CHALLENGES IN MANAGING INTELLECTUAL PROPERTY RIGHTS DURING CORONAVIRUS PANDEMIC

Mario Lukinović[1]
Larisa Jovanović[2]
Vladimir Šašo[3]

DOI: https://doi.org/10.31410/ITEMA.2020.239

Abstract: *The socio-economic impact of the pandemic on all social spheres is huge, but like any crisis, for some it is an opportunity to create, develop and promote solutions. The coronavirus pandemic has brought many changes. It has forced us all to find new ways of working, interacting and living. The field of intellectual property is particularly affected by the coronavirus pandemic, its strong influence has affected all branches of intellectual property, especially the field of copyright and patents. During the COVID-19 Pandemic, numerous anomalies in the consumption of copyrights were observed, which coincided with the isolation measures, from drastically increased consumption of illegal pirated content via the Internet, especially in countries with lockdown, through a sharp increase of Disney+ and Netflix streaming platform users.*
The identification of products that have the word Corona in their name – in their trademark, with the virus has led to a sharp drop in consumption of some products, but also to increased sales of others. The pharmaceutical industry has invested huge funds in the fight against this global challenge, especially in the field of treatment of viruses, new drugs for the prevention, as well as finding a vaccine against COVID-19. This paper discusses the challenges faced by the management of intellectual property rights and potential response measures.

Keywords: *COVID-19, Innovation, Intellectual property, Patents, Coronavirus pandemic, Generics, Drugs, Vaccines, Cybersecurity.*

1. INTRODUCTION

Application of protective measures, that was introduced by the majority of governments world-wide in order to lessen the consequences of the pandemic, impacted them in different ways and to a different extent, depending on the nature of activities of given business subjects. Even though the pandemic is gradually subsiding in a significant number of countries, the vaccine still does not exist, and the fears are still growing stronger; people fear not only its return in the colder autumn and winter periods, but also the possible sudden spread in the southern hemisphere, especially in the regions with a common lower level of hygiene among local population. The impact it leaves behind itself is enormous, and it is especially significant in the field of intellectual property. Isolation of population had a great impact on the increase in consummation of authorship works (reading books, watching movies, listening to music, etc.), while the activity of scientists in the field of inventions is extremely grand.

[1] Faculty of Law, UNION University, Belgrade, Serbia
[2] ALFA BK University, Belgrade, Serbia
[3] ALFA BK University, Belgrade, Serbia

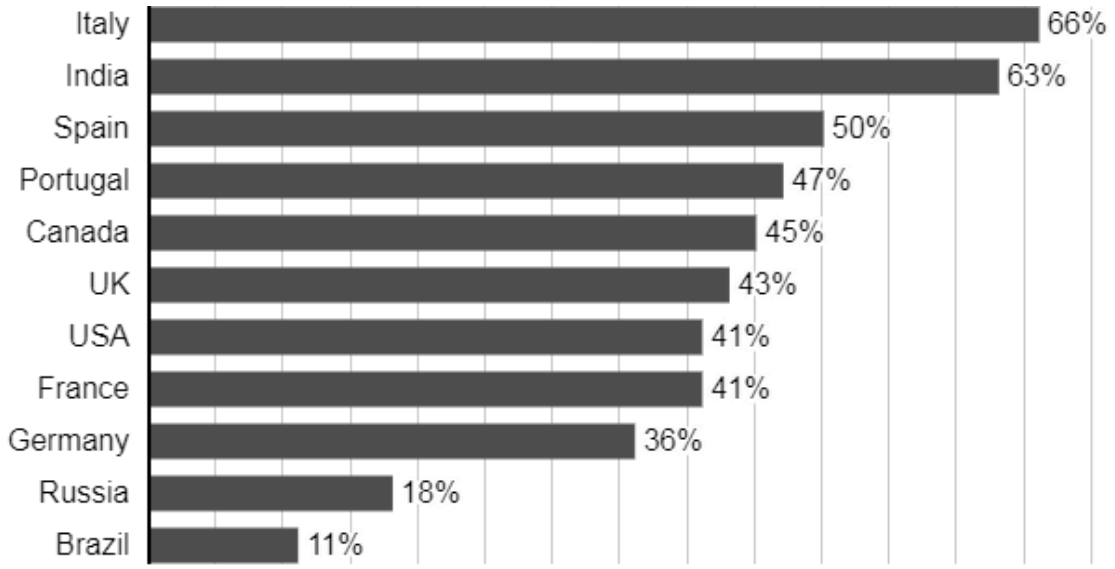
2. CHALLENGES OF MANAGING COPYRIGHTS DURING CORONAVIRUS PANDEMIC

The ban and restriction of movement directed the offer of content towards the Internet, many museums, galleries, theaters, etc. instead of classic tours, offered millions of users a virtual tour. Even some of the contents whose contents imply exclusively in vivo communication with visitors (virtual tours of national parks, children's camps, etc.), offered new types of communication which imply the consumption of author's works at a distance.

Everyone tried in their own way to be a part or to give their contribution; many companies, creators and traders offered protective masks with different designs and motifs, as well as T-shirts with messages of the funniest nature related to COVID-19.

Social distancing and millions of people in isolation have caused a drastic increase in watching online movies and TV series. American media provider *Netflix* has, during the COVID-19 pandemic, acquired 16 million of new subscribers on its streaming platform (Ryan et. al., 2020). At the same time, British company MUSO's data, which follows thousands of pirate platforms and contains a database on digital online content in 196 countries, speak of a drastic increase of Internet piracy, which is directly correlated with isolation measures. Since the last week of February and the first week of March, when mass isolation measures commenced, a drastic increase was recorded world-wide. According to this data, we can almost observe the level of isolation measures taken in certain countries. In Italy, the country which was, at one point, most harshly hit by the pandemic, the increase of movie piracy reached unbelievable 66%. Repressive isolation measures were especially strictly taken in India, where the said increase amounted to 62%; afterwards, Spain overtook the primacy from Italy, when speaking of the number of infected individuals, and illegal consumption of authorship has increased for 50%; in Britain, during the same period, the increase amounted to 43%, and in the United States, it amounted to a 41% (Chatterley, 2020).

Figure 1. Increase of movie piracy in February/March of 2020



Source: MUSO

The graph expresses the increase of movie piracy during the last week of February, in comparison to the first week of March. It is well noticeable that the highest peak occurred in

Italy, India and Spain, that is, in the countries that, exactly at that time, commenced implementation of strict isolation measures.

Parallel to exponential increase of number of visits to websites containing pirated content during the times of pandemic, the number of websites containing illegal streaming of sports events decreased, given that there are no sporting events. The loss of emitters of sports programs is enormous. They are directly dependent on their viewers, given that their massiveness brings them profit, not only from subscriptions, but from commercials as well. Without sporting transmissions, none of the previously mentioned exists. This vicious circle also includes professional athletes, whose high profits depend in many ways on TV rights, paid by cable and Internet providers.

Companies such as Disney, which have a high dispersion of authorship rights, are currently counting their losses. While Disney streaming platform acquired a record of 32 million subscribers, thanks to a great extent to isolation measures, great losses occurred due to closing of Disney parks in America, Japan, France and China, and the world premiere of "Mulan" movie was postponed due to the pandemic. Disney faced certain loss also due to reduced possibility for merchandising product placement.

The Dutch media and fashion company *RUMAG* (acronym made of the title *RUDE MAGAZINE*), famous for production of T-shirts, mugs, etc. with funny, vulgar or sexual quotes, was publicly accused of copyright infringement. The majority of quotes and slogans that they print on their products (in white lettering on a black background) were taken from social networks and other sources. During the pandemic, they have decided to introduce a special Corona collection to the market, and the entire revenue was intended for the Red Cross. Some of the quotes that sounded funny in the context of the pandemic were taken from the songs of authors popular in the Netherlands. Even though the authors of the said quotes were listed, and the funds were donated for charity, the pressure of the public on *RUMAG* was so strong that the CEO resigned.

Do producers, such as *RUMAG* company, commit infringement of authorship by such conduct? The laws on authorship of the majority of countries do not provide a legal authorship protection to small textual and artistic forms (short phrases and slogans, ornaments, etc.) (Bogdanović, 2017), and they are seen as the so-called "bits of authorship rights". Certain slogans, ornaments and phrases are protected with a trademark, and in such a way, they enjoy legal protection.

No lawmaker can foresee all life situations. When there is not a legally prescribed provision for a normative solution of a certain problem, we resort to analogy through implementation of suitable rule from a different source. In praxis, commercial use of the title of an authorship work (movies, songs, etc.) without the approval of the carrier of authorship, is very common. Within the contemporary Comparative Law, not all national legislation provides the same protection to a title. If original, the title is regarded as an authorship and enjoys independent protection within the French law. On the contrary, in Great Britain, it is defined that, in the case of use of the same or similar title for the same type of work, the protection might be demanded on the basis of the provisions on fair competition (Spasić, 2011).

According to our Law on Authorship and Familiar Rights, if the title of a work is an original, it represents the subject of authorship legal protection, independently from the piece that is marked by the said title. In praxis, however, not many titles can enjoy such a status. If the title of a work is not an original to the extent that it represents an authorship itself, but is regarded

as an integral part of the authorship named by the said title, the use of the work without its title or with a changed title is regarded as an infringement of authorship of the said title.

3. MANAGING PATENTS DURING CORONAVIRUS PANDEMIC

Nowadays, the Earth is inhabited by the highest number of habitants since its inception (currently numbering more than 7,5 billion), of which a significant percentage inhabits urban settings where they come to a close contact among themselves on a daily basis. Population fluctuation is higher than ever, and airlines have, during the course of 2019, transported more than 4,5 billion of travelers, which is more than double in comparison to the previous year. Transportation decreases distance, and thus, the world has become a "global village" in which, and all thanks to transportation, infections can reach, together with passengers, another side of the planet in just a day. Because of that, the possibility of spreading viruses will continue to grow in the years that shall follow, and the response of the humanity cannot remain in the scope of increasing physical distancing measures and other preventive measures; it is hidden in thousands of laboratories world-wide, where scientists must create new inventions for repressing their impact.

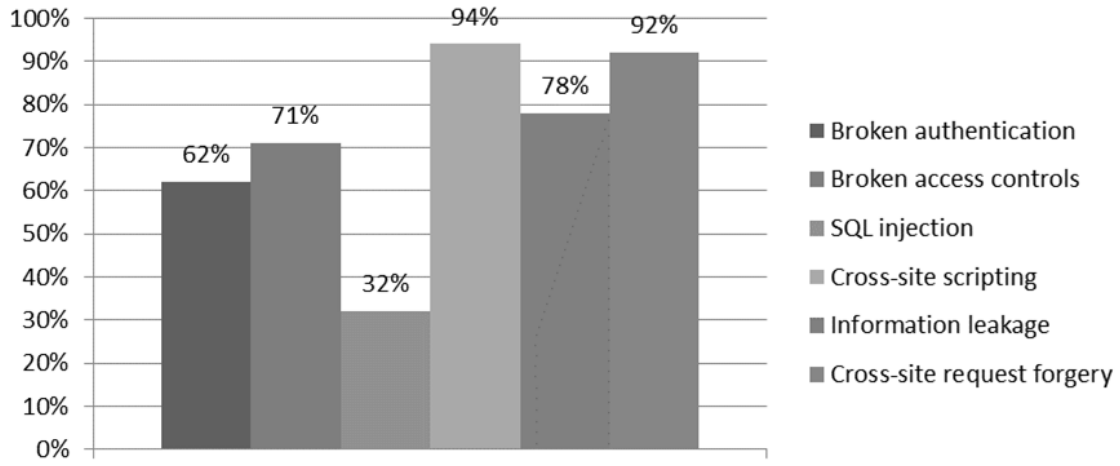
rom the invention of the first wheel, to cuneiform, steam machine, penicillin and even a computer chip, innovation represented progress, but also survival (Lukinović, 2017). A patent is a law which protects inventions. It is an award in the form of monopoly rights, given by the state to the inventor for his innovative success, materialized through a unique position on the market (Lukinović et al. 2017). The industrial property protection system is not seen as a goal itself, but as means for encouraging creative work. In order for authors and inventors to be encouraged to create, state provides them with privileges in the form of legal protection, authorship rights or inventions. Through these instruments, individuals are actually being put in the function of the general thing representing progress, as a result of some authorship work or an invention.

4. INTERNET ATTACK AND WEB APPLICATION VULNERABILITIES CAUSED BY COVID-19

Whenever a new crisis emerges, different criminal actors are the first to jump on the occasion to exploit unsuspecting victims in times of fear, uncertainty and doubt. These exploits take multiple forms, from the physical to the digital world. History has taught us that the most efficient method to initially counter these threats is through prevention and awareness towards all levels of corporate and personal life.

There is a widespread awareness of web application security issues. Users are often called upon to verify certificates because they want to entrust their information to serious organizations that store their data behind advanced cryptographic protocols. Based on the examination of security vulnerabilities of web applications in the period from 2016 to 2019, we can single out the following categories of attacks:

Figure 2. Frequency of web application vulnerabilities in the period from 2016 to 2019



Source: https://www.academia.edu/35796648/Upravljanje_bezbednoscu_u_Cyber_prostoru_i_mehanizmi_zastite_web_aplikacija

Table 1. Vulnerabilities and categories of attacks in the period 2016-2018.

Disadvantages of authentication	Include compromising and abusing various shortcomings of the system login mechanism. The method of random guessing of the user code is most often used here.
Broken Access control	Deficiencies are a case where an application is unable to protect access to data and resources. Here, the attacker is allowed to access sensitive user data on the server, or to perform privileged actions.
SQL injection	Allows an attacker to modify an SQL query intended for a database. In this way, the attacker may be able to access the data stored in the database.
Cross-site scripting	Allows an attacker to attack other users of the application, as well as gain access to their data or perform unauthorized actions on their behalf.
Cross-site requests forgery	Allows an attacker to perform unwanted actions on behalf of the user of the application. The attack is realized based on the visit of the malicious site by the victim, after which the user's browser performs certain actions that the user does not intend to do.
Information leakage	Includes cases where the application displays sensitive information that is useful to the attacker in developing mechanisms against the application itself, by printing error messages and other similar behavior.

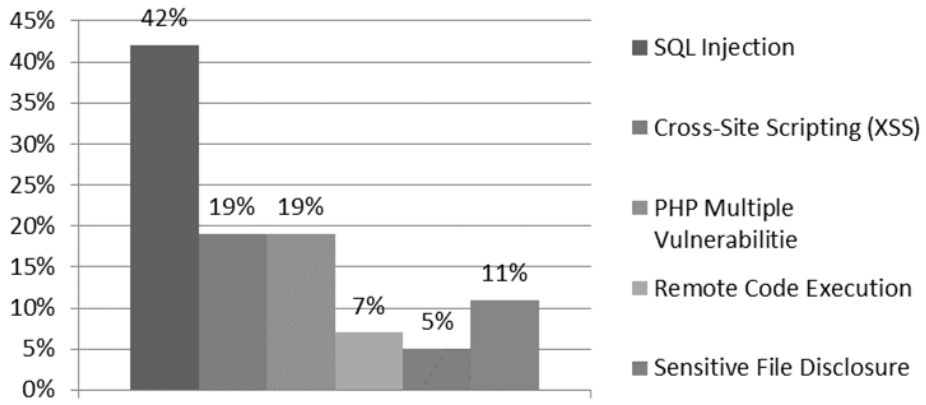
Website attack attempts per day grew by 59% from January 2018 to December 2018, ending at a peak of 80 attacks per day and averaging 62 attacks per day for the year. Rising attack volume suggests cybercriminals are automating their attacks to expand their reach and frequency. However, the sample of infected websites remained steady at about 60,000 throughout the year, indicating that website security tools are likely becoming more successful at combating the increasing number of attacks.

As 5G networks roll out, the use of connected IoT devices will accelerate dramatically. They will increase networks' vulnerability to large-scale, multi-vector Gen V cyber-attacks. IoT devices and their connections to networks and clouds, are a weak link in security. It's hard to get visibility of these devices that can have complex security requirements. What's needed is a more holistic approach to IoT security, combining traditional and new controls to protect these ever-growing networks across all industry and business sectors.

Many organizations have shifted workloads to the cloud. However, the level of understanding as to securing them remains dangerously low. Security is often an afterthought as traditional security can be perceived as inhibiting business agility. This is why security solutions need to evolve to a new paradigm of flexible, cloud-based, resilient architectures that deliver scalable security services at the speed of DevOps. Cloud computing is fastmoving and dynamic. As organizations adopt new and more efficient cloud-based services and technologies to meet their business needs, cloud attack vectors become more complex and diversified. An additional concern is that cloud has enabled the increase in the speed and agility of development teams to use new technologies, but security controls for these new technologies often lag behind new technology adoption.

Next figure shows most common critical vulnerabilities in 2020 (Internet facing):

Figure 3. Most Common Critical Vulnerabilities in 2020 (Internet facing)



Source: https://landing.edgescan.com/hubfs/BCC030%20Vulnerability%20Stats%20Report%20(2020)_WEB.pdf

Table 2. Vulnerabilities and categories of attacks 2020.

SQL injection	SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.
Cross-site scripting (XSS)	Cross site Scripting (XSS) attacks are a type of injection problem, in which malicious scripts are injected into web sites. Cross site scripting flaws are the most prevalent flaw in web applications today. Cross site scripting attacks occur

	when an attacker uses a web application to send malicious code, generally in the form of a browser-side script, to a different end user. The 'stored' variant is considered a "Critical" vulnerability as it persists across all users who access an infected page and has the potential to infect a wide user base of the web application or site.
Php multiple vulnerabilities	Many PHP vulnerabilities were discovered with ratings including both high and critical risk. Many PHP deployments have multiple vulnerabilities concurrently. PHP is still a widely used programming language but loosing popularity. Millions of sites on the Internet use PHP and will for some time to come
Remote code execution	Remote code execution (RCE) is used to describe an attacker's ability to execute arbitrary commands or code remotely across the Internet or network on a target machine. This is achieved by exploiting a vulnerability which generally, if known about, could be mitigated via a patch or configuration change
Sensitive file disclosure	This is the result of leaving unprotected files on a hosting environment, systems using inadequate authorization or poorly deployed systems which result in directory listing and sensitive data disclosure. A recent trend in such a vulnerability, are exposed AWS S3 buckets which are misconfigured, resulting in publicly exposed database back up files, internal files, configuration files and other private information being left available on the Internet

Vulnerabilities may result in complete compromise of a system or a user. They are generally highly likely to occur, high impact or both. SQL Injection was first discovered in 1998 and still lives on the Internet today together with XSS and RCE.

Since the beginning of the outbreak, a total of 90,284 new corona related domains have been registered globally. Many of them were found to be malicious and suspicious.

More online transactions mean more opportunities to hack credit card data, and people working remotely have opened up new ways for criminals to target both individuals and organizations.

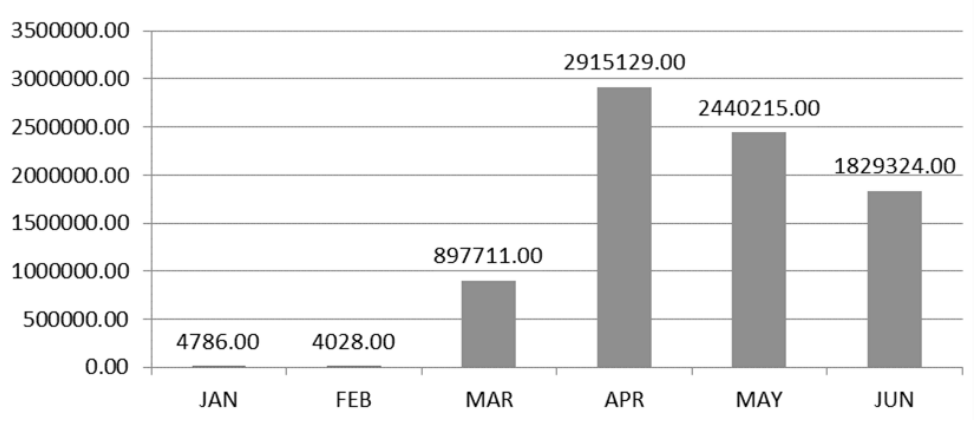
Key findings highlighted by the INTERPOL assessment of the cybercrime landscape in relation to the COVID-19 pandemic include:

- **Online Scams and Phishing -** Threat actors have revised their usual online scams and phishing schemes. By deploying COVID-19 themed phishing emails, often impersonating government and health authorities, cybercriminals entice victims into providing their personal data and downloading malicious content. Around two-thirds of member countries which responded to the global cybercrime survey reported a significant use of COVID-19 themes for phishing and online fraud since the outbreak.
- **Disruptive Malware (Ransomware and DDoS) -** Cybercriminals are increasingly using disruptive malware against critical infrastructure and healthcare institutions, due to the potential for high impact and financial benefit. In the first two weeks of April 2020, there was a spike in ransomware attacks by multiple threat groups which had been relatively dormant for the past few months. Law enforcement investigations show the majority of attackers estimated quite accurately the maximum amount of ransom they could demand from targeted organizations.
- **Data Harvesting Malware -** The deployment of data harvesting malware such as Remote Access Trojan, info stealers, spyware and banking Trojans by cybercriminals is on the rise. Using COVID-19 related information as a lure, threat actors infiltrate systems to compromise networks, steal data, divert money and build botnets.
- **Malicious Domains -** Taking advantage of the increased demand for medical supplies and information on COVID-19, there has been a significant increase of cybercriminals

registering domain names containing keywords, such as “coronavirus” or “COVID”. These fraudulent websites underpin a wide variety of malicious activities including C2 servers, malware deployment and phishing. From February to March 2020, a 569 per cent growth in malicious registrations, including malware and phishing and a 788 per cent growth in high-risk registrations were detected and reported to INTERPOL by a private sector partner.

- **Misinformation** - An increasing amount of misinformation and fake news is spreading rapidly among the public. Unverified information, inadequately understood threats, and conspiracy theories have contributed to anxiety in communities and in some cases facilitated the execution of cyberattacks. Other cases of misinformation involved scams via mobile text-messages containing 'too good to be true' offers such as free food, special benefits, or large discounts in supermarkets. The concepts of misinformation and disinformation are not new. Evidently, the current situation has made it easy to spread this across all social platforms. A very large portion of Internet users are confined in their homes and are using the Internet in a heightened capacity which enables misinformation to be posted, re-posted and added upon across any media. The techniques used are very complex and can take many forms. There are websites that are trying to investigate misinformation related to COVID-19. In a little over a month, more than 50 articles have been debunked and proven false. It has become exceedingly difficult to keep up with the amount of misinformation related to the current situation. Considering this, it has become more important than ever to ensure that the source of the information is verified, credible and corroborated before any action is undertaken in relation to the news.

Figure 4. The monthly count for Covid-19 related email threats - first half of 2020



Source: https://www.trendmicro.com/en_us/research/20/i/1h-2020-cyber-security-defined-by-covid-19-pandemic.html

Email was the most used entry point, making up 91.5% of detections for Covid-19-related threats. The numbers started rising in March and peaked in April. Some of the emails we observed include those that pose as health advisories or donation requests. These usually have attachments that carry malware.

Taking advantage of the increased demand for medical supplies and information on COVID-19, there has been a significant increase of cybercriminals registering domain names that contain related keywords, such as “coronavirus” or “COVID”. These fraudulent websites underpin a wide variety of malicious activities including C2 servers, malware deployment and phishing. Taking advantage of the increased demand for medical supplies and information on

COVID-19, there has been a significant increase of cybercriminals registering domain names containing keywords, such as “coronavirus” or “COVID”. These fraudulent websites underpin a wide variety of malicious activities including C2 servers, malware deployment and phishing. From February to March 2020, a 569% growth in malicious registrations, including malware and phishing and a 788% growth in high-risk registrations were detected and reported to INTERPOL by a private sector partner.

We can conclude that the most vulnerable parts of the application are those where the application accepts input from the user and this is where the most attention should be paid. When a vulnerability is detected, appropriate updates for the application are found relatively quickly. Attacks using client-side vulnerabilities are the ones most used and developed in the last few years. Attacks on databases (SQL Injection) are slowly disappearing, as very strong protections are being made that are impossible to circumvent. By using the PDO prepare PHP command, the application is enabled to pre-implement the structure of the SQL query before accepting the user input parameters, so that later the attacker will not be allowed to modify and abuse the query.

The impact of the COVID-19 on life on our Planet is fearful. Social relations (quarantine measures, physical distancing) and economic decline, collapse of trade, financial and commodity channels, elimination of a huge number of jobs have a strong impact on social and societal movements (Lukinović, Jovanović, 2020). The economic impact of the pandemic is evident in many sectors, from service industries (transport, tourism, hospitality, education), to manufacturing (cars, textiles, construction, consumer electronics). Pandemic measures will result in a serious decline of GDP in 2020 (Radić et al., 2020)

The global pandemic COVID-19 has proved the importance of a global response in collaborative and coordinated manner (Radanov, 2020). It is especially important to establish international cooperation in the field of pharmacy and synthesis of new drugs and vaccines. COVID-19 treatment protocols are now being supplemented with new experimental and generic drugs from different countries. Avifavir and coronavir are successfully used in the Russian Federation. Good results in the treatment of COVID-19 disease are given by antibodies from the blood plasma of donors who have suffered from COVID-19 in severe form. However, the greatest hopes of the population in all countries of the world are placed on antiviral vaccines against COVID-19 disease. Vaccination with Russian and Chinese vaccines take place in South American and Asian countries (Jovanović, Ermakov, 2020).

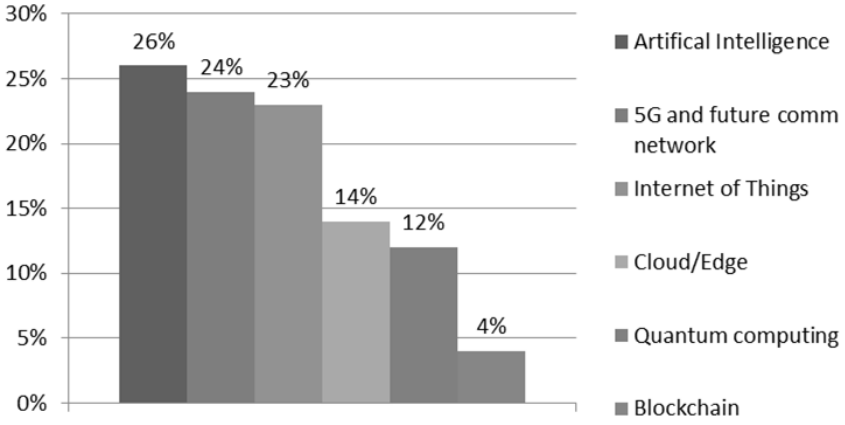
Digitalization of all branches of the economy, financial and cultural-educational sector, as well as administrative jobs in cities and suburbs, in addition to many positive aspects, opens opportunities for numerous cyber intrusions and cyber-attacks (Milošević et al., 2020, Munitlak Ivanović, 2020).

It is very important to ensure the safety of the traffic and the infrastructure of communal services in large smart cities (Kotur, Radović, 2020, Latinović, Jovanović, 2019).

Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation around the world. At the same time, the higher dependency on connectivity and digital infrastructure due to the global lockdown increases the opportunities for cyber intrusions and cyber-attacks.

The most urgent priority to address these growing cyberthreats is to further enhance international police cooperation for operational activities and to improve cybercrime information exchange with diverse partners within the global ecosystem of cybersecurity (Zlatković, Denić, 2020).

Figure 5. Key technological areas with drastic impact on the future



Source: https://www.ecs-org.eu/documents/uploads/report-on-the-ecso-members-and-the-community-survey.pdf

The European Commission's Next Generation EU proposal is a step in the right direction as it looks to harness the full potential of the EU budget and allocate €8.2 billion toward the Digital Europe Programme (DEP), involving investments in supercomputing, artificial intelligence and cybersecurity. This includes:

- Investing in more and better connectivity, especially in the rapid deployment of 5G networks.
- A stronger industrial and technological presence in strategic sectors, including artificial intelligence, cybersecurity, supercomputing and cloud.
- Building a real data economy as a motor for innovation and job creation.
- Increased cyber resilience.

5. CONCLUSION

The impact of the pandemic on humanity is incredible, modern history remembers such changes only during the great wars. Whether these changes will be permanent or temporary, time has yet to show. When we look at intellectual property, similar changes have already taken place in the field of copyright under the influence of new technical changes. Invention of radio transmission, gramophone, tape recorder, CD, etc. hit hard in the field of the copyright industry. The postulates established more than a hundred years ago were shaken, but with the necessary changes in management and law, it continued. Other intellectual property rights, primarily patents, are now facing such a challenge. It is difficult to predict how things will go on, the length of the pandemic will depend on how much and what the consequences will be. The answer to the solution to the pandemic lies in innovations, new drugs, new vaccines and the depth of the changes will depend on the speed of the inventors.

REFERENCES

Bogdanović, D., Autorsko pravo i biblioteke digitalnog doba, Bosniaca: časopis Nacionalne i univerzitetske biblioteke Bosne i Hercegovine, Vol. 22 No. 22, 2017, pp. 77- 83.

Chatterley, A., The New Normal? What The Coronavirus Means For Digital Piracy, Forbes, available at: https://www.forbes.com/sites/andychatterley/2020/04/23/the-new-normal-what-the-coronavirus-means-for-digital-piracy/#665e1c1443bc

Jovanović, L., Ermakov, V., Značaj selena i cinka u prevenciji i lečenju virusnih oboljenja, Ecologica, Vol. 27, No 99 (2020), 357-365.

Kotur, M., Radović, V., Važnost autonomnih automobila i održivog transporta u razvoju „pametnog grada“, Ecologica, Vol. 27, No 98 (2020), 273-280.

Latinović, L., Jovanović, Đ., Application of the "Smart City concept" through efficient recyclable waste collection, Ecologica, Vol. 26, No 95 (2019), 364-370.

Lukinović, M., Intelektualna svojina, Pravni fakultet Univerziteta Union/Službeni glasnik, 2017, pp. 36.

Lukinović, M., Plagiranje, naučni rad i autorsko delo, Zbornik radova Pravnog fakulteta u Nišu, LVI/2017, Issue No: 77, str. 121-132.

Lukinović, M., Jovanović, L., Uticaj pandemije COVID-19 na životnu sredinu, Ecologica, Vol. 27, No 99 (2020), 376-382.

Lukinović, M. Stamatović, M. Šarkić, N., Inovacije: pravno-ekonomski aspekti, Pravni fakultet Univerziteta Union/ Službeni glasnik, Beograd, 2017, pp. 45.

Milošević, M., Milošević, D., Stanojević, A., Simjanović, D., IAHP kao podrška primeni tehnoloških inovacija u razvoju pametnih gradova, Ecologica, Vol. 27, No 99 (2020), 407-413.

Munitlak Ivanović, O., Razvoj pametnih gradova - primer četvrte industrijske revolucije, Ecologica, Vol. 27, No 97 (2020), 15-21.

Radić, V., Radić, N., Ravić, N., Uticaj pandemije korona virusa na ciljeve održivog razvoja i ekonomiju, Ecologica, Vol. 27, No 99 (2020), 366-375.

Radanov, P., Informisanost stanovnika grada Pančeva o korona virusu – izazivaču teškog akutnog respiratornog sindroma i merama zdravstvene zaštite, Ecologica, Vol. 27, No 98 (2020), 288-299.

Ryan, B. Coppola, D. Canyon, D. Brickhouse, M. Swienton, R., COVID-19 Community Stabilization and Sustainability Framework: An Integration of the Maslow Hierarchy of Needs and Social Determinants of Health, Disaster Medicine and Public Health Preparedness, 2020, pp. 1-16.

Spasić, V., Autorska dela u digitalnom okruženju, Pravni fakultet u Nišu, Univerzitet u Nišu, 2011, pp. 51.

Zlatković, D., Denić, N., Smart cities: from urban development to digital infrastructure and cybersecurity, Ecologica, Vol. 27, No 99 (2020), 443-450.

https://landing.edgescan.com/hubfs/BCC030%20Vulnerability%20Stats%20Report%20(2020)_WEB.pdf

https://www.academia.edu/35796648/Upravljanje_bezbednoscu_u_Cyber_prostoru_i_mehanizmi_zastite_web_aplikacija

https://www.ecs-org.eu/documents/uploads/report-on-the-ecso-members-and-the-community-survey.pdf

https://www.trendmicro.com/en_us/research/20/i/1h-2020-cyber-security-defined-by-covid-19-pandemic.html

https://www.unodc.org/documents/middleeastandnorthafrica/2020/COVID19/COVID19_MENA_Cyber_Report_EN.pdf