) Начело на совесност и чесност – фундаментално начело на облигационото право, *Годишник во чест на проф. д-р Миодраг Мицајков,* Правен факултет „Јустинијан Први" Скопје.

Guide on Article 8 of the European Convention on Human Rights, (2020) Council of Europe.

Guide on Article 12 of the European Convention on Human Rights, (2020) Council of Europe.

Guide on Article 14 of the European Convention on Human Rights, (2020) Council of Europe.

Хаџи Василев Миле, (1990) *Семејно право,* Студентски збор, Скопје, 1990.

Хаџи Лега Кочо, (1994) Вонбрачна заедница: настанување, престанок и имотни односи и издржување на вонбрачните другари, *Семејното законодавство на Република Македонија,* Скопје.

Korać Radivoje,(2019)*Porodično pravo,* 3M Makarije, Podgorica.

Kovaček Stanić Gordana, (2002) *Uporedno porodično pravo,* Univerzitet u Novom Sadu.

Meulders Klein Marie Terese, (1998) „Mariage et concubinage ou les sens et contresens de l'histoire", *La Personne, La Famille et le Droit,* 1968-1998, Paris.

Mignot Mark, (2001) La partneriat enregistré en Droit International privé, *Revue Internationale de Droit Comparé,* No. 3.

Мицковиќ Дејан, Ристов Ангел, (2015) *Семејно право,* Стоби трејд, Скопје.

Мицковиќ Дејан, Ристов Ангел, (2019) Реформите во семејното право во преднацртот на Граѓанскиот законик на Република Македонија, *Зборник во чест на доцент Кристијан Таков,* Софија.

Мицковиќ Дејан, Ристов Ангел, (2015) *Закон за семејството,* Стобитрејд, Скопје.

Мицковиќ Дејан, Стојкова Лидија, (1999) „Вонбрачната заедница во современите семејства", *Евродиалог,* бр. 15, Студентски збор.

Мицковиќ Дејан, (2008) „Правното регулирање на вонбрачната заедница", *Правник,* Здружение на правници на РМ, бр. 195-196.

Мицковиќ Дејан, (2008) *Семејството во Европа 16-21 век,* Блесок, Скопје, 2008.

Мицковиќ Дејан, Шутова Милица, (2020) *Разводот на брак во европските земји,* Софија, Богданци.

Novak Barbara, (2015) *Družinsko pravo,* Uradni list, Ljubljana.

Пухан Иво, (1973) *Римско право,* Универзитет Кирил и Методиј, Скопје.

Ристов Ангел (2004),,Извори на граѓанското право во Република Македонија", *Зборник во чест на Миле Хаџи Василев,* Универзитет „Св. Кирил и Методиј" Правен факултет „Јустинијан Први'' во Скопје.

Ристов Ангел, (2015) „Вонбрачната заедница во македонското семејно право" *Охридска школа на правото,* Том 1, Iuridica Prima, Скопје, 2015.

Rodin Mirella, (2013) Protivnost moralu (contra bonos mores) kao razlog nevaljanosti ugovora, *Zbornik Pravnog fakultetu Sveučilišta u Rijeci,* v. 34, br. 2.

Русчев Иван, (2016) Противоречието със закона и накърняване на добрите нрави като основания за недействителност - хипотези от практиката. - В: *Сборник доклади от Междунар. научна конф., УНИТЕХ'16, Габрово, 18-19ноември 2016 г.* Т. IV. Габрово, Технически университет.

Rubellin-Devichi, (1990) *Des concubinages dans le monde,* Centre de droit de la famille, Editions du centre National de la Recherche Scientifique, Paris.

Ruggeri Lucia, Kunda Ivana, Winkler Sandra, et alt., (2019) *Family Property and Succession in EU Member States;* Faculty of Law in Rijeka.

„Službeni vesnik Republike Makedonije" бр. 80/92, 9/1996, 38/2004, 33/2006, 84/2008, 67/2010, 156/2010, 39/2012, 44/2012, 38/2014, 115/2014, 104/2015, 150/2015.

„Službeni vesnik Republike Makedonije " бр. 18/01, 92/08, 139/09 i 35/10.

„Službeni vesnik Republike Makedonije " бр. 37/08, 164/13, 149/14 i 192/15.

Спировиќ Трпеновска Љиљана, Мицковиќ Дејан, Ристов Ангел, (2011) Наследувањето во Европа, Блесок, Скопје.

Спировиќ Трпеновска Љиљана, (2007) Аналогија на брачната со вонбрачната заедница, *Годишник на Правниот факултет „Јустинијан Први" во чест на Борислав Благоев,* Скопје том 43.

Панов Slobodan, (2010) *Породично право,* Правни факултет Универзитета у Београду, Београд.

Alinčić Mira, Hrabar Dubravka, Jakovac-Lozić Dijana, Korać-Graovac Aleksandra, (2007) *Obiteljsko pravo,* Narodne Novine, Zagreb.

Матеева Екатерина, (2010) *Семейно право на Република България,* ВСУ „Черноризец Храбър", София, 2010;

Цанкова Цанка, Марков Методи, Станева Ана, Тодорова Велина, (2009) *Коментар на новия Семеен Кодекс,* ИК „Труд и право", София.

Марков Методи, (2009) *Семейно и наследствено право,* Сиби, София.

CAE-IRENE-CNUE, (2019-2020) *Couples in Europe,* National Law of 33 European Countries, Edition.

Др Ангел Ристов,
Ванредни професор,
Правни факултет Јустинијан Први,
Универзитет „Св.Кирил и Методиј" у Скопљу,
Северна Македонија

ВАНБРАЧНА ЗАЈЕДНИЦА У МАКЕДОНСКОМ ПРАВУ: ЗАКОНСКА БИГАМИЈА ИЛИ ПРАВНА ПРАЗНИНА

Апстракт

Ванбрачна заједница у модерним друштвима постаје све прихваћенији облик породичног живота у којем се оснива породица. Она више није само корак ка браку, већ и његова алтернатива и конкуренција. Упркос тенденцији повећања броја деце рођене ван брака, у великом броју законодавства, ванбрачна унија још увек није регулисана. У породичним правима који предвиђају ванбрачну заједницу не постоје јединствена решења за њену регулацију. У раду, аутор анализира ванбрачну заједницу у македонском породичном праву и упоредном праву како би указао на потребе од реформе у њеном уређењу. Тренутно правно решење које не предвиђа брачне препреке као услов за пуноважност ванбрачне заједнице чини македонско породично право ретки пример у упоредном праву који је у супротности са моралом и општим принципима породичног закона.

Кључне речи: *ванбрачна заједница, ванбрачни партнери, брачне препреке.*

Др Наташа Стојановић,*
Редовни професор,
Правни факултет Универзитета у Нишу,
Србија

UDK: 349.6:341.24(4-672EU)

ЕВРОПСКИ ЗЕЛЕНИ ДОГОВОР – ПУТ КА ЗЕЛЕНОЈ И ДИГИТАЛНОЈ ТРАНСФОРМАЦИЈИ ПРИВРЕДЕ И ДРУШТВА ЕВРОПСКЕ УНИЈЕ[1]

Апстракт: *Европска унија, као и читава међународна заједница, деценијама уназад суочавају се са климатским променама, енормним губитком биолошке разноврсности, великим загађењем ваздуха, воде и земљишта и сл. Значајан део „кривице" за такво стање припада неконтролисаним емисијама гасова са ефектом стаклене баште које се јављају у: процесу производње и употребе енергије, базиране на угљу, дрвету и природном гасу; затим у линеарној економији, у којој је привредни раст условљен великом потрошњом ресурса и „производњом", опет, велике количине отпада; у друмском саобраћају, који је више заступљен у пракси у односу на железнички или транспорт унутрашњим пловним путевима и са тим повезано, готово редовно, саобраћајно загушење, али и у производњи и потрошњи хране. Посебан проблем представља релативно ниска стопа обнове приватних и јавних зграда која би омогућила њихову бољу енергетску ефикасност. Како би разрешила јасно видљив дисбаланс између привреде и животне средине, Европска комисија је припремила и јавности презентовала Европски зелени договор 11. децембра 2019. године. Тим правним актом Европска унија заправо снажније и свеобухватније наставља раније започету трансформацију и модернизацију своје привреде са циљем постизања климатске неутралности, закључно до 2050. године. Европска унија, у реализацији овог амбициозног и комплексног циља, посебно рачуна на дигиталне иновације и дигиталне технологије. У раду аутор пажњу фокусира на решења која нуди Европски зелени договор и одговарајући прописи Европске уније о*

* natasa@prafak.ni.ac.rs

[1] Рад је настао као резултат финансирања од стране Министарства просвете, науке и технолошког развоја Републике Србије према уговору, евиденциони број 451-03-9/2021-14/200120.

дигитализацији, који су у директној вези са зеленом и дигиталном трансформацијом привреде и друштва Европске уније, са циљем да утврди њихов смисао и домашај у погледу стварања климатски неутралног европског континета.

Кључне речи: *Европски зелени договор, зелена трансформација привреде и друштва, дигитализација.*

1. Уводне напомене

Европска унија, суочена са значајним загађењем ваздуха, воде и земљишта, великим губитком биодиверзитета и климатским променама, припремила је и јавности презентовала Европски зелени договор 11. децембра 2019. године,[2] као одговор на постојеће и потенцијалне опасности које могу да допринесу даљем погоршању климе, животне средине и здравља људи.

Европска комисија овим правним документом жели да настави даље, до 2050. године, трансформацију европског друштва у праведно и просперитетно друштво чији ће „заштитни знак” бити нулта емисија гасова са ефектом стаклене баште, и у чијем средишту је модерна и одржива привреда која свој раст не везује за потрошњу ресурса (Европски зелени договор, 2019: 1).

У остваривању постављених циљева Европска комисија посебно рачуна на постојеће дигиталне технологије: вештачку интелигенцију, 5 Г технологију, рачунарство у облаку, рачунарства на ивици и интернета ствари,[3] али и на повећање европског суперрачунарског капацитета у циљу развоја иновативних решења, поред осталог и у сфери животне средине.[4] Амбиције Европске комисије на дигиталном плану иду и даље, па се указује на потребу улагања у нове квантне технологије и развој квантних рачунара

[2] European Commission (2019). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. *The European Green Deal*. Преузето 20. 1. 2020. године. https://www.eur-lex.europa.eu/legal-content/EN/TXT/?qid=1588580774040&uri=CELEX:52019DC0640.

[3] О појмовима: „рачунарство у облаку”, „рачунарство на ивици” и „интернет ствари”, као и о њиховим предностима и недостацима, видети код: FEFA fakultet. Rečnik IV ind. revolucije. Преузето 12. 9. 2021. године. https://www.fefa.edu.rs/Recnik-IV-ind-revolucije/

[4] Видети: European Commission (2020) *Shaping Europe's digital future*. Преузето 12. 7 2021. године. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en.

код еколошких изазова и у борби против климатских промена (Дигитални компас 2030., 2021: 8).[5]

На дигиталне технологије Европска комисија рачуна и код стварања дигиталног модела Земље (тзв. „Земљин дигитални близанац") који би требало да појача потенцијале Европске уније у предвиђању еколошких катастрофа, мерењу последица климатских промена и управљању природним и еколошким катастрофама (Европски зелени договор, 2019: 19).[6]

Како би сектор информационих и комуникационих технологија допринео смањењу глобалних емисија гасова са ефектом стаклене баште до 15% и стварању климатски неутралног европског континента, он мора и сам да се „зелено" трансформише, будући да троши 5–9% електричне енергије на светском нивоу и „доприноси" са више од 2% у емисијама гасова са ефектом стаклене баште, са тенденцијом њиховог пораста за 14% до 2040. године.[7]

У фокусу пажње аутора у раду јесу решења, садржана у Европском зеленом договору и у другим правним документима Европске уније, посвећеним дигилатизацији[8] de lege lata и de lege ferenda,[9] којима се ближе одређује улога дигиталне технологије у зеленој трансформацији привреде и друштва, са циљем стварања одрживе будућности, у којој неће бити потребе за исцрпљивањем природних ресурса и неће бити озбиљног оштећења животне средине.

2. Декарбонизација енергетског система Европске уније

Циљ Европске комисије, предвиђен Европским зеленим договором, да Европа, до 2050. године, постане климатски неутралан континент са нултом

[5] European Commission (2021). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *2030 Digital Compass: the European way for the Digital Decade*. Преузето 20. 6. 2021. године. https://www.eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.

[6] Дигитални компас 2030. потенцира примену квантних гравитационих сервиса који, поред осталог, могу да прате активности вулкана (Дигитални компас 2030., 2021: 8).

[7] Видети: European Commission (2020). *Supporting the green transition – Shaping Europe's digital future.* Преузето 14. 7. 2021. https://op.europa.eu/en/publication-detail/-/publication/bd211835-5390-11ea-aece-01aa75ed71a1/language-en/format-PDF.

[8] О разлици између појмова: „информатизација", „дигитализација" и „дигитална трансформација" видети код: Popov, 2017.

[9] У том правцу нарочито видети: European Commission (2020). Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. *Shaping Europe's digital future.* Преузето 18. 6. 2021. године. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:67:FIN.

нето стопом емисија гасова са ефектом стаклене баште, поред осталог, подразумева употребу чисте енергије, засновану на обновљивим изворима енергије која потиче из биомасе, морских струја или таласа, плиме и осеке, водотока, сунчевог зрачења, ветра и унутрашње топлоте Земље (геотермалне енергије).[10]

Процене говоре да је за више од 75% емисија гасова са ефектом стаклене баште „кривац” производња и употреба енергије (Европски зелени договор, 2019: 5). Да би се до 2030. године остварило смањење емисија гасова са ефектом стаклене баште за најмање 50%, у односу на период из 1990. године, Европски зелени договор предлаже развој енергетског система који би се темељио на обновљивим изворима енергије,[11] уз постепено искључивање угља из употребе и декарбонизацију гаса (Европски зелени договор, 2019: 3 и 5).[12] Појачана употреба ових извора енергије, осим тога, за собом повлачи и повећање енергетске одрживости система једне државе, али и доприноси безбеднијој достави енергије и смањењу зависности од увоза енергетских сировина или електричне енергије (Bošnjak, 2020).

У даљој декарбонизацији енергетског система Европска комисија посебно рачуна на промовисање и примену иновативних технологија (нпр. хватања угљеника и његовог складиштења) и успостављање енергетске инфраструктуре, попут паметних мрежа (Европски зелени договор, 2019: 5–6).

Како сматра Европска комисија, климатска неутралност европског континета је незамислива без стварања потпуно интегрисаног, међусобно повезаног и дигитализованог европског енергетског тржишта.[13]

Када је у питању декарбонизација енергетских система држава, чланица Европске уније, Европски зелени договор нарочито инсистира на повећаној прекограничној и регионалној сарадњи, у циљу бољег искоришћавања чистих извора енергија (Европски зелени договор, 2019: 5).

Како би дигитални сектор, допринео климатској неутралности европског континента до 2050. године, Европска комисија посебно потенцира већу

[10] О обновљивим изворима енергије видети детаљније код: Bošnjak, 2020.

[11] Према расположивим подацима, свега 19.7% потрошње енергије потицало је из обновљивих извора енергије у 2019. години. Eurostat (2020). Renewable energy statistics. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Renewable_energy_statistics.

[12] О другој, тамнијој страни медаље обновљивих извора енергије, видети код: Šebalj, 2021.

[13] Видети: European Commission (2019). *Energy and the Green Deal*. Преузето 8. 6. 2021. године. https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/energy-and-green-deal-en.

енергетску ефикасност центара података и телекомуникација, уз искоришћавање енергије из отпада и енергије из обновљивих извора (Изградња дигиталне будућности Европе, 2020: 12).

3. Чиста и циркуларна економија

Стремљење Европске комисије о климатској неутралности европског континента, уграђено у Европски зелени договор, незамисливо је без модернизације економије и њене трансформације из линеарне у кружну економију.

Према постојећем стању ствари, енормни раст екстракције и прераде ресурса одговоран је за губитак више од 90% биолошке разноврсности и несташице воде. Осим тога, и постојећи модел индустријског пословања „ствара" 20% емисија гасова са ефектом стаклене баште (Европски зелени договор, 2019: 6).

Европска комисија, у сузбијању ових негативних тенденција, полази од декарбонизације, модернизације и дигиталне трансформације енергетски интензивних индустрија, попут индустрија: цемента, челика и хемикалија, као и ресурсно интензивних индустрија као што су: грађевинска и текстилна индустрија, сектор производње пластике и електроника.

Европски зелени договор, у процесу стварања одрживе привреде, нарочито рачуна на дигиталне технологије попут: вештачке интелигенције 5 Г технологије, рачунарства у облаку, рачунарства на ивици и интернета ствари (Европски зелени дговор, 2019: 8), које, притом, треба да буду за предузећа, како са енергетског становишта, тако и у погледу коришћења сировина, ефикасније, али и да мање штете животној средини (Дигитални компас 2030., 2021: 3 и 9).

Европска комисија овим правним документом посебно потенцира важност дигитализације код даљинског праћења загађења ваздуха и воде, као и праћења и оптимизације употребе енергије и природних ресурса. Такође, дигитализација је, по схватању Европске комисије, кључна код побољшања доступности информација о својствима производа који се налазе на европском тржишту. У том контексту, Европски зелени договор спомиње могућност увођења електронског пасоша производа који, ако се уведе, треба да садржи податке о пореклу одређеног производа, његовом саставу, могућности поправке и „животном веку" (Европски зелени договор, 2019: 7; Дигитални компас 2030., 2021: 3).

Како би се са успехом спровела дигитална трансформација привреде, Европска комисија инсистра на одрживости самог дигиталног сектора, његовој енергетској ефикасности и успешности циркуларне економије

у његовом окриљу – од широкопојасних мрежа, преко центара података, до опреме коју користе информационе и комуникационе технологије (Изградња дигиталне будућности Европе, 2020: 12). Наравно, успешна дигитална трансформација привреде подразумева отпорност целокупоног механизма информационих и комуникационих технологија на спољне утицаје, попут соларне олује (Geopolitika, 2021).

Европски зелни договор промовише идеју програма враћања и рециклирања застарелих уређаја, попут мобилних телефона, таблета, пуњача и сл., (Европски зелени договор, 2019: 8), као и продужење века трајања свих паметних телефона Изградња дигиталне будућности Европе, 2020: 13). Ово с разлогом, јер уколико би се продужио „живот" свим смарт телефонима за једну годину до 2030. године, то би имало за последицу смањење „производње" 2.1 милиона тона CO_2 на годишњем нивоу (што одговара, примера ради, повлачењу једног милиона аутомобила из промета).[14]

Европска комисија овим правним документом, такође, снажно подржава строжије мере приликом увођења нових мрежа и већу транспарентност процене утицаја електронских комуникационих услуга на животну средину (Европски зелени договор, 2019: 8).

4. Изградња и обнова зграда уз уважавање принципа ефикасне употребе енергије и ресурса

Климатска неутралност, циљ који је установљен Европским зеленим договором, не може бити потпуно остварена без одређеног доприноса који изградња и обнова јавних и приватних зграда може да дâ.

Управо стога, Европска комисија промовише и подстиче изградњу, употребу и обнову јавних и приватних зграда, водећи нарочито рачуна о ефикасној употреби енергије и ресурса (Европски зелени договор, 2019: 8).

Према расположивим подацима, на изградњу или обнову зграда, као и њихову употребу, „одлази" 40% од укупно произведене енергије. Осим великих количина енергије, изградња и обнова зграда „тражи" и знатне количине минералних ресурса, попут цемента, шљунка или песка (Европски зелени договор, 2019: 8). Од зграда, такође, потиче 36% емисија гасова са ефектом стаклене баште.[15] Све то негативно утиче на климу, животно окружење, биолошку разноврсност и здравље људи.

[14] Видети: European Commission (2020). *Supporting the green transition – Shaping Europe's digital future*. Преузето 14. 7. 2021. https://op.europa.eu/en/publication-detail/-/publication/bd211835-5390-11ea-aece-01aa75ed71a1/language-en/format-PDF.

[15] Видети: European Commission. *European Climate Pact, Green buildings.* Преузето 22. 8. 2021. https://europa.eu/climate-pact/about/priority-topics/green-buildings_en.

Идеја је Европске комисије да се постојећа годишња стопа обнове зграда на простору Европске уније од 0.4 до 1.2% (у зависности од државе, чланице) дуплира до 2030. године. Такође, иницијатива овог тела је да се пројектовање зграда врши у складу са принципима кружне економије, као и да се граде „паметне" зграде које ће функционисати на темељу најновијих дигиталних технологија (Европски зелени договор, 2019: 7–8). Европска комисија сугерише градњу и обнову зграда уз уважавање принципа веће отпорности зграда на климатске промене, попут поплава и великих врућина.[16]

5. Одржива и паметна мобилност

Стварање Европе као климатски неутралног континента, поред осталог, подразумева и прелазак на паметан и одржив транспорт.

Према проценама, транспорт је „кривац" за 1/4 укупне емисије гасова са ефектом стаклене баште. Од тога, друмски превоз производи 71.7% гасова са ефектом стаклене баште, ваздушни 13.9%, водени 13.4%, а железнички транспорт 0.5% и остале врсте превоза 0.5%.[17]

Европски зелени договор предвиђа 90% смањење емисија гасова са ефектом стаклене баште, проистеклих из транспорта, до 2050. године (Европски зелени договор, 2019: 9).

Европска комисија, са циљем смањења штетних ефеката транспорта на здравље људи, животну средину и биолошку разноврсност, потенцира железнички и водени превоз, уместо друмског саобраћаја и залаже се за јачање мултимодалне мобилности, опремљене дигитализацијом. Наравно, Европска комисија тиме не затвара пут друмском транспорту, али јасно сугерише његово „преобликовање" које би у себи укључивало повећану производњу и употребу одрживих алтернативних горива у транспорту.[18] Осим тога, Европски зелени договор промовише аутоматизацију транспортних система који укључују паметне механизме управљања, способне да „подрже нове моделе одрживе мобилности" (Европски зелени договор, 2019: 10), а све са циљем: побољшања превоза, посебно у градским сре-

[16] Исто.

[17] Видети: European Commission (2019). *Statistical pocketbook. EU Transport*, 135. Преузето 12. 7. 2021. године. https://ec.europa.eu/transport/facts-fundings/statistics/pocketbook-2019_en.

[18] Европски зелени договор предвиђа да до 2025. године, на простору Европске уније, буде постављено око милион јавних станица за пуњење тринаест милиона возила са нултим или ниским емисијама гасова са ефектом стаклене баште. Видети: European Commission (2019). *Sustainable transport*. Преузето 20. 8. 2021. године, https://ec.europa.eu/transport/themes/sustainble_en.

динама, смањења саобраћајног загушења и загађења. У том контексту, Европска комисија предлаже увођење 5 Г коридора за повезану и аутоматизовану мобилност, за период од 2021. до 2030. године, као и 5 Г железничке коридоре, за период од 2021. до 2023. године (Изградња дигиталне будућности Европе, 2020: 7). Процена Европске комисије је да квалитативан помак у правцу одрживе и паметне мобилности треба да буду и дигитално осмишљене апликације, као и решења „мобилност као услуга”, која би допринела смањењу броја саобраћајних несрећа и побољшању ефикасности транспортних система (Европски зелени договор, 2019: 10; Дигитални компас 2030., 2021: 10). Европска комисија се такође, у циљу смањења ваздушних емисија гасова са ефектом стаклене баште залаже за реформу јединственог европског неба.[19]

6. Успостављање праведног, здравог и еколошки прихватљивог прехрамбеног система

План Европске комисије, да до 2050. године постигне климатску неутралност европског континента, незамислив је без трансформације постојећег начина производње хране, њене прераде, паковања, превоза, дистрибуције и потрошње – једном речју прехрамбеног система.

Постојећи прехрамбени систем негативно утиче на животно окружење, биолошку разноврснот, квалитет живота и животни век људи (Европски зелени договор, 2019: 11) Он, у исто време, исцрпљује велике количине природних ресурса, у знатној мери загађује ваздух, земљиште и воду и притом доприноси стварању значајних емисија гасова са ефектом стаклене баште. Процене говоре, да 10.3% укупне емисије гасова са ефектом стаклене баште на подручју Европске уније потичу од пољопривреде, а од тога, чак 70% је „заслужно” сточарство.[20] Такође, истраживања показују да и расипање хране[21] на европском простору „доприноси” емисијама гасова са ефектом стаклене баште око 6% (Stenmarck, et al., 2016).

[19] Видети: European Commission (2019). *Sustainable transport*. Преузето 20. 8. 2021. године, https://ec.europa.eu/transport/themes/sustainble_en.

[20] Известан помак, који је учињен у погледу смањења емисије гасова са ефектом стаклене баште, у домену пољопривреде Европске уније, за 21%, од 1990 до 2018. године, чини се да ни изблиза није довољан да се избегне штетан утицај прехрамбеног система на климатске промене. Наведено према: European Environment Agency, 2019.

[21] Забрињавајуће делује податак да су потрошачи на глобалном нивоу, рецимо у 2019. години бацили преко девесто тридесет милиона тона хране, или, по глави становника у свету, просечно 74 кг хране. С друге стране, шесто деведесет милиона људи је те исте године било гладно, а око три милијарде људи није могло себи да обезбеди здраву храну. Видети: UNEP, 2021: 4 и 20.

Европски зелени договор предвиђа, са циљем преласка на праведан, здрав и еколошки прихватљив прехрамбени систем, увођење читавог низа одрживих пракси, попут: органске пољопривреде, агроекологије, агрошумарства и строжијих стандарда у поступању са животињама (Европски зелени договор, 2019: 11).

Овим правним документом, и његовом Стратегијом „од њиве до трпезе",[22] заговарају се и примена дигиталних технологија у пољопривредно-прехрамбеном сектору. Њихова примена се посебно везује за прецизну (сателитску) пољопривреду[23] (Европски зелени договор, 2019: 11; Стратегија „од њиве до трпезе", 2020: 16).[24] [25]

Европска комисија снажно подржава и увођење, у руралним подручјима брзог, широкопојасног интернета, најкасније до 2025. године, који ће омогућити примену прецизне пољопривреде, али и вештачке интелигенције. По схватању ове Комисије, бенефити увођења брзог и поузданог интернета у сеоским срединама су више него видљиви: мањи трошкови за пољопривреднике, током производног процеса, боље управљање земљиштем, квалитетнија вода, употреба мање количине ђубрива и пестицида, смањене емисије гасова са ефектом стаклене баште, и побољшање биолошке разноврсности и стварање здравијег животног окружења (Стратегија „од њиве до трпезе", 2020: 16)

7. Закључна разматрања

Извесно је да дигиталне технологије представљају значајан фактор у зеленој трансформацији привреде и друштва, јер могу: помоћи у декарбо-

[22] European Commission (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *A Farm to Fork Strategy. For a fair, healthy and environmentally-frendly food system*. Преузето 10. 6. 2020. године. https://www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0381.

[23] Ради се о таквом управљања пољопривредом који, посредством дигиталних техника, посматра, мери и анализира потребе одређених земљишних парцела и усева, утичући, на тај начин, на смањење емисија гасова са ефектом стаклене баште и прекомерну употребу пестицида.

[24] О разлици између прецизне пољопривреде, паметне пољопривреде и дигиталне пољопривреде, видети код: Vukadinović, 2020.

[25] Дигитални компас 2030. заговара и примену паметне пољопривреде, која у себи укључује прикупљање података за потребе пољопривредних газдинстава, али и пружање напредних услуга пољопривредним произвођачима, попут предвиђања жетве, управљања пољопривредним газдинством и побољшања ланца снабдевања храном (Дигитални компас 2030., 2021: 8).

низацији енергетског и других сектора у привреди; унапредити кружну економију; омогућити аутоматизацију транспортних система и паметно управљање прометом; допринети изградњи паметних зграда; обезбедити развој прецизне пољопривреде и сл.

Питање је у којој мери могу бити остварени постављени циљеви, утолико више што је сам дигитални сектор велики потрошач електричне енергије и произвођач емисија гасова са ефектом стаклене баште. Од не мањег значаја је и чињеница да сектор информационих и комуникационих технологија може бити, у приличној мери, осетљив, рецимо, на соларне олује јаког интензитета.

Оно што посебно треба да забрињава јесте што последице примене дигиталних технологија на животну средину, биодиверзитет, здравље и животни век људи још нису довољно испитане, а оно што је испитано, како смо видели, далеко од тога да не штети свим овим вредностима. Реална је опасност да њихова примена у будућности можда, уместо да користи, заправо више штети остварењу циљева Европског зеленог договора.

Литература

Bošnjak, I. (2020). *OIE – Energija budućnosti. Industrija.* Преузето 12. 8. 2021. https://www.industrija.rs/vesti/clanak/oie-energija-buducnosti.

Vukadinović, V. (2020). *Koja je razlika između precizne, pametne i digitalne poljoprivrede?* (Elektronska verzija). Преузето 24. 7. 2021. године. http://tlo-i-biljka.eu>GnojidbaPDF.

Geopolitika (2021). *Zemlji prijeti internetska apokalipsa zbog solarne oluje.* Преузето 10. 9. 2021. године. https://vijesti.hr/zemlji-prijeti-internetska-apokalipsa-zbog-solarne-oluje/.

European Environment Agency (2019). *Annual European Union greenhouse gas iventory 1990–2017 and inventory report,* EEA/PUBL/2019/051. Преузето 18. 8. 2021. https://eea.europa.eu/publications/eu/european-union-greenhouse-gas-inventory-2019.

European Commission (2019). *Energy and the Green Deal.* Преузето 8. 6. 2021. године. https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/energy-and-green-deal-en.

European Commission. *European Climate Pact. Green buildings.* Преузето 22. 8. 2021. https://europa.eu/climate-pact/about/priority-topics/green-buildings_en.

European Commission (2019). *Statistical pocketbook. EU Transport*. Преузето 12. 6. 2021. године. https://ec.europa.eu/transport/facts-fundings/statistics/pocketbook-2019_en.

European Commission (2020). *Supporting the green transition – Shaping Europe's digital future.* Преузето 14. 7. 2021. https://op.europa.eu/en/publication-detail/-/publication/bd211835-5390-11ea-aece-01aa75ed71a1/language-en/format-PDF.

European Commission (2019). *Sustainable transport*. Преузето 20. 8. 2021. године, https://ec.europa.eu/transport/themes/sustainble_en.

European Commission (2020). *Shaping Europe's digital future*. Преузето 12. 7. 2021. године. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en.

European Commission (2021). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *2030 Digital Compass: the European way for the Digital Decade*. Преузето 20. 6. 2021. године. https://www.eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.

European Commission (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *A Farm to Fork Strategy. For a fair, healthy and environmentally-frendly food system*. Преузето 10. 6. 2020. године. https://www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0381.

European Commission (2020). Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. *Shaping Europe's digital future.* Преузето 18. 6. 2021. године. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:67:FIN.

European Commission (2019). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. *The European Green Deal*. Преузето 20. 1. 2020. године. https://www.eur-lex.europa.eu/legal-content/EN/TXT/?qid=1588580774040&uri=CELEX:52019DC0640.

Eurostat (2020). *Renewable energy statistics*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Renewable_energy_statistics.

Popov, V. (2017). *Informatizacija, digitalizacija i digitalna transformacija*. Преузето 10. 9. 2021. године. https://startit.rs/informatizacija-digitalizacija-i-digitalna-transformacija-u-cemu-su-razlike.

Stenmarck, A., Jensen C., Quested T., Moates G., et al., (2016). *EU FUSIONS, Estimates of European food waste levels*. Преузето 28. 12. 2020. https://www.eu-fusion.org.

United Nations Environment Programme,UNEP, (2021). *Food Waste Index Report.* Преузето 10. 9. 2021. године. https://www.unep.org/resources/report/unep-food-waste-index-report-2021.

Šebalj, A. (2021). *Obnovljivi, zeleni izvori – golemi biznis*. Преузето 23. 8. 2021. https://www.logicno.com/politika/obnovljivi-zeleni-izvori-golemi-biznis.html.

Nataša Stojanović, LL.D.
Full Professor,
Faculty of Law, University of Niš,
Serbia

EUROPEAN GREEN DEAL - ROADMAP TO A GREEN AND DIGITAL TRANSFORMATION OF THE EUROPEAN UNION ECONOMY AND SOCIETY

Summary

The European Union, as well as the entire international community, has been faced with the climatic changes, enormous loss of biodiversity, big air, water and soil pollution, etc., for decades now. A significant portion of the "guilt" for such a situation belongs to uncontrolled gas emissions with greenhouse effect that occur in the process of production and use of energy, based on goal and natural gas; then in linear economy where economic growth is conditioned with a big consumption of resources; and again, "production" of big quantities of waste; in road traffic, which is more represented in practice comparing to railway or inland waterway transportation, and connected therewith, almost regularly, traffic congestion; but also in the production and consumption of food. A special problem is a relatively low rate of renovation of private and public buildings that would enable their better energy efficiency. In order to resolve a clearly visible disbalance between economy and environment, the European Commission prepared and presented the European Green Deal to the public on December 11, 2019. With this legal act, the European Union continues, indeed more powerful and comprehensively, the already started transformation and modernisation of its economy, with a goal of achieving climatic neutrality by 2050. The European Union, in the implementation of this ambitious and complex goal, especially counts on digital innovations and digital technologies. In the paper, the author focuses her attention precisely to solutions offered by the European Green Deal and EU Digital Strategy in regard to green and digital transformation of economy and society of the European Union with a goal to assert their meaning and reach regarding the creation of a climate-neutral European continent.

Keywords: *European Green Deal, green transformation of economy and society, digitalization.*

Др Милица Вучковић,
Доцент,
Правни факултет Универзитета у Нишу,
Србија

UDK: 347.121.2

ГРАЂАНСКОПРАВНА ЗАШТИТА ОД НЕОВЛАШЋЕНОГ КОРИШЋЕЊА ЛИЧНИХ ДОБАРА У КОМЕРЦИЈАЛНЕ СВРХЕ[1]

Апстракт: *Неовлашћено коришћење личних добара у комерцијалне сврхе у упоредном праву је познато као феномен комерцијалне апропријације личности (commercial appropriation of personality). Овој правној појави се првенствено приступа са аспекта права интелектуалне својине и облигационоправног института неоснованог обогаћења, при чему се репарација, односно поправљање материјалне штете, показује довољном сврхом имовинске санкције. Проблеми у правној теорији, законодавствима и пракси настају приликом покушаја да се комерцијалној апропријацији личних добара приђе из правца грађанскоправне заштите личности од наношења нематеријалне штете. У овом раду истражујемо та спорна питања, постојеће одговоре, покушаје одговора на њих и могућа решења.*

Кључне речи*: права личности, нематеријална штета, комерцијално искоришћавање личних добара.*

1. Увод

Термин *комерцијална апропријација личности* говори доста о институту који је предмет овог истраживања, али ипак тек на његовој површини. Ради се о неовлашћеном експлоатисању туђих личних добара, која према класификацији грађанског права представљају објекат права личности, и то како у њиховом најнепосреднијем виду, као саставних делова личности (нпр. неовлашћено снимање нечијег гласа или лика и комерцијално искоришћавање тако добијеног снимка), тако и у виду опредмећеног израза личности (неовлашћено комерцијално искоришћавање туђег видео или тонског записа). Тај правни феномен и правни проблем се првенствено од-

[1] Рад је резултат истраживања на пројекту *Одговорност у правном и друштвеном контексту,* који финансира Правни факултет Универзитета у Нишу, за период 2021-2025.

носи на јавне личности из различитих сфера (културе, политике, спорта, забаве) које иначе добровољно деле са другима поједина овлашћења поводом својих личних добара за новац, у ситуацијама када неко, ради постизања добити, врши те поједине прерогативе без икаквог правног основа. Чинило се у почетку да ће тај институт припасти праву интелектуалне својине. И то је била та површина. Отишло се много дубље од тога. Он се по својим суштинским карактеристикама, које се чак нису ни дефинитивно оформиле, посматрано из глобалне упоредноправне перспективе, налази негде на граници између права интелектуалне својине и грађанског права, и то његове врло осетљиве, неравномерно развијене гране права, права личности. У оквиру права личности, централни појам који ову грану чини местом размимоилажења од првих дана, јесте сатисфакција, као специфичан циљ имовинске санкције због повреде доминантно нематеријалних правних објеката, личних добара. Институт који је предмет нашег истраживања завређује пажњу због настојања правника да се уважи и тај вид грађанскоправне заштите личности, заштита од наношења нематеријалне штете.

У раду ћемо најпре покушати да дамо једну радну дефиницију појма комерцијалне апропријације личности. Након тога ћемо се бавити упоредноправном анализом овог проблема, да бисмо на самом крају истражили могућности грађанског права Републике Србије да да одговор на овај правни проблем.

2. Скица правног феномена неовлашћеног комерцијалног искоришћавања личних добара

Под неовлашћеним комерцијалним коришћењем личних добара подразумевамо појаву неовлашћеног коришћења или искоришћавања одређених личних добара једне особе (гласа, лика, имена или компоненти приватног живота) без њене сагласности, у реклами, трговачкој кампањи, средствима јавног информисања или на други начин погодан за то да се широј јавности саопште одређени садржаји, ради постизања добити.

Лична добра која су у пракси најчешће предмет неовлашћеног лукративног посезања су име, глас, лик и приватни живот. У правној теорији се засебно разматрају право на име, право на сопствену слику, право на глас и право на приватни живот (Finžgar, 1988: 105, 117, 133,139) али се право на сопствени лик, право на сопствени глас, заједно са правом на личну преписку, изучава и у оквиру шире конципираног права на приватност (Gavella, 2000: 211-216).

Право на име је право једног лица да се служи одређеним личним именом, да сваког трећег искључи из употребе његовог имена и да од трећих лица захтева да га називају тим именом (Finžgar, 1988: 106).

Право на сопствени лик је право личности које овлашћује титулара на слободно уживање свог лика, као засебног личног добра, у смислу искључења сваког трећег лица од захвата у овај атрибут личности, и самосталног и слободног одлучивања о објављивању и искоришћавању његове слике, отеловљене у снимку, фотографији, статуи, бисти, слици, графици, плакату итд (Finžgar, 1988: 119-120, Gavella, 2000: 251-252).

Право на глас је право на уживање свог гласа и искључиво искоришћавање добровољно снимљеног тонског записа гласа, и право личности да се супротстави сваком неовлашћеном и тајном снимању његовог гласа, као и свим видовима комерцијалног и некомерцијалног искоришћавања тако добијеног тонског записа (Finžgar, 1988: 133-138, Gavella, 2000: 259).

Право на приватност може се посматрати у ширем и у ужем смислу. Право приватности у ужем смислу је право личности да свој интимни, породични и кућни, као и приватни живот у јавном простору, води засебно, у складу са сопственим потребама, вредностима и жељама и неометано од стране трећих неовлашћених лица. Право на приватност у ширем смислу обухвата право приватности у ужем смислу, проширено компонентом заштите права на лик, глас и тајност записа и преписке (Gavella, 2000: 211-214).

Неки од примера неовлашћеног комерцијалног искоришћавања туђих личних добара су: неовлашћено коришћење имена и слике познатог глумаца у реклами за „такмичење у популарности" познатог дневог листа[2], неовлашћено објављивање фотографија и биографије истраживача непознатог за живота, након његове смрти[3], коришћење имена и слике познатог адвоката и политичара на реклами за цигарете[4], неовлашћено објављивање имена, праћено лажном изјавом, у реклами за животно осигурање[5], коришћење фотографије познатог фудбалера, активисте против конзумирања алкохола, у реклами за пиво[6], неовлашћено објављивање фотографија са интервјуом о болничком опоравку познатог глумца након тешке саобраћајне незгоде, при чему је интервју добијен када је био

[2] *Marks v. Jaffa,* 6 Misc. 290, 26 N.Y.S. 908 (N.Y. Misc. 1893).

[3] *Collis v. Walker*, 272 Mass. 46, 172 N.E. 228 (Mass. 1930).

[4] *Atkinson v. John E. Doherty & Co,* 121 Mich. 372, 80 N.W.. 285 (1899).

[5] *Pavesich v. New England Life Ins. Co.*, 122 Ga. 190 (Ga. 1905).

[6] *O'Brien v. Pabst Sales Co*. - 124 F.2d 167 (5th Cir. 1941).

у полусвесном стању, а фотографије су узимане на препад[7], неовлашћено објављивање неовлашћено снимљених фотографија са венчања познатих глумаца[8], објављивање фиктивног интервјуа са принцезом[9], неовлашћено објављивање тајно снимљених фотографија принцезе током приватних активности као што су шопинг, јахање, вожња бицикле итд.[10], коришћење фотографије девојке на амбалажи за брашно[11], коришћење фотографије дечака у реклами за накит[12], новлашћено објављивање на блогу снимка пореског инспектора на послу[13], коришћење фотографије плесачице на паковању за шећер[14].

Правни приступ може бити двојак, са становишта права интелектуалне својине, које је усмерено на заштиту економских интереса, и са становишта грађанског права, којим се може обезбедити заштита и материјалних и нематеријалних интереса (Beverly-Smith, 2004: 23-24). У највећем броју ових случајева ради се о заштити личних добара о којима смо говорили. Атрибут *неовлашћено* указује да је наш правни проблем једна од других страна медаље. Име, глас и лик су од прве појаве масовних медија били извор зараде, а у новије време, све учесталији „рудник блага” јесте и приватни живот, који се у изворном или модификованом облику приказује публици за велику зараду[15]. Из тих разлога се овај институт нашао растрзан између права интелектуалне својине и грађанског права. Отвориле су се и нове перспективе, хибридних права, која представљају идеју имовинских интереса у сопственој личности. Док је развој права личности ишао трновитим путем, управо због проблематичне синтагме *право над самим собом*, развој тржишта, медија и права наметнули су другачију перцепцију личности и њеног самоодређења. Један од главних проблема у оквиру формирања и развијања личних права јесте и право накнаде нематеријалне штете. Већина правних система је проблем накнаде материјалне штете решавала лако, без проблема у утемељивању правног резона у праву интелектуалне својине или у грађанском праву. Остваривање захтева за

[7] *Kaye v. Robertson* [1990] EWCA Civ 21.

[8] *Douglas v. Hello! Ltd* (2005) EWCA Civ 595.

[9] Rechtsprechung BGH, 15.11.1994 - VI ZR 56/94.

[10] Rechtsprechung BGH, 19.12.1995 - VI ZR 15/95.

[11] *Roberson v. Rochester Folding Box Co.*, 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902).

[12] *Munden v. Harris*, 153 Mo. App. 652 (Mo. Ct. App. 1911).

[13] Cour de cassation, civile, Chambre civile 1, 15 janvier, 2015., 13-25.634.

[14] Cour de cassation, civile, Chambre civile 1, 5 avril, 2012., 11-15.328.

[15] https://www.britannica.com/topic/reality-show, https://en.wikipedia.org/wiki/The_Osbournes, https://www.eonline.com/shows/kardashians.

накнаду нематеријалне штете није једнако у третману са захтевом за накнаду материјалне штете.

3. Упоредноправни преглед

У *англоамеричком праву* историјски је запажена тенденција да се проблему апропријације личности приступа са становишта права интелектуалне својине, или из шире перспективе трговачког права. Постоје нијансиране разлике, пре свега између америчког права и права Велике Британије. У америчком праву је за решавање случајева повреде материјалних интереса блиских правима интелектуалне својине осмишљено специјално хибридно лично право интелектуалне својине, право публицитета (Dogan, Lemley, 2006: 1162-1166). Ово право омогућава славним личностима које остварују профит од својих личних добара да контролишу њихову комерцијалну експлоатацију. С друге стране, право приватности добило је врло значајно место у америчком правном систему, чиме је омогућено да и познате и непознате личности, чија су лична добра неовлашћено коришћена у лукративне сврхе од стране трећих лица, постигну забране такве повреде правно заштићене сфере њихове индивидуалности, повраћај у пређашње стање, у мери у којој је могуће тим путем поправити последице повреде, и накнаду претрпљене неимовинске штете. У праву Велике Британије судови се држе конзервативног схватања права приватности, што отежава остваривање захтева за накнаду нематеријалне штете. По правилу се ослањају на познате деликте одштетног права, и уколико није могуће уклапање чињеничног стања у те оквире, оштећеном је готово немогуће да оствари заштиту, наравно ако се не ради о заштити материјалних интереса везаних за комерцијално искоришћавање личних добара. Право приватности, као посебна основа за заштиту у оваквим случајевима, теже се и спорије развија у односу на америчко право. У новије време се говори о будућем развоју права приватности под утицајем Европске конвенције и Human Rights Act-a из 1998. године (Beverly-Smith, 2004: 214-224).

У *немачком праву* постоји опште право личности, као судска творевина настала кроз примену индиректног хоризонталног дејства уставних одредаба о заштити личности. Грађанскоправна заштита права личности заснива се на двема одредбама BGB-a, које су истовремено и главни стубови одштетног права у Немачкој. Поред општег права личности, постоје и посебним прописима регулисана право на име и право на слику. Параграф 823 представља први стуб немачког одштетног права и грађанскоправне заштите личности. Први став овог параграфа нормира да је свако ко намерним или нехатним противправним чином повреди нечији живот,

тело, здравље, слободу, својину или било које друго право једне личности, дужан да му накнади сву штету проузроковану том повредом, док је у другом члану истог параграфа предвиђена иста таква обавеза за сваког ко прекрши законску одредбу намењену заштити личности. Други стуб грађанскоправне заштите личних права садржан је у одредби § 826 BGB -а, који нормира да је свако ко на начин супротан јавном поретку намерно нанесе штету другом, дужан да ту штету надокнади. Право на слику регулисано је у § 22 и § 23 Закона о ауторском праву на делима визуелне уметности – Kunsturheberrechtsgesetz – KUG, а право на име у § 12 BGB -а. У Закону о ауторском праву на делима визуелне уметности предвиђено је да се портрети личности могу објављивати и дистрибуирати само уз сагласност оног о чијем се лику ради. Изузеци од овог правила су могући у таксативно наведним случајевима, који се односе на личности из сфере савремене историје, личности које су случајно снимљене као делови пејзажа или неке локације, на фотографије окупљања, процесија и сличних активности у којима су портретисане личности учествовале, и у случајевима портрета који нису прављени по наруџбини, ако њихово излагање или дистрибуирање служи вишим уметничким циљевима и интересима. Ипак, ни ови изузеци не важе у случају повреде оправданог интереса портретисане личности, или, уколико је та особа преминула, интересима њених сродника. Када је реч о праву на име, у § 12 BGB -а је предвиђено право сваког да се супротстави повреди или угрожавању свог права на име.

Грађанскоправна заштита личности од неовлашћеног комерцијалног искоришћавања у немачком праву се остварује применом општих правила о грађанскоправној заштити личности. У овом случају, реч је о аналогној примени §1004 BGB -а, који се односи на заштиту права својине од узнемиравања[16]. У овом параграфу је нормирано да власник ствари има право да, уколико је право својине сметано на неки другачији начин од одузимања државине, захтева уклањање сметњи, а уколико се то не може постићи, може захтевати престанак активности од које потиче узнемиравање. Услов за успех овог тужбеног захтева јесте доказ постојања узнемиравања. Узнемиравање треба да буде противправно, односно без правног основа, неовлашћено, али се то не доказује. Онај ко врши сметање мора доказати да је на то овлашћен неком правном нормом. Не захтева се ни доказ, односно постојање кривице. Поред захтева за престанак радње којом се повређује право личности, може се тражити и повраћај у пређашње стање, што би у случају комерцијалног искоришћавања личности могло бити нпр.,

[16] У немачком праву је могуће да се примена једне законске одредбе прошири по аналогији на случајеве на које се она не односи непосредно, ако је неспорно да законска празнина није била намерна (Beverly-Smith, Onty, Schloeter, 2005:138).

уништење примерака новина, магазина, плаката, паковања робе на ком се налази фотографија оштећеног, уклањање видео снимака са блога итд (Beverly-Smith, Onty, Schloeter, 2005: 139). Јако устаљено средство заштите по овом параграфу јесте објављивање пресуде, односно корективе изјаве, уколико је право повређено приписивањем неистинитих исказа одређеној личности (Beverly-Smith, Onty, Schloeter, 2005: 139).

По одредбама § 823 BGB -а може се тражити и накнада штете. Ове одредбе се, међутим, односе на материјалну штету, док се захтев за накнаду нематеријалне штете може заснивати на § 847 BGB -а, која предвиђа право лица на накнаду неимовинске штете у случајевима повреде тела или здравља, или у случају неоснованог притварања. Судови примењују ову одредбу по аналогији и на случајеве повреде других права личности, уз констатацију да се повреда личних права може третирати као повреда интелектуалне слободе (Beverly-Smith, Onty, Schloeter, 2005: 144). Такође, судови у Немачкој додељују накнаду нематеријалне штете због повреде права личности позивањем на индиректно хоризонтално дејство чланова 1 и 2 Устава[17].

У *француском праву* постоји врло ефикасна и либерална грађанскоправна заштита личности од неовлашћене лукративне експлоатације, заснована на некадашње чувеном чл. 1382 C.civ., сада члану 1240., који представља главни стуб опште одговорности за штету у грађанском праву (Beverly-Smith, Onty, Schloeter, 2005 :150): „Ко другом проузрокује штету својом кривицом дужан је да је накнади." О ингениозности оваквог приступа прилично говори један цитат из компаративне правне теорије: „Очигледно је да један правни систем може усвојити врло флексибилан приступ проблему заштите људске личности, ако се његово одштетно право примењује на заштиту свих правних интереса (супротно § 823 BGB), и уколико се у њему врло слободно може досудити и накнада нематеријалне штете (супротно §§ 253, 847б BGB). Француски судови никада нису оклевали да квалификују као *faute* (кривицу) објављивање поверљивих писама, дистрибуирање чињеница о нечијем приватном животу, или неовлашћено

[17] ***Article 1 [Human dignity – Human rights – Legally binding force of basic rights]***:(1) Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority. (2) The German people therefore acknowledge inviolable and inalienable human rights as the basis of every community, of peace and of justice in the world. (3) The following basic rights shall bind the legislature, the executive and the judiciary as directly applicable law. ***Article 2 [Personal freedoms]***: (1) Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law. (2) Every person shall have the right to life and physical integrity. Freedom of the person shall be inviolable. These rights may be interfered with only pursuant to a law.

коришћење нечијег имена, и да оштећеном досуде накнаду моралне штете подједнако као и накнаду материјалне штете (Zweigert, Kotz, 1987: 733).

Када је реч о заштити личних права, класични услови одговорности (кривица, штета и узрочна веза) прилично су релаксирани. С. civ. регулише у чл. 9 право на поштовање приватног живота[18], а судови су креирали и право на име и право на слику. Ова права су грађанска субјективна права, тако да сама чињеница њихове повреде представља кривицу (Beverly-Smith, Onty, Schloeter, 2005: 167). Поред поменутог права на накнаду и материјалне и нематеријалне штете, у случају повреде права личности, сама чињеница повреде оправдава сваку меру усмерену на престанак и спречавање понављања повреде: суд може у сумарном поступку (Lindon, 1985: 61) наложити сваку меру, попут секвестрације, заплене и осталих мера подобних да спрече, односно окончају повреду интимности приватног живота[19]. Те мере могу бити нпр. уништење фотографије, уклањање изјаве и фотографије са интернет стране, предузимање мера да се лице оштећеног не може разазнати на снимку или фотографији итд (Beverly-Smith, Onty, Schloeter, 2005: 183).

Можемо приметити да се успешност захтева за накнаду нематеријалне штете креће на скали од најмање уважености, због тешкоћа у превазилажењу оквира постављених постојећим деликтима одштетног права и темељних начела правног система, у енглеском праву, преко средње лаке остваривости у америчком и немачком праву, до потпуно отвореног и либералног приступа у француском праву.

4. Грађанскоправна заштита од неовлашћеног комерцијалног коришћења личних добара у праву Републике Србије

У праву Републике Србије може се говорити о општој и посебној грађанскоправној заштити личности, при чему не постоје сметње за примену тих норми у пољу заштите од неовлашћеног комерцијалног искоришћавања личних добара. Општа заштита управља се према одредбама Закона о облигационим односима (ЗОО)[20], а посебна је, моделирана према посебно заштићеним сферама испољавања материјалних и нематеријалних инте-

[18] „Свако има право на поштовање свог приватног живота. Суд може, без утуцаја на право на накнаду претрпљене штете, наложити све мере, као што су секвестрација, заплена и друге мере, погодне да се спречи или прекине повреда интимности приватног живота. Ове мере се у случају хитности могу наложити и у сумарном поступку."

[19] Art. 9 C. Civ., https://www.legifrance.gouv.fr.

[20] *„Сл. лист СФРЈ"*, бр. 29/78, 39/85, 45/89 – одлука УСЈ и 57/89, *„Сл. лист СРЈ"*, бр. 31/93, *„Сл. лист СЦГ"*, бр. 1/2003 – Уставна повеља и *„Сл. гласник РС"* бр. 18/2020.

реса личности, уређена бројним посебним прописима из области јавног информисања, заштите од дискриминације, медицинског права итд (Симоновић, Лазић, 2014: 274). Одредбама ЗОО регулисано је право на новчану накнаду материјалне и нематеријалне штете због повреде права личности и посебни видови натуралне реституције у одређеним случајевима повреде[21]. У ЗОО је прихваћен, при уређивању новчане накнаде нематеријалне штете, њен субјективни појам, по ком се нематеријалном штетом не сматра сама повреда личног права, већ тек последице те повреде, исказане кроз физички и душевни бол, страх и осећање наруженості, па је предвиђено да ће суд досудити правичну новчану накнаду за претрпљене физичке и душевне болове и страх у случајевима умањења животне активности, наруженості, повреде угледа, части, слободе или права личности, уколико утврди да је то оправдано с обзиром на интензитет и трајање болова и страха (Радованов, 2010: 25-33). Међутим, када су у питању специфични облици натуралне реституције, очигледан је печат ширег схватања овог појма, објективног, по ком повреда личног права сама по себи чини нематеријалну штету. Тако је предвиђено да суд може наредити објављивање пресуде или исправке, односно повлачење изјаве којом је повреда учињена, односно нешто друго чиме се може остварити сврха која се постиже накнадом[22], (Симоновић, Лазић, 2014: 282-283). Ово су видови поствентивне (накнадне) заштите права личности, док се превентивна грађанскоправна заштита од неовлашћеног комерцијалног искоришћавања личности може остварити позивањем на одредбе чланова 156 и 157 ЗОО. Свако може захтевати уклањање извора опасности од ког прети знатнија штета њему или неодређеном броју лица и уздржавање од делатности од које потиче узнемиравање или опасност штете, ако се настанак узнемиравања или штете не може спречити одговарајућим мерама[23]. Свако има право да захтева престанак радње којом се повређује интегритет људске личности, личног и породичног живота и других права његове личности[24].

Посебна грађанскоправна заштита од неовлашћеног комерцијалног искоришћавања личних добара може се остваривати по одредбама Закона о јавном информисању и медијима[25]. Њима је предвиђено да се информа-

[21] Чл. 156, 157, 199, 185-198 и 200-205 ЗОО. *„Сл. лист СФРЈ”,* бр. 29/78, 39/85, 45/89 – одлука УСЈ и 57/89, *„Сл. лист СРЈ”,* бр. 31/93, *„Сл. лист СЦГ”,* бр. 1/2003 – Уставна повеља и *„Сл. гласник РС”* бр. 18/2020.

[22] Чл. 199 ЗОО. *„Сл. лист СФРЈ”,* бр. 29/78, 39/85, 45/89 – одлука УСЈ и 57/89, *„Сл. лист СРЈ”,* бр. 31/93, *„Сл. лист СЦГ”,* бр. 1/2003 – Уставна повеља и *„Сл. гласник РС”* бр. 18/2020.

[23] Чл. 156, ст. 1 ЗОО.

[24] Чл. 157, ст. 1 ЗОО.

[25] *„Сл. гласник РС”,* бр. 83/2014, 58/2015 и 12/2016 – аутентично тумачење.

ција из приватног живота, лични записи, као што су писма, дневници и сл., записи нечијег лика, попут фотографије, филмског записа или цртежа, и записи нечијег гласа (магнетофонски, грамофонски, дигитални), могу објавити само уз пристанак лица чија су лична добра у питању, односно, у случају смрти тог лица, уз пристанак његових сродника[26]. Предвиђене су и посебне тужбе за објављивање одговора и исправке, уколико се ради о информацијама којима се може повредити право или интерес одређене личности, односно ако је право личности повређено неистинитом, непотпуном или нетачно пренетом информацијом[27].

Регулисана је и садржина тужбеног захтева у случајевима повреда претпоставке невиности, забране говора мржње, права и интереса малолетника, забране јавног излагања порнографског садржаја, права на достојанство личности, права на аутентичност и права на приватност, објављивањем информације или записа. У таквим случајевима тужбом се може захтевати утврђење да је објављивањем информације или записа повређено право или интерес, пропуштање објављивања и забрана поновног објављивања информације или записа и предаја записа, уклањање и уништење записа[28]. Предвиђена је и могућност изрицања привремене мере забране поновног објављивања исте информације или записа до правноснажног окончања поступка[29].

Када је реч о праву Републике Србије и његовом приступу питању накнаде нематеријалне штете, законско нормирање даје могућност за флексибилнији приступ, сличан француском праву. У чл. 200, ст. 1 ЗОО дата је формулација која омогућава слободније поступање судова по захтевима за накнаду нематеријалне штете. Овде је предвиђено право на накнаду нематеријалне штете за претрпљене физичке и душевне болове и за страх, између осталих набројаних случајева, и посебно у случају повреде права личности. Питање је само како ће се судови опредељивати, будући да је Закон о јавном информисању и медијима могуће схватити као специјалан закон у грађанскоправној заштити личности од неовлашћеног комерцијалног искоришћавања. Но, како за сада не постоји пажње вредан

[26] Чл. 80, ст. 1 и чл. 81, ст. 1. Закона о јавном информисању и медијима *„Сл. гласник РС"*, бр. 83/2014, 58/2015 и 12/2016 – аутентично тумачење.

[27] Чл. 83, ст. 1 и чл. 84, ст. 1. Закона о јавном информисању и медијима *„Сл. гласник РС"*, бр. 83/2014, 58/2015 и 12/2016 – аутентично тумачење.

[28] Чл. 101. Закона о јавном информисању и медијима *„Сл. гласник РС"*, бр. 83/2014, 58/2015 и 12/2016 – аутентично тумачење.

[29] Чл. 104. Закона о јавном информисању и медијима *„Сл. гласник РС"*, бр. 83/2014, 58/2015 и 12/2016 – аутентично тумачење.

корпус судске праксе у овој материји, све остаје само на пољу нагађања и, евентуално, претпоставки.

5. Закључак

Комерцијално коришћење личних добара, својих или туђих, није нова појава. Развој индустрије, занатства, трговине, штампе и фотографије, довели су до рађања овог феномена још у XIX веку. По правилу се ради о уговорном односу са усаглашеним позицијама чинидбе и противчинидбе. У ново доба, често именовано као *ера глобализације,* интернет и нове технологије дају огромне могућности за најразличитије видове прометања појединих личних добара, у тој мери да су се појавила и нека хибридна права трговачке својине на појединим атрибутима сопствене личности. Чести су и случајеви неовлашћеног комерцијалног искоришћавања туђих личних добара. Правни системи, као и у многим другим питањима, не дају једнаке одговоре на питања која са собом носи овај проблем. Разлике постоје првенствено у томе да ли ће се проблем решавати са позиција права интелектуалне својине или са позиција грађанског права. Затим се појављују различите нијансе у решавању захтева за накнаду нематеријалне штете. У неким правним системима постоје битна ограничења у поступању судова при одлучивању о захтеву за накнаду штете, у другим правима судови имају широку слободу да уваже и овакве захтеве везане за неовлашћено комерцијално искоришћавање личних добара. Право Републике Србије је нормативно добро опремљено за један врло темељан и врло прецизан захват у ово релативно ново поље правних проблема и неизвесности.

Проблем комерцијалне апропријације личности може постати препрека приближавању и уједначавању правних система, а то опет може представљати проблем на глобалном плану, нарочито због све веће везаности, чак зависности савкодневице огромног броја људи од масовних медија и интернета. Лична добра привлаче велику пажњу, а сваки економски промет нема никаквих граница, и правни промет тежи да га следи, док правни системи и даље, у питању већине правних института, живе унутар географских граница својих држава.

Литература

Beverly-Smith, H. (2004). *The Commercial Appropriation of Personality*. Cambridge: Cambridge University Press.

Gavella, N. (2000). *Osobna prava, I dio.* Zagreb: Pravni fakultet u Zagrebu.

Dogan, S. L. Lemley, M. A. (2006). What the Right of Publicity Can Learn from Trademark Law. *Stanford Law Review*. 58 (4). 1161-1220.

Lindon, R. (1985). *Le juge de référes et la presse*. Paris: Dalloz.

Радованов, А. (2010). Накнада нематеријалне штете (појам, врсте и одређивање висине накнаде). *Право – теорија и пракса*. 9-10. 22-48.

Симоновић, И. Лазић, М. (2014). Грађанскоправна заштита права личности. *Зборник радова Правног факултета у Нишу*. 68 (LIII). 269-290.

Финжгар, А. (1988). *Права личности.* Београд: Службени лист СФРЈ.

H. Beverly-Smith, H. Onty, A. Lucas Schloeter, A. (2005). *Privacy, Property and Personality, Civil Law Perspectives on Commercial Appropriation.* Cambridge: Cambridge University Press.

Zweigert, K. Kotz, H. (1987). *An Introduction to Comparative Law.* Oxford: Oxford University Press.

Прописи:

Basic Law for the Federal Republic of Germany. Преузето 05.08.2021. https://www.btg-bestellservice.de.

Bürgerlichen Gesetzbuches BGB. Преузето 05.08.2021. https://www.gesetze-im-internet.de.

Закон о јавном информисању и медијима. *Службени гласник РС.* Бр. 83. 2014. 58.2015. 12. 2016 – аутентично тумачење.

Закон о облигационим односима. *Сл. лист СФРЈ.* Бр. 29. 78. 39.85. 45.89 – *одлука УСЈ*. 57.89, *Сл. лист СРЈ*. Бр. 31. 93, Сл. лист СЦГ. 1. 2003 – *Уставна повеља*. *Сл. гласник РС.* 18. 2020.

Code Civil. Преузето 05.08.2021. https://www.legifrance.gouv.fr

Судске одлуке:

Atkinson v. John E. Doherty & Co, 121 Mich. 372, 80 N.W.. 285 (1899). Преузето 05.08.2021.

https://ur.booksc.eu/book/26081102/580832.

Douglas v. Hello! Ltd (2005) EWCA Civ 595. Преузето 05.08.2021. https://www.5rb.com/case/douglas-v-hello-ltd.

Kaye v. Robertson [1990] EWCA Civ 21. Преузето 05.08.2021. https://www.5rb.com/case/kaye-v-robertson-sport-newspapers-ltd.

Marks v. Jaffa, 6 Misc. 290, 26 N.Y.S. 908 (N.Y. Misc. 1893). Преузето 05.08.2021. https://casetext.com/case/marksjaffa?__cf_chl_jschl_tk__=pmd_87f3229ea443c1eb63d2f969a8ea52f1077dcec0-1628022831-0-gqNtZGzNAiKjcnBszQjO.

Munden v. Harris, 153 Mo. App. 652 (Mo. Ct. App. 1911). Преузето 05.08.2021. https://casetext.com/case/munden-v-harris.

O'Brien v. Pabst Sales Co. - 124 F.2d 167 (5th Cir. 1941). Преузето 05.08.2021. https://www.lexisnexis.com/community/casebrief/p/casebrief-o-brien-v-pabst-sales-co.

Pavesich v. New England Life Ins. Co., 122 Ga. 190 (Ga. 1905). Преузето 05.08.2021. https://www.lexisnexis.com/community/casebrief/p/casebrief-pavesich-v-new-england-life-ins-co.

Rechtsprechung BGH, 15.11.1994 - VI ZR 56/94. Преузето 05.08.2021.

https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=15.11.1994&Aktenzeichen=VI%20ZR%2056/94.

Rechtsprechung BGH, 19.12.1995 - VI ZR 15/95.

Преузето 05.08.2021. https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=19.12.1995&Aktenzeichen=VI%20ZR%2015%2F95.

Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902). Преузето 05.08.2021. https://www.lexisnexis.com/community/casebrief/p/casebrief-roberson-v-rochester-folding-box-co.

Collis v. Walker, 272 Mass. 46, 172 N.E. 228 (Mass. 1930). Преузето 05.08.2021. https://casetext.com/case/collis-v-walker.

Cour de cassation, civile, Chambre civile 1, 15 janvier, 2015., 13-25.634., Преузето 05.08.2021. https://www.legifrance.gouv.fr/juri/id/JURITEXT000030114477/.

Cour de cassation, civile, Chambre civile 1, 5 avril, 2012., 11-15.328., Преузето 05.08.2021. https://www.legifrance.gouv.fr/juri/id/JURITEXT000025662321/.

Електронски извори:

https://www.britannica.com/topic/reality-show, Посећено 05.08.2021.

https://en.wikipedia.org/wiki/The_Osbournes, Посећено 05.08.2021.

https://www.eonline.com/shows/kardashians. Посећено 05.08.2021.

Milica Vučković, LL.D.,
Assistant Professor,
Faculty of Law, University of Niš,
Serbia

CIVIL LAW PROTECTION OF PERSONALITY FROM UNLAWFUL COMMERCIAL EXPLOATATION

Summary

In comparative law, unlawful commercial exploatation of personal atributes is wider known as phenomenon of commercial appropriation of personality. This legal phenomenon is being approached to from the aspects of intellectual property law and from the aspect of institute of unjust enreachment, and in that area, the principal aim of property sanction is reparation of material damage. Problem occur, in legislature, legal theory and legal practice, in relation to efforts of approaching to it from the field of civil law protection of personality from infliction of immaterial damage. In this paper, we are researching those controversial questions, existing answers, attempts of answers and probable solutions.

Keywords*: personality rights, immaterial damage, commercial appropriation of personality.*

Мр Сања Грбовић*[1]*,
Сарадница у настави,
Правни факултет Универзитета Црне Горе,
Црна Гора

UDK: 338.46:004.738.5(4-672EU)

ЕВРОПСКА УНИЈА И СЛОБОДА ПРУЖАЊА УСЛУГА ПУТЕМ ИНТЕРНЕТА

Апстракт: *Улазећи у еру дигитализације, ЕУ ради на јачању своје економије, позивајући се на циљеве Лисабонске стратегије из 2000. године у којој се закључило да европска економија треба да буде најконкурентивнија на свијету. Коришћењем интернета отвара се читав низ нових могућности која ће битно утицати на пораст броја радних мјеста и на даљи економски развој. Ако се осврнемо на чињеницу да изградња европског јединственог дигиталног тржишта доприноси европском расту са 177 милијарди ЕУР годишње*[2] *онда нам је јасно зашто је Дигитална агенда за Европу, уведена у оквиру стратегије Европа 2020, дала Унији главну улогу у даљем развоју информационих и комуникационих технологија.*

Да би могли добро пословати на данашњем свјетском тржишту предузећа се користе информатичком технологијом, како у контакту са својим клијентима, тако и са добављачима. Међутим, у циљу стварања јаке економије, није довољно само инкорпорирати дигиталну технологију у процес производње, тј. у тренутак настанка услуге, већ ће бити потребно имати квалификоване запослене и информатички писмене потрошаче, како би се реално и остварила продаја добара и услуга путем интернета. Европско јединствено дигитално тржиште је имало кључну улогу у одржавању економије и пружању помоћи грађанима ЕУ у вријеме пандемије COVID-19. У раду ће се анализирати однос између интернет платформе, пружатеља и корисника услуга као и правни оквир и судска пракса Суда правде ЕУ, са освртом на борбу против информатичког криминала и заштиту личних података.

Кључне ријечи*: слобода пружања услуга; интернет платформа; јединствено дигитално тржиште; Директива о електронској трговини;информатички криминал.*

[1] sanjag@ucg.ac.me

[2] Видјети w*ww.ec.europa.eu*

1. Појам слободе пружања услуга

На самом почетку, неопходно је дати пар дефиниција кључних појмова која ће бити предмет детаљне анализе током рада. Слобода пружања услуга је имала битну улогу у процесу настанка и развоја јединственог европског тржишта. Члан 57 Уговора ФЕУ[3] подразумијева под „услугом" сваку услугу дату уз одговарајућу надокнаду која није регулисана неком од одредби везаних за слободу кретања људи, робе и капитала, групишући тако као услужне дјелатности услуге индустријског и комерцијалног карактера, дјелатности слободних занимања и занатске дјелатности.[4] Резидуални карактер исте подразумијева да Суд правде прво мора оцијенити да ли одређена активност спада у област преостале три слободе да би на крају одлучио да ли ту исту активност може третирати као услугу.[5] С друге стране, пружалац услуге може, у сврху пружања исте, своју дјелатност привремено обављати у држави чланици у којој се услуга пружа под истим условима који су прописани за држављане те државе чланице.[6] Сами термин „услуга" је нужно економског садржаја, па самим тим иста изискује бити реална и ефективна.[7]

Резимирајући претходно наведене чињенице, под услугом се подразумијева свака активност која има следеће карактеристике: економску релевантност, прекогранични елемент и привремени карактер.[8] Чланови 56 и 57 Уговора ФЕУ се примјењују сваки пут када држављанин државе чланице нуди своје услуге у другим државама чланицама, без обзира на мјесто у ком је настањен њен корисник.[9] Што се тиче привременог карактера услуге, он се огледа не само у дужини њеног трајања већ и у њеној учесталости и периодичности захваљујући којој можемо разграничити

[3] Уговор о функционисању Европске уније (прочишћена верзија), СЛ Ц 202, 7.6.2016. (даље у тексту УФЕУ). За више информација о слободи пружања услуга као и о релевантној судској у: Enchelmaier, S. *Always at your service (within Limits), The ECJ's Case Law on Article 56 TFUE* (2006-2011), E.L.Rev. 36/2011, стр. 615.

[4] У оквиру члана 57. Уговора ФЕУ убрајају се такође и услуге које се врше на сличан начин нарочито ако имамо у виду одредбе Генералног програма о елиминацији ограничења слободи пружања услуга од 1961.године усвојеног од стране Савјета.

[5] Видјети нпр. случај *Sacchi*, C-155/73, I-409 и случај *Комисија в. Италија*, C-180/89, I-709.

[6] Члан 57 Уговора ФЕУ.

[7] Видјети случај *Steymann*, C-52/79, I-6159.

[8] Када говоримо о прекограничном карактеру, требамо имати у виду да се ради о појму који је предмет широког тумачења од стране Суда правде ЕУ.

[9] Видјети случај *Syndesmos ton en Elladi Touristikon*, C-398/95, I-3091.

слободу пружања услуга у односу на остале три слободе, а нарочито у односу на слободу пословног настањивања.[10]

2. Ка једној информатичкој заједници

Захваљујући новим технологијама, нарочито интернету, значајно се допринјело прогресивном развоју информатичке заједнице као и размјени услуга које се пружају онлајн. Правни систем се из тих разлога налази у једној врло тешкој позицији због тешкоће очувања како приватних тако и јавних интереса, јер интернет платформа није само мјесто на којем појединци пружају и примају услуге већ је и мјесто путем којег се исти могу обратити и органима државне управе. С друге стране, не треба сметнути с ума колики је допринос интернета био како у области образовања, тако и у областима слободе изражавања и приступа информацијама претходних година током пандемије узроковане вирусом Covid 19.

Још 2008. године финансијска криза је додатно истакла одређене структуралне мањкавости европске економије. Стратегија „Европа 2020"[11] коју је започела Европска комисија 2010.г. представљала је једну врсту одговора тадашњој кризи, постављајући циљеве у областима запошљавања и социјалне кохезије. У складу са члановима 179 и 190 Уговора ФЕУ, Европска унија имала је намјеру промовисати развој и дифузију нових информатичких технологија, да би 2015. године објавила Комуникацију о Стратегији јединственог дигиталног тржишта за Европу[12] захваљујући којој јединствено дигитално тржиште добија обрисе унутрашњег тржишта које је појачано дигиталном технологијом. Стратегија се базирала на три стуба и то: бољи приступ потрошача и предузећа роби и услугама на интернету; јачање сигурности дигиталних услуга и употребе личних података; максимално искоришћавање раста европске дигиталне економије. Треба имати у виду да унутрашње тржиште улази у доба дигитализације па самим тим биће неопходно нормативно интервенисати како би обезбиједили коришћење свих његових предности од стране цјелокупне европске заједнице. На бази претходно вршених процјена, сматра се да би јединствено дигитално тржиште могло допринијети расту европског БДП-а за 415 милијарди ЕУР-а.[13]

[10] Видјети случај C-55/94, *Reinhard Gebhard v Consiglio dell'Ordine Avvocati e Prociratori di Milano*, EU C 1995, 411, стр.39.

[11] Европска комисија, Комуникација Комисије, COM (2020), бр.2020.г.

[12] Европска комисија, Комуникација Комисије Европском парламенту, Вијећу, Европском економском и социјалном одбору и Одбору Регија „Стратегија јединственог дигиталног тржишта за Европу", COM (2015) 192, final. Брисел, 6.5.2015.г.

[13] Европска комисија, *Commission Staff Working Document, „A digital Single Market Strategy for Europe- Analysis and Evidence"*, SWD (2015) 100 final, Bruxelles, 6.5.2015., стр.5.

Задњих година биљежи се константан пораст онјалн садржаја, а услуге тих садржаја могле би у значајној мјери ојачати конкурентност европске индустрије у области музике, филма и онлајн игара. Из ових разлога је Комисија 2007. године предложила да се створе одговарајући механизми који би охрабрили развој јединственог унутрашњег тржишта са креативним садржајима на мрежи. Са све већом могућношћу приступа интернету као и све већом дифузијом његовог садржаја стварају се нове могућности за европску онлајн индустрију и за њене кориснике. Циљеви који се желе постигнути стварањем овакве врсте тржишта су првенствено повећање конкурентности, већи степен ажурирања података као и фаворизовање што већег учешћа корисника услуга и дифузије самог садржаја.

Са развојем тзв.пиратерије онлајн, уочено је да се дистрибутери услуга не успију увијек договорити са ауторима истих везано за њихову дистрибуцију на мрежи као и за маркентишке услове коришћења. Још један проблем представљају високи трошкови везани за уступање права коришћења. Комисија је заузела једну позицију „медијатора" у овој области покушавајући да успостави конструктивни дијалог међу заинтересованим странама. Пошто не постоје мултитериторијалне лиценце за креативне садржаје, ставља се једна врста кочнице у прекограничном коришћењу европских културалних дјела. Европска комисија захваљујући блиској сарадњи са државама чланицама покушава сузбити одвећ распорстрањену пиратерију, охрабрујући стварање система дигиталног управљања који ће дати јасну информацију услова коришћења садржаја онлајн корисницима тих услуга. Биће задатак пружатеља услуга и корисника створити једну врсту кодекса доброг понашања, како би се супроставили пиратерији, гарантујући широку и закониту понуду услуга на мрежи. Као што се имало прилике видјети у претходним годинама, свака држава чланица је покушала на свој начин да се суочи са овим проблемом, промовишући преузимање како музике, филма тако и осталих садржаја само са интерент страница које су за то ауторизоване.

3. Борба против информатичког криминала и сигурност на мрежи

Готово све наше дневне активности, биле оне приватног или професионалног карактера везане су за коришћење интернета. Пошто између држава чланица не постоји координација у области онлајн сигурности, Европска комисија је била мишљења да такво стање ствари ствара фрагментацију и неефикасност система на нивоу Уније,[14] предлажући заузимање заједничког става у случају да дође до озбиљнијих прекршаја, како би на тај

[14] Видјети : Европска комисија, Комуникација бр.194, 2009.г.

начин ефикасније превазишла проблем неусклађености националних законодавстава.

Унутар ЕУ постоји један минимум у координацији нормативних система држава чланица макар што се тиче казнених одредби везаних за информатички криминал. Ојачавајући сарадњу између судских органа држава чланица, кривични закони би се на адекватнији начин обрачунали са сајбер нападима и упадима у информатичке системе.

У том смјеру покушало се дјеловати са оквирном одлуком из 2005. године која је за циљ имала борбу против ових криминалних активности побољшавајући сигурносну структуру информационих система и омогућавајући органима гоњења обезбијеђивање адекватних услова како би дјеловали у том смјеру.[15] Поменуту одлуку је касније замијенила Директива 2013/40[16] која је додатно ојачала заштиту информатичких система у циљу што униформисанијег приступа саставним елементима казнених дјела. Релевантан елемент јесте транснационални карактер дјела, а кажњиви требају бити како покушај тако и намјера, с тим да кривичне санкције држава чланица морају бити ефикасне и пропорционалне.[17] Нормативна база за сваку будућу директиву која би покушала приближити национална законодавства могао би бити члан 83 Уговора ФЕУ на основу којег Парламент и Савјет могу дефинисати минимум норми које би дефинисале злочине и санкције транснационалног карактера проширујући на тај начин сферу криминалитета на коју се односе, а уколико се ради о областима у којим је надлежност подијељена примјениће се принцип супсидијарности.

Питање онлајн сигурности постаје све већи проблем Европске заједнице. Термин сигурност мреже и информације представља способност једне мреже, тачније једног информатичког система да издржи тј. да се одупре спољним нападима који би угрозили њену аутентичност, интегритет и приватност похрањених података. Уредба 2016/679 и Директива 2016/680 би требале да гарантују грађанима једноставнији приступ личним подацима и информацијама о начину обраде истих као и право да буду обавијештени кад су њихови подаци били на мети хакерских напада.[18]

[15] Оквирна одлука Савјета 2005/222/ПУП о нападима на информатичке системе.

[16] Директива 2013/40 о нападима на информатичке системе, ОЈ Л 218, 14.8.2013. стр. 8-14.

[17] Свака држава је одговорна за кривична дјела почињена на њеној територији или од стране њеног држављанина.

[18] Уредба 2016/679 о заштити појединца приликом обраде личних података и о слободном кретању таквих података, ОЈ Л 119, 4.5.2016., стр.1-88. и Директива 2016/680 о заштити појединца у вези са обрадом личних података од стране надлежних тијела у сврхе спрјечавања, истраге, откривања или прогона казнених дјела или извршавања

Како би обезбиједила што већи степен сигурности корисницима, Унија је основала 2004. године ЕНИСУ-а, Агенцију ЕУ за киберсигурност. Агенција помаже ЕУ и државама чланицама да дају бољи одговор на бројне проблеме информатичке сигурности; даје практичне савјете и рјешења за јавни и приватни сектор државама чланицама и институцијама ЕУ. Њен дјелокруг обухвата: организацију вјежби за случајеве кибернетичке кризе у цијелој Европи; помоћ у развоју националних стратегија информатичке сигурности; промовише сарадњу међу тимовима за хитне рачунарске интервенције.[19] ЕНИСА такође учествује у састављању нацрта политика и права ЕУ из области информатичке сигурности. Захваљујући својој присутности и сарадњи са великим бројем корисника како у јавном тако и у приватном сектору, ЕНИСА пружа подршку Унији у суочавању са новим изазовима информатичке сигурности. Оно што је битно напоменути јесте и улога коју ЕНИСА има у помагању државама чланицама и институцијама Уније у развоју и примјени политика потребних ради испуњавања правних и регулаторних захтјева.

ЕНИСА такође сарађује и са Еуруполом и Европским центром за кибернетички криминал, спроводећи заједничка истраживања и размјењујући информације ради ефикаснијег рјешавања проблема кибернетичке сигурности.

4. Заштита личних података

Директивом из 1995.[20] године дала се једна општа нормативна слика на нивоу ЕУ која би успјела да успостави равнотежу између два јако битна и конфронтирана интереса као што су заштита приватности и слобода кружења личних података унутар ЕУ. Дефинисана су прецизна ограничења у сакупљању личних података, тражећи од сваке државе чланице да конституише независно национално тијело које би се бавило њиховом заштитом. Подаци морају бити тачни и ажурирани, а у њиховом третирању мора постојати експлицитни пристанак заинтересоване особе. У случају повреде ових права, судским путем је гарантована њихова заштита предвиђајући и надокнаду штете у случају повреде истих. Поменута Директива из 1995. године о заштити личних података унутар ЕУ предвиђа двије области јако битне у процесу интеграција и то: заштита права и основних слобода што

казнених санкција и о слободном кретању таквих података, ОЈ Л 119, 4.5.2016.г. стр. 89-131.

[19] Видјети на : *www.europa.eu/european-union/about-eu/agencies/enisa*

[20] Директива 95/46/ЕЗ 24.10.1995, ОЈ Л 281 23.11.1995. стр.31, реформисана Уредбом 1882/2003/ЕЗ, 20.11.2003, ОЈ Л 284, 31.11.2003.г.

уједно обухвата и заштиту личних података и креирање унутрашњег тржишта за слободу кружења тих података.

Ипак, брзина технолошке еволуције као и сам процес глобализације битно су промијенили свијет у којем живимо, суочавајући нас са новим изазовима у заштити личних података. Друштвене мреже са својим милионима корисника у цијелом свијету су можда најевидентнији одраз овог феномена. Овај проблем је само дјелимично био предмет Директиве 2002/58/ЕЗ[21] која је допунила и интегрисла генералну Директиву из '95. године.[22]

Суд правде је више пута био позван да тумачи Директиву 95/46/ЕЗ, бавећи се поготово односом између принципа заштите личних података и коришћења нових технологија, афирмишући принцип на основу којег је дозвољено третирање личних података у новинарске сврхе.[23] У прошлости је Суд правде дао битна упутства како би боље разумјели када се коришћење личних података онлајн сматра недозвољеним. У случају *Lindqvist*[24] Суд правде је заузео став да све мјере предузете од стране држава чланица у области заштите личних података морају бити у складу са одредбама и циљем Директиве 95/46/ЕЗ а који се састоји у одржавању равнотеже између слободе кретања личних података и заштите права поштовања приватног живота.

Како се види у случају из 2010. године[25], заштита личних података је загарантована као основно право. Повеља ЕУ о основним правима, која након Лисабонског уговора има исту правну снагу као и Уговори, у члану 8 признаје право на заштиту личних података. Уговором ФЕУ у члану 16 афирмисао се принцип на основу ког свако има право на заштиту личних података које се на њега односе, дозвољавајући Унији да утврди правила о заштити физичких лица приликом обраде њихових података од стране институција, органа, служби и агенција Уније и држава чланица, а такође и правила за слободан проток тих података.

[21] Директива 2002/58/ЕЗ 12.07.2002.године, о заштити личних података и заштити приватног живота у сектору електорнских комуникација, ОЈ Л 201, 31.07.2002. године стр.37.

[22] Директива 95/46/ЕЗ, модификована Уредбом 1882/2003, ОЈ Л 284.

[23] Видјети случај *Tietosuojavaltuutettu,* 16.12.2008. с-73/07, 2007, I-9831.

[24] Видјети случај *Lindqvist* 6.11.2003. године, С-101/01. 2003, I-12971.

[25] Видјети случај *Volker und Markus Schecke GbR* 9.11.2010. С-92/09.

5. Нове прилике на мрежи

5.1. Еуропеана

Еуропеана је име европске дигиталне библиотеке која омогућава држављанима држава чланица да приступе европској културној баштини захваљујући процесу дигитализације. Већи број држава чланица је креирало националне портале тог типа, али се истовремено забиљежио слаб прогрес у смислу одржавања истих. Што се тиче дигиталне конзервације, развили су се бројни специфични програми у том полгеду, али неминовно је да ће се и на овом пољу тежити што већој сарадњи међу државама чланицама, имајући у виду да ЕУ има врло ограничену надлежност у овој области. Еуропеана је омогућила несметан приступ једном великом броју књига, штампе, докумената и умјетничких слика. Државе чланице су успјеле да инкорпорирају своје културно благо и преведу га у дигитални ресурс Еуропеане, како би сви држављани држава чланица могли да им приступе онлајн. Сигурно је многим младима у данашње вријеме ова врста дигиталне библиотеке постала мјесто редовног посјећивања.

5.2. Дигитализовани здравствени систем

Могућност развоја дигиталног здравственог система представља прилику за коришћење информатичких технологија како би се побољшала здравствена услуга држава чланица одржавајући стабилне трошкове са могућношћу њихивог умањења, као што ће се истовремено значајно умањити и вријеме чекања пацијената. Намјера је створити европски електронски систем здравства који би обухватао стварање дигиталних здравствених картона, издавања рецепата и сл. Данас се то у већини држава и остварило, али оно на шта треба скренути пажњу јесу корисници тих услуга које треба додатно обучити како би боље и лакше користили понуђене услуге. Корисници услуга требају увијек бити на вријеме и тачно информисани везано за трошкове услуга који се на овај начин пружају. Захваљујући дигитализацији здравства знатно се побољшао квалитет самих услуга, смањујући медицинске грешке које би се могле направити у издавању рецепата односно упута.

5.3. E-learning

Комисија је усвојила програм који је намјењен унапријеђивању квалитета и приступа европским образовним системима коришћењем нових технологија.[26] Жели се фаворизовати квалитетан образовни систем при-

[26] Одлука Савјета 2318/2003/EZ ОЈ Л 345 31.12.2003.г.

лагођавајући их потребама друштва. На овај начин су се охрабрили Универзитети и кампуси да створе нове организационе системе креирајући бројне програме размјене и подјеле дигиталних ресурса. Битно се утицало на проблем социјалне неједнакости и створила се култура сарадње међу бројним европским институтима. Програм e-*learning* заједно са програмом *Socrates* и *Leonardno da Vinci* само су једни од бројних програма који су допринели у том погледу.

Имајући у виду тренутну ситуацију узроковану пандемијом e-*learning* је постао саставни дио живота како студената тако и ђака. У том смислу се развио и програм учења на даљину, HELP, која је доступна бесплатно свим заинтересованим студентима и другим полазницима курсева који на тај начин не похађају класична предавања већ директно остварују комуникацију са предавачима (менторима). Путем платформе доступан је велики број курсева на енглеском језику, и у све већем броју, на другим језицима земаља Савјета Европе. Постоје два основна типа HELP курсева: HELP онлајн курсеви који обрађују различите теме везане за људска права доступни су сваком кориснику који има налог на платформи и тзв. "менторски курсеви" (енг. *tutored courses*) који су доступни само одабраној групи правника који похађају "пилот" курс који је организован у сарадњи са надлежном националном институцијом за обуку, Адвокатском комором или Правним факултетом и којим модерира HELP предавач.

5.4. E-goverment

Под e-*goverment/*ом се подразумијева употреба информатичке технологије у јавној управи која би довела до организацијских промјена унутар саме управе. Комисија је уочила да се захваљујући све већем стручном оспособљавању запослених подиже ниво услуге пружен грађанину, омогућавајући лакши приступ информацијама, смањујући вријеме чекања, док су процедуре за издавање дозвола битно поједностављене. Увођењем онлајн система у јавним управама створио се директни контакт са грађанином који ће на тај начин моћи да се обрати одговроним лицима у управи. Интернет портали са јединственом контактном тачком су у константном порасту. Омогућавајући приступ свима јавној управи, која је саставни дио e-*goverment/a,* подразумијава истовремено и гаранцију сигурног приступа корисницима као и право на жаштиту личних података. На овај начин се покушао јавни сектор учинити што транспарентнијим могуће, омогућавајући грађанима да боље разумију начин рада јавне управе и њеног степена одговорности према грађанима.[27]

[27] *E-goverment* унутар стратегије *i*-2010, Европска Комисија, Комуникација бр.229 од 2005.г.

6. E-commerce

Под електронском трговином подразумијева се свака иницијатива подршке било којој комерцијалној активности која се спроводи путем интернета. Е-трговина на јединственом дигиталном тржишту достиже свој пуни потенцијал захваљујући иновативним дигиталним алатима. С друге стране интерент платформе су релативно нов феномен и оне обухватају један широк спектар разноврсних дигиталних рјешења као што су веб претраживачи, друштвене мреже, аудио и видео платформе и сл. Интернет платформа дјелује као посредник између пружатеља и корисника услуге или робе стварајући на тај начин двострана или вишестрана тржишта.[28] Не постоји јасна и прецизна дефиниција електронске трговине, већ се до ње долази путем тумачења директива ЕУ. *E-commerce* се односи на сектор трговине добрима и услугама, на дистрибуцију истих путем интернета, као и на финансијске операције онлајн и на берзи. Различите форме електронске трговине могу да имају за предмет како материјалне тако и нематеријалне ствари, правећи тако разлику између директне и индиректне електронске трговине. Што се тиче индиректног *e-commerce*/а, оно се састоји у закључењу уговора путем интернета, док се предаја предмета врши на уобичајен начин, путем доставе. За разлику од њега, директни *e-commerce* се карактерише чињеницом да се цјелокупна радња одвија само и искључиво путем интернета.

Када говоримо о новим моделима пружања услуга путем интернетских платформи, најбитнији регулаторни инструменти на нивоу Уније су Директива 2000/31[29] и Директива 2015/1535.[30]

6.1. Директива 2000/31- Директива о електронској трговини

Активности везане за развој електронске трговине, на нивоу Европске Уније, отпочеле су још 1997. године (саопштење Комисије под називом „Европска иницијатива за електронску трговину"), јасно дефинишући жељу да се овај вид трговине униформно и коерентно дефинише на нивоу заједнице унутар 2000 године. Европски савјет је у Лисабону 2000. године поставио као стратешки план за предстојећу деценију формирање „економије бази-

[28] Европска комисија, *Commission Staff Working Document, „A digital Single Market Strategy for Europe- Analysis and Evidence", S*WD (2015) 100 final, Bruxelles, 6.5.2015., str. 52.

[29] Директива 2000/31/ЕЗ Европског парламента, Вијећа од 8.6.2000.(Директива о електронској трговини), СЛ Л 178, 17.7.2000.г.

[30] Директива 2015/1535 Европског парламента и Вијећа од 9.9.2015. о утврђивању поступка пружања информација у подручју техничких прописа и правила о услугама информацијског друштва, СЛ Л 241, 17.9.2015.г.

ране на знању, најконкурентије и најдинамичније на свијету". Признало се да је, не само грађанима, већ и предузећима потребна комуникацијска инфраструктура свјетског реномеа, која неће захтјевати огромне издатке. Како би све то остварила, Унија је себи дала задатак формирања тј. развоја електронске трговине и интернета. Директива 2000/31/ЕЗ[31] је елиминисала ограничења у прекограничним услугама на унутрашњем тржишту, доприносећи на тај начин да грађани и предузећа јасније сагледају садржину својих права у тој области. Директива је унаприједила правилно функционисање унутрашњег тржишта осигуравајући слободно кретање услуга информацијског друштва између држава чланица.[32] На овај начин повећала се конкурентност између пружаоца услуга, стимулисао процес иновације као и стварања већег броја радних мјеста.

Директива уређује електронску трговину у законодавном смислу, узимајући у обзир само фундаменталне аспекте како би омогућила што боље функционисање унутрашњег тржишта у тој области. Односи се на одређени број услуга које се пружају путем интернета почевши од услуга из области информација, услуге продаје производа као и финансијских услуга. Ова директива има хоризонталну примјену, и примјењује се у електронској трговини између два предузећа, тзв. *business to business* и на трговину између предузећа и клијента, *business to consumer*. Са клаузулом унутрашњег тржишта, Директива има намјеру да формира један јасан и прецизан нормативни контекст који је неопходан пружаоцима услуга информатичког друштва како би на што бољи начин могли пружати своје услуге унутар Уније. (Carriero, 2002:137). Такође и одредбе које се односе на одговорности посредника дају један висок степен сигурности за пружање фундаменталних услуга медијације тј. посредништва путем интернета.

Захваљујући својој природи, електронска трговина не познаје границе и управо то је био разлог нормативне интервенције. Давањем јасног нормативног оквира цијелој дисциплини, захваљујући Директиви 2000/31/ЕЗ, корисници услуга ће имати већи осјећај сигурности у коришћењу понуђених услуга на мрежи. Због тога се и развио концепт клаузуле унутрашњег тржишта, на основу којег свака држава чланица мора гарантовати да ће пружаоц услуге електронске трговине који се налази на њеној територији поштовати национално законодавство те државе чланице. У исто вријеме, држава чланица не може наметнути рестрикције нити ограничења слободи пружања услуга оним предузећима која долазе из других држава чланица. Клаузула унутрашњег тржишта предвиђа минимална

[31] Директива 2000/31/ЕЗ од 8.јуна 2000.године, ОЈ Л 178, од 17. јула 2000. године, стр.1.

[32] Члан 1 став 1 Директиве о електорноској трговини. Данас је на снази Директива 2015/1535.

одступања, и у овом контексту државе чланице могу предузети низ мјера како би заштитиле одређене интересе.[33] Сама активност пружања услуге не може бити условљена претходном овлашћењем нити било којим другим захтјевом који би имао исти учинак.[34] На овај начин покушало се учинити лакшим пружање услуге избјегавајући да пружаоц буде условљен додатном бирократијом. Са друге стране битно је напоменути да члан 5 Директиве 2000/31/ЕЗ гарантује транспарентност у погледу информација о идентитету и сједишту пружаоца услуге.

Што се тиче информација комерцијалног карактера, свако привредно друштво може на интернету рекламирати услуге и производе које нуди, имајући у виду да је то најбољи начин упознавања и пружања информација својим корисницима. Директива електронске трговине је интегрисала претходне директиве везане за заштиту потрошача дајући још већи степен транспарентности сваком облику рекламе онлајн. На основу Директиве 2000/31/ЕЗ, адвокати, доктори, фармацеути, рачуновође и агенти некретнина су формирали кодекс понашања на нивоу Уније како би на што бољи начин савладали проблем комерцијалних информација (Peterson, Fink, Ogus, 2013:27). Сви ови кодекси заједнички имају обавезу достављања информација које морају бити тачне и прецизне како би сачували престиж и достојанство сопствене професије.

Када говоримо о уговорима онлајн, члан 9 Директиве предвиђа да државе чланице морају осигурати да њихово законодавство дозвољава склапање уговора електронским путем. Истовремено је дата могућност државама чланицама да се овај члан не примјењује на уговоре којима се стварају или преносе права на некретнине (изузев најма), уговоре за које закон прописује интервенцију судова, уговоре о јемству и уговоре уређене породичним и наследним правом. Чланови 10 и 11 додају и обавезу достављања информација везаних за закључивање уговора као и обавезу потврде пријема одређеног налога. Добијене повратне информације држава чланица о статусу имплементације поменуте Директиве управо указују на чињеницу да су пружатељи услуга врло брзо униформисали своје интернет странице са прописима садржаним у Директиви.

Што се тиче интернет посредника, као и њихове одговорности чланови, 12 и 14 Директиве 2000/31/ЕЗ, долазе до изражају јер пружају услуге меморисања, преноса и хостинга онлајн. Поменути чланови прецизно дефинишу ситуације у којима се посредници не могу сматрати одговорнима и ситуације када државе чланице не могу додати нове услове од оних већ

[33] Директива 2000/31/ЕЗ, члан 3 став 4, 5, 6.

[34] Директива 2000/31/ЕЗ, члан 4 став 1.

предвиђених Директивом. Одговорност може бити како кривична тако и грађанска за све врсте илегалних активности предузетих од стране трећих лица. Државе чланице могу наметнути пружаоцу услуге да прекине или предухитри одређену илегалну радњу, имајући у виду да је то у оквиру надлежности држава чланица. Ограничење одговорности посредника сматрано је неопходно, у циљу гаранције исправности пружене услуге и очувања континуитета слободе пружања услуга. Члан 15, са друге стране, забрањује државама чланицама да намећу посредницима обавезу контроле информација које се преносе имајући у виду обиље интернет страница и активности које се пружају. Без обзира на то, члан 15 не брани државним органима државе чланице да наметну обавезу контроле у појединачним тачно дефинисаним случајевима. На овај начин ствара се троугао односа између три категорије учесника и то: пружатеља услуге, корисника услуге и интернет платформе као посредника који олакшава трансакције између пружатеља и корисника услуге.

6.2. Директива 2015/1535- Директива о транспарентности на унутрашњем тржишту

Директива о транспарентности на унутрашњем тржишту обавезује државе чланице да Комисији доставе нацрт о техничким прописима о производима и услугама информацијског друштва. Ова врста техничких прописа односи се на техничке спецификације за производе и правила за пружање услуга, који би могли бити препрека у трговини, тј. у пружању услуга. На овај начин је дата могућност да Комисија и други заинтересовани учесници изнесу мишљења и коментаре о нацртима прописа, а које држава чланица може узети у обзир прије доношења истих.

Директива дефинише „услугу информацијског друштва" као услугу која се пружа уз накнаду, на даљину, електронским путем на лични захтјев корисника услуге.[35] Сматраће се да се пропис изричито односи на услуге информацијског друштва уколико се из његовог образложења, циља и сврхе произилази експлицитна намјера регулације тог типа услуге.[36] Уколико се донесе пропис без претходне нотификације или противно ставу Комисије о његовој усклађености са унутрашњим тржиштем, такав пропис неће се аутоматски сматрати ништавим. Свакако могуће је покренути поступак пред Судом правде ради повреде права Уније, у складу са чланом 258 Уговора ФЕУ. Овакав тип пропуста државе чланице према судској пракси

[35] Члан 1 став 1 (б) Директиве 2015/1535.

[36] Члан 1 став 1 (е) Директиве 2015/1535.

Суда правде ЕУ може онемогућити примјену таквог националног прописа у судском спору између странака.[37]

Комисија је дефинисала три кључна критеријума ради објективног пресуђивања, а која се у основи своде на: степен утицаја платформе над услугом тј. његовим пружатељем; услови пружања услуге; власништво над кључним средствима за пружање услуге.[38] Суд правде је углавном слиједио ова разматрања, иако су га теоретичари често критиковали, сматрајући да прилично компликује питање примјењивог правног режима.[39]

Имајући у виду да постоје различите врсте интернет платформи, јако је тешко пронаћи одговарајући регулаторни оквир, а једине које се издвајају су интернет платформе у економији сарадње.[40] Специфичност ове врсте платформе јесте што пружатељ услуга не мора нужно бити професионалац. У том случају ради се о узајамном пружању услуга појединаца, гдје се надокнађује трошак појединцу а не плаћа се накнада за пружену услугу.[41] На нивоу ЕУ својство пружатља услуге не подразумијева нужно пружање услуге на професионалној основи[42] па самим тим, због недостатка јасних критеријума, намеће и низ питања везаних за допуштеност постојећих ограничења у државама чланицама као што су лиценце, овлашћења и сл.

7. Циљеви „приступа интернета свима"[43]

Иако европско друштво из године у годину ствара све више информатичких производа и услуга, као што је познато, одређени дјелови популације још увијек немају приступ њима. У том смислу је Комисија покушала створити једну врсту заједничког приступа у области *e-accessability*. Овај програм обухвата првенствено особе са инвалидитетом као и старије особе, омогућавајући им куповину онлајн као и приступ органима државне управе. Побољшање приступа интернету представља једну очигледну предност у смислу побољшања конкурентности међу привредним

[37] Видјети случај *Security International SA v Signalson SA i Securitel SPRL*, C-194/94, EU:C:1996:172.

[38] Европска комисија, COM(2016), 356 final, стр.6.

[39] Видјети нпр. Hatzopoulos, S. Roma, *„Caring or sharing? The collaborative economy under EU Law", CML Rev 54/2017, str.127.*

[40] Комуникација Комисије „Европски програм за економију сарадње", COM (2016) 356 финал и Комуникација Комисије „Интернетске платформе и јединствено дигитално тржиште. Могућности и изазови за Европу", COM (2016) 288 final.

[41] Европска комисија, COM(2016) 356 final, стр.5.

[42] Члан 4 став 2 Директиве о услугама.

[43] Европска комисија, Комуникација 2008 бр.804.

друштвима. У том смислу треба напоменути и труд који је Унија уложила како би подржала иницијативе држава чланица у пружању „дигиталног образовања" својим грађанима.[44] Медијско образовање конципирано је као оспособљавање појединца да умије консултовати, схватити и критички се односити према медијском садржају. Имајући у виду да је иста неопходна ради пуног и комплетног развоја грађанства, нуди држављанима држава чланица да учествују у економској и културолошкој димензији интернет сајтова, тв-а, видеоигрица и виртуелних садржаја. Медијско образовање треба сваког да охрабри, без икакавог вида дискриминације, омогућавајући корисницима све оне предности еволуције информатичког друштва. Како би подржала ту иницијативу, ЕУ је од држава чланица затражила да се што више ангажују у том смјеру.

Унија је себи поставила за циљ промоцију једне дугорочне иницијативе у корист даљег развоја информатичке технологије (која има битну улогу у погледу конкуренције ЕУ) у контексту модернизације, превазилазећи истовремено дефицит информатичке стручности и стварајући једну праву економију знања[45]. Пошто не постоји глобална стратегија у области информатичке стручности на нивоу ЕУ остају и даље разлике у законодавству међу државама чланицама које треба превазићи.[46] Допуштајући Европи да има сопствени интернет идентитет, ојачало се њено присуство на мрежи, а самим тим се поспјешио и развој електронске трговине на унутрашњем тржишту Уније. Домен „eu" који је дефинисан на основу Уредбе[47] из 2002. године није имао намјеру замијенити домене који су постојали раније, већ их је желио инкорпорирати. На овај начин се хтјела дати могућност корисницима да приликом регистрације изаберу да ли ће се регистровати под националним доменом или доменом Уније, промовишући на тај начин Унију на свјетским информатичким мрежама. Истовремено ЕУ је задржала сва права интелектуалне својине на домену „eu", а накнадном реформом Уредбе наведени су и неопходни елементи у циљу спрвођења њеног дејства.[48]

[44] Европска комисија, Комуникација 2007, бр.711.

[45] Европска комисија, Комуникација 2007, бр.496

[46] Циљеве које је себи поставила ЕУ односе се на сарадњу и мониторинг прогреса који су били остварени од стране држава чланица, подржавање једног европског информатичког садржаја, промоција размјене информација и праксе међу државама чланицама повећавајући на тај начин запосленост и друштвену кохезију.

[47] Уредба 733/2002 о увођењу домена .eu од 22. 04.2002, ОЈ Л 113 од 30.4.2002.г.

[48] Уредба 874/2004 28.04.2004. OJ L 162 од 30.4.2004.г.

8. Закључак

У јеку епидемије узроковане вирусом Covid 19, интернет је представљао једну врсту „прозора у свијет" милионима људи. Наше свакодневне активности су се претвориле у онлајн праћење наставе, виртуелни одлазак на посао, онлајн дружење са пријатељима. Радикална промјена стила живота наметнута поменутим вирусом је учинила то да се шира популација која можда раније није била информатички писмена сада то и постане. Свједоци смо времена који сви лидери свијета називају „највећом кризом од Другог свјетског рата" и која је неминовно оставила последице и на наш стил живота. Морали смо се прилагодити „животу на мрежи" односно учењу са интернет платформи, раду путем Zoom платформи, виртуелном одласку у самопослугу. Нити једна држава свијета, па ни чланице Уније нису биле спремне на овакву врсту кризе, али су се временом морале прилагодити. Научили смо да наставимо са својим животима из карантина, не посустајући у нашем образовању и даљем пословном усавршавању. Захваљујући информатичкој технологији тако нешто смо и успјели остварити, упркос чињеници да, не све државе чланице, могу искористити предности дигиталног тржишта.[49] Потреба за већом правном регулацијом постаје све јаче изражена, јер иста може одиграти кључну улогу у даљем усклађивању националних законодавстава. Да ли су системи интернет платформи и остале услуге испуниле наша очекивања је одговор који ћемо добити временом, временом када ћемо моћи да се вратимо свакодневном животу без социјалне дистанце.

Литература

Бодирога-Вукобрат Н., Мартиновић А., *"Изазови пружања услуга на дигиталном тржишту ЕУ-а- услуге информацијског друштва и "позадинске" услуге*", Зборник Правног факултета у Ријеци, вол.40, бр.1, 2019.г. стр. 37-58.

Enchelmaier, S. *"Always at your service (within Limits), The ECJ's Case Law on Article 56 TFUE* (2006-2011)", E.L.Rev. 36/2011, стр. 615.

Peterson I., Fink M., Ogus A., *Economic Impact of Regulation in the Field of Liberal Professions in Different Member States*, Research report for the European Comission, Vienna, Austria, Institute for Advanced Studies, 2013.

Carriero G., „*E-commerce. La direttiva 2000/31/CE e il quadro normativo della rete*", Milano, Giuffre, 2002, стр.137.

[49] Бодирога-Вукобрат Н., Мартиновић А., "Изазови пружања услуга на дигиталном тржишту ЕУ-а- услуге информацијског друштва и "позадинске" услуге", Зборник Правног факултета у Ријеци, вол.40, бр.1, 2019.г. стр. 37-58.

ЕУ прописи и радни документи:

Директива 95/46/ЕЗ 24.10.1995, ОЈ Л 281 23.11.1995. стр.31, реформисана Уредбом 1882/2003/ЕЗ, 20.11.2003, ОЈ Л 284, 31.11.2003.

Директива 2000/31/ЕЗ Европског парламента, Вијећа од 8.6.2000.г. (Директива о електронској трговини), SЛ Л 178, 17.7.2000.г.

Уредба 733/2002 од 22. 04.2002, ОЈ Л 113 од 30.4.2002.г.

Директива 2002/58/ЕЗ 12.07.2002.године, о заштити личних података и заштити приватног живота у сектору електорнских комуникација, ОЈ Л 201, 31.07.2002. г.стр.37.

Одлука 2318/2003/ЕЗ, ОЈ Л 345 31.12.2003.г.

Директива 2015/1535 Европског парламента и Вијећа од 9.9.2015. о утврђивању поступка пружања информација у подручју техничких прописа и правила о услугама информацијског друштва, СЛ Л 241, 17.9.2015.г.

Европска комисија, *Commission Staff Working Document, „A digital Single Market Strategy for Europe- Analysis and Evidence", S*WD (2015) 100 final, Bruxelles, 6.5.2015.г.

Европска комисија, Комуникација Комисије Европском парламенту, Вијећу, Европском економском и социјалном одбору и Одбору Регија „Стратегија јединственог дигиталног тржишта за Европу", COM (2015) 192, final. Брисел, 6.5.2015.г.

Комуникација Комисије „Европски програм за економију сарадње", COM (2016) 356 финал и Комуникација Комисије „Интернетске платформе и јединствено дигитално тржиште. Могућности и изазови за Европу", COM (2016) 288 final.

Hatzopoulos, S. Roma, „*Caring or sharing? The collaborative economy under EU Law", CML Rev 54/2017.*

Уговор о функционисању ЕУ, доступно на: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A12016ME%2FTXT

Пракса Суда правде ЕУ:

Случај *Sacchi*, C-155/73, I-409

Случај *Steymann*, C-52/79, I-6159.

Случај *Комисија в. Италија*, C-180/89, I-709.

Случај *Security International SA v Signalson SA i Securitel SPRL*, C-194/94, EU:C:1996:172.

Случај C-55/94, *Reinhard Gebhard v Consiglio dell'Ordine Avvocati e Prociratori di Milano*, EU C 1995, 411.

Случај *Syndesmos ton en Elladi Touristikon*, C-398/95, I-3091.

Случај *Lindqvist* 6.11.2003. године, C-101/01. 2003, I-12971.

Случај *Tietosuojavaltuutettu,* 16.12.2008. C-73/07, 2007, I-9831.

Случај *Volker und Markus Schecke GbR* 9.11.2010. C-92/09.

Mr Sanja Grbović,
Teaching Assistant,
Faculty of Law, University of Montenegro,
Montenegro

EU AND THE FREEDOM TO PROVIDE SERVICES ONLINE

Summary

Entering the era of digitalization, the EU is working on strengthening its economy, in accordance with the aims of the Lisbon Strategy from 2000, set out to make the European economy the most competitive in the world. The use of the Internet opens up a whole range of new opportunities that will result in further economic growth and consequently more jobs. If we look at the fact that building a European digital single market contributes to European growth of € 177 billion a year, then it is clear why the Digital Agenda for Europe, launched as the part of the Europe 2020 strategy, has given the Union a major role in further development of information and communication technologies.

In order to do well at today's global market, companies use information technology to contact either their customers or their suppliers. However, to create a strong economy, it is not enough just to incorporate digital technology into the production process at the time of their service, but it is going to be necessary to have qualified employees and IT-literate consumers to sell goods and services via Internet. The European digital single market has been playing a key role in sustaining the economy and providing support to EU citizens during the COVID-19 pandemic. This paper will analyze the relationship among the Internet platform, service providers and users, as well as the legal framework and court practice of the EU Court of Justice, with special emphasis on the fight against information crime and personal data protection.

Keywords*: freedom to provide services; internet platform; digital single market; Electronic Commerce Directive, IT Crime.*

Др Жељко Мирјанић,[1]
Редовни професор,
Правни факултет Универзитета у Бањој Луци,
Република Српска, Босна и Херцеговина

UDK: 349.2
340.137(497.11:4-672ЕУ)

УТИЦАЈ ДИГИТАЛИЗАЦИЈЕ НА РАДНО ПРАВО

Сажетак*: Значај теме огледа се у томе што актуелизује потребу за сагледавањем читавог низа питања која за радно право носи развој информационих и комуникационих технологија, дигитализација пословања и рада, као што су рад код куће, заштита личних података запослених лица, итд. Промјена стандардног пословног окружења у ново, чије су главне карактеристике глобализација, дигитална економија, флексибилност и развој дигиталних компанија и бизниса, утиче на пословање. То, поред осталог, подразумијева промјене у начину стицања знања и образовања, промјене и систему личних и друштвених вриједности. Технологије су промијениле начин живота појединаца, њихову комуникацију и на такав начин их увеле их у ново, информационо друштво. У садашњој фази информационог друштва једини начин системске заштите и развоја је квалитетно информисање и оспособљавање кадрова за рационално функционисање у свијету информација. Послодавац путем информационих технологија прикупља, обрађује, користи и чува личне податке запослених потребне за остваривање права и обавеза у радном односу. Једна од посљедица јесте успостављање нових друштвених норми,којима се појединац и друштво у цјелини прилагођавају. Све више профит долази на прво мјесто, те се поставља питање докле је друштво спремно да толерише ову појаву. Садашња фаза развоја радног права заснива се на концепту социјалне тржишне привреде и на промјени свијета рада под утицајем концепта неолибералне глобализације. Ток даљег развоја домаћег радног права зависи од прилагођавања европског радног права и радног права у земљама чланицама ЕУ најважнијим промјенама у свијету рада и капитала. За успостављање дугорочно одрживог социјалног мира недостаје међусобно повјерење између социјалних актера. Држава као организација грађана мора преузети*

[1] zeljko.mirjanic@pf.unibl.org,

улогу балансера између рада и капитала. Повјерење се може градити кроз употребу информатичких технологија будући да оне омогућавају стално информисање о економском и социјалном развоју. Употреба информатичких технологија убрзава еволутивне промјене у свијету рада и олакшава социјални дијалог као облик институционализованог друштвеног дијалога, усмјерен ка рјешавању најважнијих проблема у свијету рада.

Кључне ријечи: *радно право, хармонизација радног права, заштита приватности и личних података запослених, рад код куће.*

1. Увод

Промјене међународног, европског и домаћег радног права које су започете у другој половини прошлог вијека под утицајем најважнијих глобалних процеса у које спадају дигитализација и настанак информатичког друштва, трају и током двадесет првог вијека. Дигитализација мијења свијет рада и, као што констатује Европска комисија, дигитална комуникација, интеракција на друштвеним медијима, електронска трговина и дигитална предузећа постепено мијењају свијет. Генерише се све више података који могу омогућити нове начине и нивое стварања вриједности. Трансформација је подједнако корјенита као она узрокована индустријском револуцијом.2 У питању је универзални прелазак са механичке и аналогне технологије на дигиталну електронику, увођење рачунарских комуникационих технологија и увод у информатичко доба (Анђелковић, Радосављевић, Лилић, 2021:19). Дигитализација утиче на промјену облика и садржаја рада у низу дјелатности и настанак нових професија, на флексибилизацију радних односа и флексибилно запошљавање, заштиту личних података, заштиту приватности радника, достојанство рада, мјере заштите здравља радника приликом коришћења информатичке опреме, итд. уз сразмјеран раст зависности послодаваца и радника од нових технологија.

Многе студије упућују на индиректно стварање послова због дигитализације. Према једној студији нови посао заснован на интернету подржава стварање око 1,54 додатних послова негдје другдје у економији. Процјена је да сваки посао створен у технолошки високо развијеној индустрији као што је роботика може створити додатних пет нових послова у широј економији. Ипак није јасно, надмашују ли новостворени послови бројчано

[2] Европска комисија. *Изградња дигиталне будућности Европе*, Брисел, 19.2.2020. COM (2020) 67. Преузето : 1.9.2021. https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=COM%3A2020%3A0067%3AFIN

послове који због дигитализације нестају. Удио послова који су угрожени дигитализацијом зависи од степена аутоматизације поједине државе те расте са смањењем тог степена (Butković, Samardžija, 2019:17).

Дигитализација тражи да радници стално стичу знања и вјештине неопходне за коришћење нових технологија да би успјели задржати или пронаћи ново запослење, а да послодавци стално уводе нове технологије да би сачували или побољшали позицију на тржишту. Стога изгледа оправдан став изнијет у литератури да идеја о послу за цијели радни вијек постаје ствар прошлости. У свјетлу утицаја глобалне економије и тражње за "флексибилном" радном снагом, поједини социолози и економисти сматрају да ће све већи број људи постати радници који ће посједовати "портфељ вјештина" – одређен број различитих вјештина и квалификација које ће користити како би се у току радног вијека кретали с једног радног мјеста на друго и како ће релативно мали број радника имати постојану "каријеру", у данашњем смислу те ријечи (Гиденс, 2007: 417). Европска комисија сматра да повећање нивоа образовања и вјештина представља кључни дио опште визије дигиталне трансформације, да европским предузећима требају радници са дигиталним вјештинама на глобалном тржишту заснованом на технологији, а да радницима требају дигиталне компетенције да успију на динамичном и све више дигитализованом тржишту рада.[3]

У Европи је око 350.000 слободних радних мјеста намијењених за висококвалификоване техничке стручњаке у областима вјештачке интелигенције, анализе података и сајбер-сигурности. Уочено је да 90% свих радних мјеста захтијева бар минимални ниво дигиталних вјештина и да расте тражња за дигиталним стручњацима. Према подацима Европске Комисије 44 % становништва и 37 % радне снаге у Европској унији нема довољан ниво тих вјештина, а половина предузећа још увијек не проводи стратегије за преквалификацију радне снаге (Negreiro, M. Tamiama, M. 2019: 3). Након дугог раздобља током кога је Европа смањила разлике у продуктивности у односу на САД, од 1995. та се разлика повећава и не показује знаковесмањивања, а један одкључнихразлогаје то што европске државе нису успјеле искористити предности од информационо-комуникационих технологија као САД (Degryse, 2016: 13).

Дигитализација утиче на тржишта рада на начин да се однос мијења у корист рада на даљину, али није могуће предвидјети мјеру у којој ће овај облик рада потиснути рад у просторијама послодавца. У посматраним за-

[3] Европска комисија. *Изградња дигиталне будућности Европе*, Брисел, 19.2.2020. COM (2020) 67. Преузето : 1.9.2021. https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=COM%3A2020%3A0067%3AFIN

конима о раду, рад у просторијама послодавца је регулисан као редован начин обављања послова, а рад ван просторија послодавца је регулисани као одступање од правила. Радник обавља рад у просторијама послодавца под непосредним надзором, а може изузетно да га обавља ван ових просторија. Послодавац може уговорити обављање послова ван својих просторија на издвојеном мјесту рада, а које радник може да обавља ако нису опасни или штетни по здравље радника и других лица и ако не угрожавају радну и животну средину.[4] Радник који ради ван просторија послодавца је дужан да примјењује мјере заштите здравља и безбједности на раду.

Радно право не иде у корак са дигитализацијом и правни односи у вези са обављањем рада уз помоћ дигиталне технологије су често недефинисани и нерегулисани, а један од разлога за то је што основна рјешења почивају на традиционалном запошљавању. Да би се „дигитални запослени” боље заштитили морају се пронаћи нови начини регулисања радних односа и трансформисати многи базични институти радног права. Уводе се нови начини регулисања радног ангажовања са упливом уговора грађанског права и зато је потребно да се преиспита и „флексибилизује” појам радног односа, „запосленог”, „послодавца”, „предузећа” (Јашаревић, 2016: 1104). При томе је важно и упозорење са Конгреса ЕТУЦ-а 2015, по коме ако се крене од става да појам квалитетног запослења укључује пристојну плату, заштиту здравља и безбједности, прихватљиве услове рада, прилике за оспособљавање и напредовање и ако уговор о раду на неодређено вријеме са пуним радним временом „за све” треба и даље да остане правило, утицај дигиталне револуције на тржишта рада отвара бројне недоумице и разлоге за забринутост (Degryse, 2016: 14).

Упоредо са повећањем значаја рада на даљину и других облика рада за чије се обављање користе информационе и комуникационе технологије повећава се значај регулисања и истраживања правних односа поводом тог рада. Стваралоцима права недостају резултати пројектних истраживања о овим облицима рада упркос томе што су резултати истраживања аналитичка основа која може придонијети конструктивном суочавању са ризицимадигитализацијекоја уноси велике промјене у развој друштва у цјелини, а посебно на тржишту рада (Butković, Samardžija, 2019:17). Резултати истраживања повезаних са утицајем дигитализације на радно право указују да су потребна систематска преднормативна истраживања,

[4] Закон о раду („Службени гласник Републике Српске” бр. 1/16 и 66/18) чл. 44; Закон о раду („Службени гласник Републике Србије”, бр. 24/05, 61/05, 54/09, 32/13 и 75/14, 13/17 – УС, 113/17, 95/18) чл. 44; Закон о раду („Службене новине Федерације Босне и Херцеговине” , бр. 26/2016 и 89/2018) чл. 26; Закон о раду („Народне новине” Републике Хрватске 93/14, 127/17) чл. 17.

а што показује бројност истраживачких питања као што су: праћење запослених путем видео надзора, службене електронске поште и службеног телефона (Обрадовић, 2021: 19); регулисање коришћења технологија на начин да се обезбиједи заштита личних података и приватности угрожених усљед праксе електронског надзора, софистицираног праћења запослених и прикупљања њихових биометријских података (Мирјанић, 2019: 166); негативни аспекти дигитализације, нпр. раст незапослености, слабљење синдикалног утицаја, утицај на здравље на раду (Јовевски, 2021: 21).

Утицај дигитализације на промјену, нестанак, аутоматизацију и роботизацију низа послова расте и поставља се питање да ли ће и даље човјек бити кључна фигура у процесу рада, да ли ће се рад обављати на исти начин као данас, колико ће људска радна снага постати замјењива категорија, као значајно питање за радно право и право на рад у будућности (Брковић, Антоновић, 2019: 280-281). У којој ће мјери нова дигитална економија отворити, уништити или замијенити радна мјеста? Који ће сектори бити највише погођени? Које ће нове вјештине и квалификације бити потребне? Како ће се одвијати транзиција? На та питања нема јединственог одговора (Degryse, 2016: 39). Дигитална револуција је довела до значајних промјена у условима рада и радном окружењу, као и до питања да ли са дигитализацијом долази до промјене друштвеног статуса радника, да ли дигитализација рада води до урушавања права радника на достојанствен рад (Ковачевић, 2019: 86)? Степен „дигитализације свега" је толико велики да неки аутори овај процес називају „дигиталном револуцијом", модерну економију „дигиталном економијом". Назире се ново друштво које неки називају „дигитални капитализам". За „виртуелне послодавце" у оваквој „виртуелној економији" и „кибернетском простору" раде „дигитални радници" који су углавном невидљиви и обесправљени, а који су названи „дигитални пролетеријат" (Јашаревић, 2016: 1115). У овом тексту се полази од става да дигитална технологија не може замијенити нити у већој мјери маргинализовати улогу радника и да једино они могу обављати сложене интелектуалне послове у науци, медицини, просвјети, култури, правосуђу, итд. а да то не може дигитална технологија. Како је истакнуто у документу о дигиталној будућности - колико год биле напредне, дигиталне технологије су само алат и не могу ријешити све наше проблеме, али је због њих могуће оно што је прошлој генерацији било незамисливо.[5]

[5] Европска комисија. *Изградња дигиталне будућности Европе*, Брисел, 19.2.2020. COM (2020) 67. Преузето : 1.9.2021. https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=COM%3A2020%3A0067%3AFIN

2. Рад на даљину

Рад на даљину, мобилни и масовни рад преко дигиталних платформи служе за обављање низа креативних, консултантских, савјетодавних, асистентских, образовних и других послова, и послова неопходних за функционисање информационе и комуникационе технологије. За разлику од рада на даљину који се обично обавља на фиксном мјесту рада, код мобилног (агилног) рада радници су покретљивији и могу да раде код куће, у изнајмљеном или неком другом простору који не припада послодавцу. Дигитализација подстиче флексибилизацију радних односа и раст броја нестандардних уговора о раду који су правни основ за нове облике рада. Еурофонд је формулисао трендове који мијењају традиционалне односе између послодаваца и радника међу које спадају: мобилни рад који радници обављају са било ког мјеста у било ком тренутку и масовни (групни) рад у коме дигитална платформа повезује послодавце и раднике при чему се већи задаци често дијеле у мање задатке међу радницима у „виртуелном облаку".[6] Однос социјалних партнера према наведеним облицима рада је различит, тако што послодавци позитивно оцјењују нове облике рада, а синдикати наглашавају да тај рад често представља избор из нужде, при чему се социјални партнери слажу да постоји потреба за проширивањем појма радника како би тај појам обухватио нове облике рада у дигиталној економији (Butković, Samardžija, 2019: 89). Разлози за брзо ширење наведених облика рада су предности које имају у односу на рад у просторијама послодавца: послодавци смањују пословне трошкове, док радници добијају већу аутономију у обављању послова и коришћењу радног времена, лакше усклађују приватне и професионалне обавезе, итд. Рад на даљину подстиче запошљавање лица са отежаним кретањем, родитеља са хендикепираном дјецом, породиља које могу само дјелимично користити одсуство, незапослених лица у привредно неразвијеним мјестима, итд. Промоција иновација и ширење технологије су предуслови за добар квалитет живота, веће могућности запослења и смањење разлика у учешћу на тржишту рада, посебно у сеоским и удаљеним подручјима с проблемима старења и губитка становништва.[7] Недостаци рада на даљину су мањи обим социјалних контакта између радника, спорије професионално напредовање, смањена могућност за приправнички рад, увећани проблеми заштите података које радник обрађује, итд.

[6] Eurofound, *New forms of employment,* 2015, Publications Office of the European Union, Luxembourg, Преузето: 1.8.2021.https://www.eurofound.europa.eu/publications/report/2015/working-conditions-labour

[7] Европска комисија. *Изградња дигиталне будућности Европе*, Брисел, 19.2.2020. COM (2020) 67. Преузето : 1.9.2021. https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=COM%3A2020%3A0067%3AFIN

У међународном радном праву није усвојена посебна конвенција о раду на даљину и на раднике који га обављају примјењује се Конвенција о раду код куће број 177 упоредо са другим ратификованим конвенцијама Међународне организације рада, на начин да се једнако поступа према радницима независно од тога да ли раде у просторијама послодавца или ван ових просторија, односно да ли раде на типичан или атипичан начин.[8]

Рад на даљину се увијек обавља коришћењем информатичке опреме за разлику од рада код куће као традиционалног облик рада ван просторија послодавца. У смислу рада код куће, запослени обавља посао код куће или у другом простору по сопственом избору (*стационарни рад*), а рад на даљину карактерише већи степен аутономије запосленог у организацији рада, избору мјеста рада (*ротирајући рад*), распореду радног времена итд. Код рада на даљину радници обично користе персонални компјутер или другу опрему са екраном коју могу да користе и када су у покрету или на путу (*мобилни рад на даљину*) (Јовановић, 2018: 215). Основна особеност рада ван просторија послодавца јесте одсуство непосредне, строге и уобичајене контроле послодавца над радом запосленог, а надзорна овлашћења се прије своде на контролу резултата рада него на уобичајену контролу начина извршавања престације рада, независно од тога што се основна обавеза запосленог не састоји у предаји готовог производа или пружању одређене услуге, већ у стављању радних способности на располагање послодавцу (Шундерић, Ковачевић, 2019: 188). Рад ван просторија послодавца радник обавља у име и за рачун послодавца и такав рад не доводи у питање правну подређеност радника послодавцу као једно од основних обиљежја радног односа. Према Конвенцији бр. 177 из 2000. године и Препоруци бр. 184 Међународне организације рада о раду код куће, то је рад који подсјећа на самостално вршење рада у виду предузетништва, али радник нема степен аутономије и економске независности као предузетник (Мирјанић, 2020: 131). За рад на даљину је карактеристичан већи степен аутономије запосленог у начину извршавања рада, што је у теорији отворило питање да ли се ради о радном односу, који карактерише однос подређености, управљање резултатима рада запосленог од стране послодавца. Будући да терет ризика пословања сноси послодавац, а не запослени на даљину, то без обзира на аутономију запосленог у погледу радног времена и организације рада, радник на даљину ради за рачун и у име послодавца, тако да се не може сматрати самозапосленим лицем (Лубарда, 2013: 134).

[8] У преамбули ове конвенције је констатовано да се већина међународних конвенција рада и препорука које утврђују норме опште примјене у погледу услова рада може примијенити на раднике код куће. Конвенција Међународне организације рада о раду код куће број 177. (1996)

Рад на даљину је предмет регулисања законских одредби које се односе на овај облик рада или одредби које се односе и на рад на даљину и на рад код куће или одредби које се односе на рад код куће. У питању је континуирани рад ван просторија послодавца који радник обавља у облику стандардног или флексибилног радног односа тако што користи информационе технологија и електронски пренос података. Закони регулишу облик рада, додатни садржај у уговору о раду и обавезу заштите животне средине.

Конвенција број 177 о раду код куће се односи на рад у радном односу и примјењује на раднике који испуњавају предвиђене услове у погледу мјеста и плаћености рада, а што посматрано из угла теорије радног права значи да је у питању добровољан, плаћени рад који радник обавља лично уз субординацију од стране послодавца. Према Конвенцији израз "рад код куће" значи посао који радник ради накнаде обавља код куће или на другом мјесту према свом избору, осим простора послодавца и чији је резултат производ или услуга одређен од стране послодавца, без обзира коме припадају опрема, материјал и друга производна средства. Радници који обављају послове у просторијама послодавца могу повремено обављати послове ван тих просторија на начин да раде код куће или у другом простору, али тако не могу постати радници код куће (чл.1.).

Државе чланице Међународне организације рада које су ратификовале Конвенцију број 177 дужне су усвојити, примијенити и повремено ревидирати политику рада како би побољшале положај радника који раде код куће савјетујући се са најрепрезентативнијим организацијама послодаваца и радника (чл.3.). Упркос томе, промјене политике рада и државних извора радног права касне за промјенама које доноси рад на даљину. То кашњење није у складу ни са теоријом радног права која сматра да се динамичност радног права очитује у непрестаном мијењању и допуњавању, прописи радног права унапрјеђују и мијењају у складу са развојем економских и друштвених односа и да радно право карактеришу квалитативне и квантитативне промјене (Tintić, 1969: 22). Изгледа оправдан став како су промјене у правним системима споре, како не иду у корак са брзим друштвеним промјенама као што су промјене везане за организацију рада и нове облике рада и како би најбоље рјешење за послодавце и раднике на даљину било да уговором о раду покрију што већи број могућности и тешкоћа са којима би се могли суочити у међусобном односу, умјесто да пресуђивање препусте интерпретацији судова (Bilić, 2011: 638). Није спорно да преговори приликом закључивања уговора о раду не могу бити замјена за колективне преговоре, али ни то да је потребно избјећи радни спор.

Европска унија је покренула регулисање дигиталне трансформације закљученим Европским оквирним споразумом о раду на даљину, у циљу да постигне европску технолошку суверености засновану на европском социјалном моделу, издвајајући три циља: технологија у интересу грађана; економија која подстиче тржишну конкуренцију тако што предузећа под истим условима развијају, стављају на тржиште и употребљавају дигиталне технологије, производе и услуге; и демократско одрживо друштво.[9] У оквирном споразуму је рад на даљину дефинисан као облик организације и/или извођења рада уз употребу информационих технологија у оквиру уговора о раду у којем се посао који се може обављати у просторијама послодавца, редовно обавља ван тих просторија.[10] У складу са наведеном дефиницијом, радник на даљину је лице које обавља рад на даљину независно од тога да ли је такав рад установљен прије или у току заснивања радног односа. Како је истакнуто у литератури, овај споразум није инкорпорисан у директиву и постоји обавеза да се имплементира на прикладном нивоу националног система индустријских односа, а што значи у складу са праксом и процедуром карактеристичном за социјалне партнере држава чланица. Најчешћи начин имплементације је путем колективног уговора, други начин је путем заједничких смјерница, правилника и препорука о раду на даљину необавезујућег и добровољног карактера, а трећи начин имплементације је путем легислативе, што представља принцип претварања европског soft law у национални hard law (Bilić, 2011: 636).

Према Европском оквирном споразуму о раду на даљину, радници који обављају овај рад имају иста права као упоредиви радници који раде у просторијама послодавца, укључујући и право на једнаку зараду. Оквирни споразум наводи специфична обиљежја рада на даљину која представљају додатне елементе уговора о раду на даљину, а који се односе на организацију рада, обраду и заштиту података, коришћење информатичке опреме и интернета, извјештавање, надзор, приступ послодавца у просторије гдје се обавља рад, остваривање колективних права, итд. Према Конвенцији бр. 177 радници који раде код куће имају једнак положај као радници који обављају рад у просторијама послодавца у погледу права која се односе на зараде, заштиту пред инспекцијом рада, заштиту од дискриминације, социјално осигурање, стручно усавршавање, заштиту безбједности и здравља на раду, итд. а узимајући у обзир специфичности овог облика

[9] Европска комисија. *Изградња дигиталне будућности Европе*, Брисел, 19.2.2020. COM (2020) 67. Преузето : 1.9.2021. https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=COM%3A2020%3A0067%3AFIN

[10] Европски оквирни споразум о раду на даљину донијет 2002. године од стране социјалних партнера на европском нивоу (ETUC, UNICE i CEEP).

рада (чл. 2.). Међутим, према упозорењу Међународна организација рада није постигнута једнакост у пракси, те радницима који раде код куће треба обезбиједити праведне плате, социјално осигурање, регулисано радно вријеме, као и право да оснивају организације и учествују у њиховим активностима.

Права и обавезе радника који рад ван просторија послодавца су у посматраним законима о раду регулисана истим нормама као права и обавезе радника који раде у просторијама послодавца. Они имају једнака права и обавезе. Тако ЗРС (чл. 42) и ЗРХ (чл. 17) прописују да основна зарада запосленог (плата радника) који обавља рад ван просторија послодавца не може бити у мањем износу од основне зараде запосленог (плате радника) који ради на истим пословима у просторијама послодавца. Одредбе о радном времену, прековременом раду и прерасподјели радног времена, ноћном раду, одморима и одсуству примјењују се исто на раднике који обављају послове ван просторија послодавца, осим ако другачије није одређено општим актом или уговором о раду. У вези са заштитом здравља радника и достојанства на раду, Европска конфедерација синдиката се залаже за право на дисконектовање. Уколико би се омогућило право радника на дисконектовање које не би произвело никакве посљедице по радни однос могло би се закључити да је рад на платформама достојанствен са овог становишта (Ковачевић, 2019: 96). Право на дисконектовање значи да радници немају обавезу да одговарају на електронску пошту ван радног времена, што представља заштиту од прековременог рада и заштиту здравља.

Радници на даљину су исто као и радници који раде у просторијама послодавца одговорни за штету учињену послодавцу ако је учине намјерно или из крајње непажње. Радник има право да му послодавац надокнади штету коју претрпи у току рада на даљину, осим ако је штета настала кривицом радника или грубим немаром. Ако се између послодавца и радника не постигне договор о висини и начину накнаде штете, оштећени права може остварити путем суда. Поред тога, уговор о раду за обављање послова ван просторија послодавца садржи податке који одражавају разлике између положаја радника који раде у просторијама послодавца и ван ових просторија. Подаци се односе на трајање радног времена, врсту послова, услове рада, начин организовања рада, начин надзора над радом и квалитетом обављања послова, висину плате и рокове исплате плате, употребу и накнаду за употребу опреме радника и других трошкова рада. Уговор о раду за обављање послова ван просторија може да садржи и друга права и обавеза (на примјер, обавезу послодавца да набави и одржава средства за рад) (Мирјанић, 2020: 132).

Према Европском оквирном споразуму о раду на даљину послодавац проводи мјере којима спрјечава изолацију радника на даљину од радне заједнице у предузећу. Није спорно да социјални контакти радника који раде на даљину остварени путем информатичке опреме не могу у потпуности замијенити непосредне и личне међусобне контакте које могу да успоставе радници у просторијама послодавца. Посматрано с друге стране, коришћење информационих и комуникационих технологија омогућава да радници буду непрекидно и благовремено информисани о проблемима економског и социјалног развоја и на основи тога постизање повјерења између субјеката радних односа, а насупрот могућем запостављању информисања радника и маргинализацији социјалног дијалога (Мирјанић, 2017: 15).

3. Утицај пандемије на дигитализацију

Пандемија изазвана вирусом ковид-19 има значајан глобални утицај на дигитализацију рада и развој радног права. Епидемиолошке мјере су убрзале ширења рада на даљину и показале значај примјене информационих и комуникационих технологија за заштиту здравља на раду. Послодавци су да би обезбиједили континуитет обављања рада упућивали раднике на рад ван просторија послодавца, при чему дислоцирани рад може трајати колико траје пандемија. Закони о раду не садрже одредбе да је пандемија разлог за упућивање радника на рад ван просторија послодавца без измјене уговора о раду, али то није била препрека послодавцима да упуте раднике на рад ван радних просторија, нити да радници задрже иста права, укључујући и зараду, независно од тога да ли су упућени без измјене уговора о раду. Ако је законом регулисано право послодавца да у појединим случајевима може одредити радна мјеста на којима се послови обављају ван просторија послодавца, начин обављања ових послова, вријеме доступности радника послодавцу и слично, код темпоралног успостављања рада од куће није нужно мијењати уговор о раду. То је у складу са Конвенцијом бр. 177 која утврђује како повремено обављање послова код куће не значи својство радника од куће за раднике којима је послодавац омогућио рад од куће као привремену мјеру (Розић, Мехмедовић, Божичковић, 2020: 96).

Послодавац је у обавези да у рјешењу или у анексу уговора о раду, којим се запослени упућује на рад од куће наведе трајање радног времена према нормативима рада, начин вршења надзора над радом и квалитетом обављања послова запосленог, средства за рад за обављање послова које је дужан да набави, инсталира и одржава, коришћење и употребу средстава за рад запосленог и накнаду трошкова за њихову употребу,

накнаду других трошкова рада и начин њиховог утврђивања и друга права и обавезе, који су у вези са радом од куће запосленог (Урдаревић, Антић, 2020:37). Независно од пандемије или неког другог разлога, послодавац може раднику понудити измјену уговора о раду према којој би радник обављао рад ван просторија послодавца. Без обзира да ли је рад на даљину дефинисан у иницијалном опису посла на коме се заснива радни однос или касније, послодавац мора да писмено обавијести запосленог о свим важним елементима радног односа, укључујући све специфичности обављања послова на даљину. Правни прописи који регулишу рад на даљину у одређеним земљама (на примјер, Француска, Белгија, Пољска, Румунија, Мађарска, Словачка, Бугарска) изричито предвиђају да права и обавезе уговорних страна, организација рада и услови рада радника на даљину, морају бити регулисани у облику “анекса” уговора о раду (Каламатиев, Ристовски, 2020: 66). Радник може прихватити понуђени анекс уговора о раду и оспорити га у судском поступку или одбити анекс, али у том случају може добити отказ уговора о раду. Друкчије, када радник упути послодавцу приједлог измјене уговора о раду у циљу да ради на даљину умјесто у просторијама послодавца, послодавац није обавезан ни да прихвати понуду, нити да одговори на понуду.

Примјена епидемиолошких мјера је утицала на начин примјене неких института радног права, као што су радно вријеме, одсуство, годишњи одмор, заштита здравља и безбједности на раду, итд. у циљу да се радници удаље са мјеста рада. Проблем односа између правних одредби о правима и обавезама у радном односу и правних одредби о обавезним епидемиолошким мјерама је посебно изражен по питању заштите здравља и безбједности на раду. Како је уочено, „посебне околности” настале пандемијом Ковид-19 стварају „посебне” мјере и односе који детерминишу „стандардне” услове рада. То јесте детерминанта, али то не дерогира, а поготово не може „ставити ван снаге” хетерономне норме (нарочито норме *ius cogens*) којима се уређују правила заштите на раду. „Посебне обавезе” не смију онемогућавати остваривање права на заштиту здравља и безбједности на раду, али повећавају обавезе свих субјеката у тим односима, посебно послодавца. Изнад прописа и мјера у вези с пандемијом болести Ковид-19 су извори права заштите на раду, уз дословну примјену начела уставности и законитости и начела заштите лица на раду (Učur, 2021: 53). У прилог овог става може се навести то да је према Европском оквирном споразуму о раду на даљину, послодавац дужан да примјењује правила о безбједности и здрављу на раду у складу са директивама, законима и колективним уговорима.

4. Рад преко дигиталних платформи

Рад преко дигиталних платформи подстиче запошљавање и самозапошљавање незапослених лица. Са аспекта права на рад, уз помоћ дигиталних платформи ово право је учињено доступнијим, те су многи радници погођени кризом изазваном транзиционим процесом, помоћу ових платформи успјели да ријеше питање запослења (Антоновић, Галић, 2021: 250). При томе постоји разлика у томе да ли су платформе радницима који раде путем њих главни или споредни извор зараде. Истраживање које је 2016. провела Фондација за европске прогресивне студије у пет држава чланица ЕУ-а (Велика Британија, Њемачка, Аустрија, Низоземска и Шведска)[11] показало је да је 11% становништва тих земаља радило путем платформи. Међутим, за чак 45% испитаника тај облик рада осигуравао је мање од 10% укупних прихода. Само 2,4% испитаника истакнуло је да им рад путем платформи представља главни облик зараде (ФЕПС, 2016) (Butković, Samardžija, 2019: 20).

За разлику од типичног рада који је по правилу предмет стандардног радног односа, рад преко платформе је нетипичан рад код кога се разликују три лица - лице која обавља послове/радник, платформа и клијент/наручилац посла. Три стране у вези рада постоје код привременог запошљавања, а који је регулисано тако да је радник у радном односу са агенцијом за привремено запошљавање да би га она уступила предузећу кориснику да под његовим надзором и руководством ради одређено вријеме. За разлику од привременог агенцијског запошљавања, рад преко дигиталних платформи није предмет посебних одредби у радном законодавству. У Европској унији, прва је платформски рад уредила Француска, Законом о раду 2016. године, прописујући начело друштвене одговорности за платформе, а што подразумијева да оне требају радницима плаћати осигурање за случај несреће на раду и стручно оспособљавање, и поштовати право радника на синдикално организовање и штрајк (Vidas, 2021). Умјесто креирања нове категорије радника и уређивања њихових уговорних односа, Француска је одлучила да тој специфичној категорији радника гарантује одређена минимална социјална права под условима прилагођеним њиховој економској активности. (Garben, 2017: 32).

Основни проблем код рада преко онлајн платформе је статус лица која га обавља и питање да ли се оно налази у радном односу. Ради се о преиспитивању персоналног домета раднозаштитног законодавства, јесу ли пружаоци услуга преко платформи радници којима треба осигурати радноправну заштиту, самозапослена лица изван домета радног законодав-

[11] Велика Британија је 2016 била чланица Европске уније.

ства или се ради о потпуно новом облику рада који треба посебан правни статус. Лица која раде преко платформи најчешће формално класификују као самозапослена лица (Bjelinski Radić, 2018: 323-324). Питање које је овдје кључно је сљедеће: јесу ли пружатељи дигиталних услуга на платформама стварно самозапослени или дјелују у односу подређености – или овисности – у односу на тврtку или платформу? Имају ли право одбити неки задатак? Узимају ли износи њихове плаће у обзир чињеницу да користе и морају одржавати властиту опрему, да сами себи плаћају осигурање, да би требали плаћати доприносе за социјално осигурање, и да нису осигурани у случају болести или озљеде и несреће (Degryse, 2016: 14)?

У Конвенцији о раду код куће број 177 коришћени израз “рад код куће” се не односи на самозапослене раднике будући да они нису у радном односу. Самозапослени радник је лице ван радног односа које ради за себе као власник предузећа, фриленсер (freelancer) или независни извођач на основу уговора са предузећем које има партнерски однос са дигиталном платформом. Он проналази послове, сноси ризик пословања, плаћа доприносе и порезе, уз обавезу да предузећу посреднику и дигиталној платформи даје одређени проценат од зараде, при чему нема годишњи одмор, плаћено одсуство, итд.

Дигиталне платформе имају различите ставове о статусу лица које обавља рад, на начин да већина платформи сматра да су то самозапослена лица и да оне нису послодавци или посредници у запошљавању, док неке признају да су ова лица њихови радници и плаћају доприносе, а неке се залажу за “трећи статус” тако што их сврставају као лица између самозапослених и запослених лица.

Нека упоредна законодавства познају концепт „економски зависних лица”, односно „парасубординисаних лица” и дају овим лицима ограничену правну заштиту. Ради се о облицима рада који показују карактеристике и самосталног и несамосталног рада, стога се налазе у тзв. „сивој зони” између радног и грађанског права. Таква су лица формално самозапослена, али су економски зависна о једном наручиоцу посла (Vidas, 2021). Упркос општем ставу онлајн платформи, многе карактеристике односа указују на сличност са радним односом – радници регистрацијом на платформи прихватају њене услове коришћења, прихватају задатке на које им алгоритамски указује платформа, дају информације о доступности за обављање одређених задатака, у неким случајевима платформа намеће низ других обавеза које уколико се не извршавају, резултирају брисањем профила радника са платформе, а што указује на одређене елементе субординисаног односа радника и онлајн платформе. Степен сличности са радним односом

разликује се зависно од карактеристика односа између радника и онлајн платформе, са једне стране, и дефиниције појма радника утврђене законодавством примјењивим на конкретан случај. У овом погледу поставља се питање флексибилности постојећих дефиниција појма радника, начина квалификације појединих карактеристика радника на онлајн платформама, те, у коначници, постојањем и других видова заштите ових лица уколико се не призна њихов радноправни статус (Грубешић, 2019: 965). Дигитални рад врло често носи карактеристике рада у оквиру радног односа. Јер, иако је суштина рада на платформама флексибилан приступ у погледу обављања задатака, могућност слободног организовања времена проведеног у рјешавању истих, те слободно уговарање накнада са клијентима, а што су карактеристике статуса самозапослених лица, ипак је флексибилан приступ врло често ограничен надзором од стране самих платформи, наметањем обавезујућих инструкција у погледу обављања радних задатака, контролом квалитета извршеног рада, те одређивањем накнада за обављени рад (Грубешић, 2019: 977).

Европска комисија истиче да су још отворена питања у вези правне заштите лица која немају статус радника, а са радницима дијеле одређене осјетљиве тачке. Европски одбор регија сматра да утврђивање постојања радног односа треба заснивати на чињеницама које се односе на стварно обављање рада, а не на то како странке описују однос и да при томе треба поћи од дефиниција у важећем праву, колективним уговорима или пракси у државе чланице. Одбор наводи да је највећи изазов за социјалне партнере питање како доћи до радника у најновијим облицима запослења као што је рад путем дигиталних платформи, те позива на доношење мјера за подстицање и олакшавање социјалног дијалога у том сегменту тржишта рада.12 Са техничке стране, дигитализација значајно олакшава комуникацију у социјалном дијалогу, а при чему се социјални дијалог може посматрати упоредо као процес у коме партнери учествују у рјешавању конкретних питања која не утичу на промјену поретка, али и као дуготрајни континуирани процес у коме партнери утичу на постепене промјене поретка (Мирјанић, 2014: 131).

Традиционална улога синдиката да организује раднике је у колизији са радницима који раде на платформама које им формално негирају статус радника, а тиме и право на удруживање у синдикате ради заштите економских и социјалних интереса. У литератури се тако често налазе ставови да постојећи начини дјеловања синдиката морају еволуирати како

[12] Мишљење Европског комитета региона. Рад кроз платформе – регулаторни изазови на локалном и регионалном нивоу. Службени лист Европске уније, (2020/C 79/07) Посјећено: 25.08.2021.

би нашли начин синдикалног организовања те специфичне категорије (Bjelinski Radić, 2018: 327). Препрека за синдикално организовање је недостатак комуникације између радника који раде преко платформи. Радник на дигиталним платформама може се повезати са другим запосленима широм свијета ради размјене искустава у раду. Иако ово представља једну врсту социјалне интеграције, социјална интеграција одвија се најчешће виртуелно. Ови радници свој социјални капитал креирају у виртуелном свијету дигиталних платформи, те се њихови канали комуникације своде на размјену искустава путем мејла, друштвених мрежа и других видова виртуелно посредоване комуникације. Тако је за адекватну заштиту права на рад и права радника, поред синдикалне заштите кључна радничка организација. У вези с тим су настале радничке задруге као посебан облик радничког организовања, а најприје као платформске задруге са циљем стварања конкуренције радним дигиталним платформама. Радничке платформе су по уређењу личиле на дотадашње дигиталне платформе, а заправо су уређене по моделу који погодује раднику и радничким интересима (Антоновић, Галић, 2021: 254). Поред недостатка комуникације, као фактори који утичу на синдикализацију ових радника истичу се: радници се не познају лично, лични однос радника према послу којег обављају преко платформи (као примарна или секундарна професионална активност), велика флуктуација радника те директна конкуренција радника на платформи међусобно (кроз појединачне оцјене и конкурентне методе расподјеле посла). Ови фактори не доприносе солидарности и сарадњи, а који стандарди су неопходни за синдикално удруживање; томе се може додати и чињеница да се радници на платформама често поистовјећују са самозапосленим лицима, што и из формалног угла може искључити синдикално удруживање (Garben, 2017: 4).

Европски синдикати траже да се лицима која раде преко дигиталних платформи признају основна права која припадају радницима, полазећи од става да то нису самозапослена лица, већ радници који имају право на минималну плату, право на плаћени годишњи одмор и социјална права. У погледу услова рада на дигиталним платформама Европска конфедерација синдиката у својој резолуцији под називом Ка праведном дигиталном раду, захтијева: добар и правичан дигитални рад заснован на добрим условима рада, сигурном радном окружењу и фер радним односима, и ЕУ оквир за раднике на платформама да би се заштитила њихова основна права (право на зараду, радно вријеме, социјално осигурање, итд.). Конфедерација захтијева да се користе репрезентативна тијела за организовање самозапослених радника и да представници радника у управним одјељењима компанија врше надзор над увођењем нових технологија,

да се користе колективни преговори да би се примијенила нова права у вези са дигитализацијом и да синдикати активно прате дигитализацију како би конфедерацији омогућили да склопи што повољније споразуме о разним облицима дигитализације рад (Ковачевић, 2019: 94). Радници дигиталних платформи теже синдикалном организовању у циљу законског регулисања радног статуса и права која им припадају по основу рада.[13]

Новост дигитализације су дигитални номади, а који обично као фриленсери обављају послове програмирања, графичког дизајна, дигиталног маркетинга, новинарске и друге послове који се могу обављати преко интернета. Разлози за појаву дигиталних номада су различити, а најчешће су то бољи животни стандард, тражење пословних веза, повољнији климатски услови, здравији стил живота, авантуризам, епидемија, итд.

5. Закључак

Основно питање које се поставља приликом законског регулисања радног положаја, права и обавеза лица која раде на даљину и преко дигиталних платформи је питање да ли ова лица обављају рад у радном односу или ван радног односа. Регулисања положаја, права и обавеза радника који обављају рад на даљину или неки други облик рада ван просторија послодавца на начин да они користе информационе и комуникационе технологије као средство рада, касни за развојем облика дигиталног рада. Законско регулисање правних односа који се успостављају у вези овог рада је у правилу, начелно и само дјелимично, те је садржај права и обавеза радника предмет преговора који претходе закључивању уговора о раду. Тако није могуће изједначити садржај права и обавезе ових радника са садржајем права и обавеза других упоредивих радника. У питању је нормативни приступ који не одговара успостављеној пракси да се уговором о раду ближе регулишу права и обавезе радника и послодавца која су претходно јасно и прецизно регулисана хетерономним и аутономним изворима радног права. Рад на даљину, као и други облици рада ван просторија послодавца нису регулисани прецизно, јасно и гипко, иако није спорно да је то важно учинити полазећи и од преднормативних истраживања о утицају дигитализације на рад. На нормативне недостатке указује и раширена правна пракса која у циљу примјене епидемиолошких мјера одступа од законских одредби. Показало се да недостају законске одредбе о привременом и повременом упућивању радника на рад на даљину, али

[13] Као примјер синдикалног организовања ових лица може се навести да је у Хрватској основан Синдикат радника дигиталних платформи чии је циљ побољшање њихових радних услова.

и одредбе о примјени других института радног права у циљу заштите здравља радника од заразних болести. Пракса указује да се послије краја пандемије може очекивати тренд да привремени рад на даљину постане трајни облик рада за многе раднике који су вољни да на приједлог или уз сагласност послодавца, наставе и даље обављати послове дјелимично или у цјелости у облику рада на даљину. За трајно обављање рада на даљину потребна је писана сагласност радника у облику анекса или новог уговора о раду који садржи специфичности овог рада.

За раднике који обављају флексибилне облике рада је важно да су им права изједначена са правима упоредивих радника који раде у просторијама послодавца, али је важно да се не умањи значај стандардних радних односа на којима почива радно законодавство. Регулисање рада на даљину је важно и зато што подстиче запошљавање родитеља са малом и болесном дјецом, лица са отежаним кретањем, незапослених лица становника привредно неразвијених мјеста, итд.

Заштита права лица која раде преко дигиталних платформи је важан мотив да се они синдикално организују, укључујући и оснивање струковних синдиката. Синдикати су по својој улози позвани да учествују у преговорима и социјалном дијалогу који имају за предмет аутономно регулисање нестандардних радних односа унутар дигиталне економије. У литератури је присутан захтјев да треба додатно регулисати услове рада радника који раде унутар дигиталне економије, посебно услове за образовање и усавршавање за коришћење информационих и комуникационих технологија као све важнијег професионалног захтјева. Улога синдиката је да утиче да се радна и социјална сигурност радника који обављају рад на даљину изједначи са радном и социјалном сигурношћу радника који раде у просторијама послодавца, али и да заштити радну и социјалну сигурност самозапослених радника.

Литература

Atkinson R.D., McTernan M. Reed A. (ur.) (2015.) *Sharing the success of the digital economy, a progressive approach to radical innovation*. London: Rowman & Littlefield International. Преузето из: Degryse, C. (2016). Digitalizacija ekonomije i njezin utjecaj na tržišta rada. Zagreb: SSSH.

Анђелковић, М. Радосављевић, М. Лилић, В. (2021). Дигитална економија у четвртој индустријској револуцији. *Међународна конференција право, економија и менаџмент у савременим условима – LEMiMA 2021.*

Антоновић, Р. Галић, Б. (2021). Право на рад у савременим условима дигитализације. *Правна ријеч. Удружење правника Републике Српске*. 64/21.

Bilić, A. (2011). Rad na daljinu prema međunarodnom, europskom i hrvatskom radnom zakonodavstvu. *Zbornik radova Pravnog fakulteta u Splitu*, 3(XLVIII).

Bjelinski Radić, I. (2018). Izazovi radnog i socijalnog prava u svjetlu digitalizacije rada. *Zagrebačka pravna revija,* 3(VII). 309-331.

Brković, R. Antonović, R. Global changes in employment in the Republic of Serbia, *Ius Romanum*, 2/19. 273-287.

Butković, H. Samardžija, V. (2019). *Digitalna transformacija tržišta rada u Hrvatskoj,* Zagreb : Institut za razvoj i međunarodne odnose.

Vidas, I. (2021). *Posebni oblici rada - rad putem digitalnih platformi*. Preuzeto 25.08.2021. https://www.iusinfo.hr/aktualno/u-sredistu/45739

Garben, S. (2017). *Protecting Workers in the Online Platform Economy: An overview of regulatory and policy developments in the EU*. European Agency for Safety and Health at Work.

Гиденс, Е. (2007). *Социологија.* Београд: Економски факултет.

Грубешић, И. (2019). Редефинисање појма радник у условима рада на online платформама. *Зборник радова Слобода пружања услуга и правна сигурност*, Правни факултет Крагујевац. 959-981.

Јашаревић, С. (2016) Утицај дигитализације на радне односе. *Зборник радова, Правног факултета у Новом Саду*, 4(L). 1103–1117.

Јовановић, П. (2018). *Радно право*. Нови Сад: Правни факултет Универзитета у Новом Саду.

Јовевски, Л. (2021). Дигитална трансформација радних односа - правни и економски изазов у новој декади. *Зборник сажетака са Међународне научне конференције Право и дигитализација Ниш.*

Каламатиев, Т. Ристовски, А. (2020). Рад на даљину (telework) као "одговор" на кризу узроковану COVID-19 - услови и изазови с којим се суочава македонско радно право. *Радно и социјално право, Удружење за радно право и социјално осигурање Србије*, 1(24). 61-84.

Ковачевић, А. (2019). Ка достојанственом дигиталном раду – Положај радника на дигиталним платформама. *Годишњак Факултета политичких наука Универзитета у Београду*. 22(XIII). 85-100.4

Лубарда, Б. (2013). *Увод у радно право.* Београд: Правни факултет Универзитета у Београду.

Мирјанић, Ж. (2014). Значај социјалног дијалога у процесу усклађивања домаћег права са правом Европске уније. *Зборник радова Правног факултета у Нишу*. 68 (III). 129-142.

Мирјанић, Ж. (2017). Influence of technologies to social actors. *Proceedings 9th International Scientific Conference*.

Мирјанић, Ж. (2019). Заштита личних података запослених у условима коришћења информационих технологија. *Зборник радова Правног факултета у Нишу*. 85(LVIII). 153-181.

Мирјанић, Ж. (2020). *Увод у радно право, књига прва*. Бања Лука: Правни факултет Универзитета у Бањој Луци.

Negreiro, M. Tamiama M. (2019). *Digitalna transformacija*. Služba Evropskog parlamenta za istraživanja.

Обрадовић, Г. (2021). Границе послодавчевог права на електронски надзор над запосленим. *Зборник сажетака са Међународне научне конференције Право и дигитализација Ниш*.

Розић, И. Мехмедовић, Е. Божичковић. Н. (2020). Радни односи у доба пандемије: могу ли флексибилни облици рада бити адекватан одговор на изазове ванредних околности. *Радно и социјално право, Удружење за радно право и социјално осигурање Србије*. 2(24). 83-101.

Tintić, N. (1969). *Radnovil i socijalno pravo*. Zagreb: Pravni fakultet.

Урдаревић, Б. Антић, А. (2020). Нека отворена питања у погледу рада код куће за време пандемије вируса. *Радно и социјално право, Удружење за радно право и социјално осигурање Србије*, 2(24). 27-40.

Učur, M. (2021). Niti jedna odredba niti mjera u "posebnim okolnostima" ne smije derogirati načelo ustavnosti i zakonitosti niti načelo zaštite osobe na radu. *Radno pravo*. 06/21.

Шундерић, Б. Ковачевић, Љ. (2019). *Радно право*. Београд: Службени гласник.

Željko Mirjanić, LL.D.,
Full professor at the Faculty of Law,
University of Banja Luka,
Republika Srpska, Bosnia and Herzegovina

THE INFLUENCE OF DIGITALISATION ON LABOUR LAW

Summary

The significance of this topic is that it actualizes the need for a multidisciplinary approach to the whole spectrum of issues that the development of information and communication technology and the digitization of business and work brings to labour law, such as work from home, the issue of protection of personal data of employees etc. By changing the standard business environment to a new one, whose main features are globalization, digital economy, flexibility and development of digital companies and businesses, business conditions are affected. This includes, among other things, changes in the way of acquiring knowledge and education and changes in the system of personal and social values. Technologies have changed the way of life of individuals, their communication mode, and in this way, they ushered in the new information society.

In the present phase of the information society, the only way of systemic protection and development is the quality information and training of cadres for the rational functioning of the world of information. Through information technologies the employer collects, processes, uses and saves personal data of his employees, that are necessary for exercise of rights and obligations during the employment relationship. One of the consequences is the establishment of new social norms, to which individuals and society as a whole are adapting. Increasingly, profit became the most important goal, and the question arises as to how long is the human society willing to tolerate this phenomenon. The current stage of labour law development is based on the concept of social market economy and the change of the labour world being affected by the concept of neoliberal globalization. The path of further development of national labour law depends upon the adjustment of European labour law and labour law in the EU member states to most important changes in the world of work and capital.

Establishing of sustainable social peace is lacking mutual confidence between the social actors. The state, as an organization of citizens, must assume the role of a balancer between the labour and the capital. This confidence can be built through use of information technologies, as they enable permanent information about economic and social development. The use of information technologies is speeding-up evolutionary changes in the world of labour and facilitates the social dialogue as

a form of institutionalized social dialogue, directed towards solving the most important problems in the sphere of labour.

Keywords: *labour law, harmonization of labour law, protection of privacy and personal data of employees, work from home.*

CIP - Каталогизација у публикацији

Народна библиотека Србије, Београд

34(082)

004.9(082)

МЕЂУНАРОДНА научна конференција Право и дигитализација (2021 ; Ниш)

Зборник радова / Међународна научна конференција Право и дигитализација, Ниш, 2021. = Collection of papers / International Scientific Conference Law and digitalization ; [организатор конференције, conference organizer Центар за правна и друштвена истраживања ; уредници, editors-in chief Горан Обрадовић, Марко Димитријевић]. - Ниш : Правни факултет Универзитета, 2021 (Ниш : Медивест). - 218 стр. ; 25 cm

Радови на срп. и енгл. језику. - Тираж 80. - Реч уредника: стр. 5. - Апстракти ; Summaries.

ISBN 978-86-7148-286-8

а) Право -- Зборници б) Дигитализација -- Зборници

COBISS.SR-ID 54350345