CYBER SECURITY AND PRIVACY PROTECTION DURING CORONAVIRUS PANDEMIC

Vida M. Vilić*

Clinic of Dentistry Niš,
Assistant Director for Legal Matters,
Niš, Serbia

Abstract:
The coronavirus pandemic has brought a new reality to people around the world, who are facing uncertainty, fear of disease, sudden change of habits and lifestyles, while physical distance, social isolation, restriction of freedom of movement, mandatory self-isolation and other health measures during the epidemic instructed people to transfer their everyday habbits and professional obligations to cyberspace. The right to privacy is one of the fundamental human rights, which is recognized by the United Nations Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other international and regional treaties. This right includes privacy of personal data or information, the protection of human body, protection of personal living space and the privacy of communications. Data security aims to ensure that any personal information that is collected, used, or stored is protected from unauthorized use. In order to fight Covid-19, the laws on the state of emergency are promulgated in the countries of Central and Southeast Europe, which has led to an increasing number of arbitrary arrests, surveillance, wiretapping and violations of privacy.

Keywords:
coronavirus, cyber security, right to privacy, personal information, privacy protection.

INTRODUCTION

As COVID-19 continued to spread, one of the necessary health measures for combat coronavirus pandemic was to reduce or even completely ban social contacts, in order to make people stay in their homes and to isolate them from other people. The coronavirus pandemic has brought a new reality to people around the world. People are suddenly facing uncertainty, fear of disease, sudden change of habits and lifestyles, which are stressful. [1] This led to the fact that the companies had to allow employees to work from their home, although this resulted in an inadequate level of cyber security, security loopholes, and a mass of deviant behaviours which made businesses vulnerable. Employees using home network and public internet services to access their official resources added a new set of security challenges, since privacy issue remain ignored in the wake of COVID-19.

Correspondence:
Vida M. Vilić

e-mail:
vila979@gmail.com

DOI: 10.15308/Sinteza-2021-158-164

The right to privacy is one of the fundamental human rights, promulgated by the United Nations Declaration of Human Rights, the International Covenant on Civil and Political Rights and other international and regional treaties. This right includes privacy of personal data or information (such as people's medical records), the protection of human body (like for drug or other kind of testing), protection of personal home and the privacy of communications (via electronic mail or telephones).

Data security "aims to ensure that any personal information that is collected, used, or stored is protected from unauthorized use." [2] In this paper, we will present some of the most common problems that occurred worldwide as a result of cyber security breaches during the Covid-19 pandemic.

2. ABUSE OF MEDICAL DATA OF INFECTED PERSONS AND THEIR CONTACTS

Healthcare institutions around the world have introduced the practice of sharing medical information in order to coordinate the health strategic response to prevent the spreading and improve the control of coronavirus. These procedures must be in full compliance with national laws which are protecting the privacy of patients and infected persons, as well as protection of their right to the confidentiality of personal medical data and health status.

The World Health Organization declared COVID-19 a global pandemic on March 11, 2020. Governments have taken immediate measures to prevent the spreading of the virus and to protect the population. As countries around the world declared the state of emergency due to the pandemic, emergency rules of conduct transferred the responsibility on the citizens as individuals, since the government has imposed restrictions that often endanger some of their human rights.

The governments of Montenegro and Moldova exposed the medical data of people infected with the COVID-19 virus, while Croatia and Romania suffered from cyber-attack carried out on official websites and hospital computer systems. [3]

With a population of 640,000 inhabitants, the Government of Montenegro has taken drastic measures. Namely, the Government published a list of citizens who, according to the authorities, should have been isolated, since some did not respect the movement restriction order given to them. The government announced that they have received approval for this from the Agency for Personal Data Protection of Montenegro. After the Government of Montenegro published a list of all citizens in self-isolation, unknown authors created a web application that can locate all persons in self-isolation, as well as their possible movement. [4] From the human rights violations point of view, there are two reasons why this application is dangerous and humiliating: people who are in self-isolation are being practically hunted and stigmatized, but there is also a problem related to providing data and geo-location to unauthorized persons who want to see who is, in their close environment, in self-isolation. It remained unknown who is the owner of this application.

The right to data protection of the patient's health condition was also violated in Moldova, when the President himself on March 9, 2020 publicly named the first woman patient infected with Covid-19, who was in the hospital in Chișinău. This action clearly violated the Moldova law. [5]

Human Rights Watch (HRW) published on March 19, 2020 the document points out that "health data are particularly sensitive and that publishing data online can pose a significant risk, especially for people who are already in a specific situation or on the margins of society." [6] Moreover, "the scale and severity of the COVID-19 pandemic clearly rises to the level of a public health threat that could justify restrictions on certain rights, such as those that result from the imposition of quarantine or isolation limiting freedom of movement" [7] but "at the same time, careful attention to human rights such as non-discrimination and human rights principles such as transparency and respect for human dignity can foster an effective response amidst the turmoil and disruption that inevitably results in times of crisis and limit the harms that can come from the imposition of overly broad measures that do not meet the above criteria." HRW stated in this document that "even during previous health crises in the world, people with infection or disease and their families often faced discrimination and stigma, as was the case, for example, with HIV infection. Since the coronavirus outbreak, news reports from a number of countries have documented bias, racism, xenophobia, and discrimination against people of Asian descent." [8] This kind of data clearly incites discrimination and stigmatization and has been targeted by internet attackers.

Romanian antivirus company Bitdefender [9] has issued a statement that during March 2020, the number of web attacks associated with the Covid-19 increased by 475% compared to the February 2020, and that this

number is expected to continue to grow. It is worrying that almost one third of all attacks related to Covid-19 are targeted government authorities, retail, hospitals and health system institutions, transportation and field of education and research. [10]

3. ILEGALL CONTROL OF INDIVIDUALS' RIGHT TO FREEDOM OF MOVEMENT

State governments use a variety of technology to identify, monitor and to control the spread of the virus.

China and Iran were the first countries that started to use mass surveillance during the crisis, followed by Israel and other countries around the world.

China was the first country that introduced facial recognition and infrared temperature cameras in public transportation infrastructure, in order to immediately identify individuals who have a fever and who are, thus, potential carriers of the infection. [11] At the beginning of the pandemic, South Korea started using the "Corona 100m (Co100)" application, which would signal to mobile phone owners whether there are any people infected with coronavirus within 100 meters, giving everyone information not only about the location of an anonymous person, but also reveal the information about the date of infection of that person, their nationality, sex, age and locations that person visited. [12]

In Italy, immediately after the outbreak of the pandemic, the government began to develop an application that would identify people who were in contact with an infected person, and a similar program began to develop in both Australia and India. [13]

Israeli authorities have authorized domestic country's security agency to monitor mobile devices in order to track people infected with the coronavirus, but also to identify those they have encountered and seeing. [14] The Shin Bet's surveillance technology software has been tracking people and their contacts since March 2020 and through Jan. 20, 2021. This program was used to identify anyone with whom people infected with Covid-19 came into contact, in order to stop the spreading of the virus. At the beginning of March 2021, the Supreme Court of Israel banned this type of monitoring, stating that this is an example of a serious violation of people's civil rights and freedoms. [15]

The Constitution of the Republic of Serbia [16] guarantees the right to protection of personal data as a basic human right even during a state of emergency, while Article 128 of the Law on Electronic Communications [17] stipulates that access to mobile data (including geolocation) is allowed only by court decision.

4. PROTECTION OF EDUCATIONAL INSTITUTIONS AND STUDENTS FROM COVID-19 INTERNET FRAUD

As teaching in education institutions around the world has mostly been shifted to online classes, this pandemic crisis has provided hackers endless opportunities to see all the vulnerabilities of school's online systems, who are obligated helping their staff, students and their parents to avoid phishing attacks by providing them clear guidance how to communicate online: to clearly define all official and legal methods of communication and to be clear about other sources from which teaching materials are downloading and on which these materials are uploading; to explain to the users that IT staff will never ask for their login credentials via email; to provide and implement two-factor or multi-factor authentication whenever possible; to check out whether the email messages have been sent from authorized persons or institutions from secure servers, preventing spam and identifying false of phishing messages; to warn the students that they should not provide a credit card number for accessing the school resources; to avoid sending links via emails; to introduce to the staff and students an email address for forwarding suspected phishing attacks emails. [18]

5. PROTECTION OF EMPLOYERS AND EMPLOYEES WHO WORK FROM HOME

Covid-19 has disrupted working and professional lives in ways that seemed quite unimaginable a few years back. Mass working-from-home patterns have called into question the cybersecurity and technological solutions made in order to control the virus could seriously threaten our human right to privacy if the data involved is not handled responsibly.

Companies around the world have been forced to disrupt traditional workflows and to enable their employees to work from home. Many companies have taken data security risks they may never have agreed to in normal circumstances, which has largely jeopardized the already relative security of computer systems and the functioning mechanisms of large enterprises. Unlike employers, cybercriminals have adapted their own tactics to better exploit these new working patterns.

State authorities and health care institutions have a large amount of data at the moment while trying to develop technological solutions for bringing the virus

under control, such as different contact tracing applications. Every symptom update and restaurant check-in provides more and more information about the health and whereabouts of entire populations. [19]

6. FAKE NEWS WEBSITES AND SPREADING PANIC

Social networks and tabloid magazines have become flooded with fake news and propaganda spreading misinformation. Turkey, Serbia, Hungary and Montenegro imposed large fines, but also arrested citizens for posting on social networks because, according to the authorities, they caused panic and endangered security. [20]

The unit for cybercrime security of the Hungarian police has arrested several people for spreading false news since the beginning of February 2020, when the raid was at first been carried out. The sites that wrote about the coronavirus were closed by the police when they started writing about the presence of the coronavirus in Hungary before the official confirmation, [21] and after that, the police started to monitor the Hungarian online media due to false news related to the coronavirus. After these media reported about the state of the health system in Hungary, a package of pandemic-related laws passed by the Hungarian Parliament on March 30 gave the government power "to rule by decree indefinitely, bypassing normal parliamentary procedures: the act allows prison terms of one to five years for those who "spread falsehoods or distorted facts" that could alarm the public. These measures were temporary." [22]

On March 19, 2020, the Government of the Republika Srpska decided to ban panic and riots (including presenting and transmitting false news in the media and on social networks) during an emergency situation [23]. This decision was repealed on April 14, 2020. [24]

7. HOW HACKERS USE PANIC AND FEAR TO SPREAD COMPUTER VIRUSES

As the corona virus spreads around the world, hackers are using fear and confusion to spread computer viruses in increasingly calculated ways. As the phenomenon began to gain momentum during the pandemic, the BBC began to track some of the email scams reported by cybersecurity organizations.[25]

Hundreds of different criminal actions were noticed with millions of fake emails sent.

"Phishing" campaigns and online identity theft which rely on current news situations are not new, but information security experts say that increase in attacks related to Covid-19 are increased in the past year. Cyber attackers have mainly been active in hacking on individuals and their personal data, as well as to industry, healthcare, insurance companies, hospitals and factories.

It is impossible to determine the true scale of the e-mail epidemic, but some of the most commonly observed are these:

- „**Click here for a cure**"[26] – From February 2020, internet users began to receive various emails with the text that it is possible to receive coronavirus vaccines with one click. The message was sent by a mysterious medical expert, claiming to have exclusive news concerning the vaccine against corona virus, and that these news is provided by the Chinese and British governments. A user who clicks on the link provided in the message would be redirected to a website that looks convincing and credible, but it is actually designed to steal the user's personal information and to retrieve all users' login details, such as account names and passwords. This way, the user who is trying to get informed about the medicine against coronavirus becomes a victim of identity theft, giving hackers access to all documents and other sites to which the user previously logged in using the same email and password. The best way to see where the link will actually take you is to hold the mouse cursor over the given link and a real caption of its URL will appear. If it's suspicious, just don't click on it.
- „**WHO: Covid-19 tax refund**" - Many hacker campaigns falsely present themselves as the World Health Organization (WHO), allegedly offering users useful tips on coronavirus protection. Analysts say that the users who download content do not receive any useful advice, but instead their computer becomes infected with malicious software called Agent Tesla Keylogger.[27] Once installed, this malware records everything that is typed on a computer and sends it to attackers, which is a tactic that can provide access to online banking and financial accounts. In order for users to avoid this scam, it is necessary to avoid emails like this one from the WHO, because they are probably fake, but instead to visit the official website or WHO channels on social networks to get the latest advice.

- „ **We refunded your tax to help protect you from Kovid-19" / Little measure that saves**"[28] –This type of attack happened in the UK, as hackers devised an email sent on behalf of the UK tax authorities with a false promise that citizens who go to the site given in a sent message, entering personal data and their bank account details, will be able to recover taxes due to Kovid-19. This is one of the variations of the classic "phishing" campaign regarding tax refunds used by cybercriminals. The most effective fight against this type of fraud is not to respond to any request sent via e-mail concerning financial transactions, and especially not to enter data on users' bank accounts.
- „**CDC: Donate here to help the fight**"[29]– Represents another fake email allegedly collecting donations to work on the development of a coronavirus vaccine, exclusively in bitcoins. Like the WHO, the Centres for Disease Control and Prevention (CDC) has been used to misrepresent numerous different "phishing" campaigns. The e-mail address itself looks very convincing, just like the design of the e-mail. This example was reported to malware experts Kaspersky. Kaspersky says it has detected more 513 different files with coronavirus in their title, which contain malware.
- **Online Shopping Fraud** [30] – The media has reported that there are new specific scams related to online shopping, "selling" people protective face masks, hand sanitizers and other essential items from questionable and malicious sites, which have never been delivered to the buyers. The advice is to always check whether the online store you are making the purchase from is legitimate.
- **Malicious Newsletters** [31] – Cyber criminals are providing numerous articles about COVID-19 with a link to malitious and fraudolent company website, where victims are encouraged to click on a malicious link to subscribe to their daily newsletter for further updates on COVID-19.

8. CONCLUSION AND RECOMMENDATIONS FOR MAINTAINING CYBERSECURITY DURING THE PANDEMIC

As the whole world struggles globally both to stop the spreading of COVID-19 infection and raising panic for one's own health and the health of others, cyber attackers and hackers are profiting from people's fears and panic. However, it is obvious that we are witnessing major changes in the way that the world today operates –changes have been made "that will most likely have an impact long after this situation is over and we all return to our normal lives". [32]

In just over a year of the pandemic, only some of the problems threatening the cyber security and privacy of each individual in cyberspace have crystallized.

One of the problems was the spread of panic and misinformation at the very beginning of the pandemic. It is necessary to convince citizens that the best way to handle fake news is by warn the users to use only reliable sources of information, not just social media posts and suspicious emails.

Cyberspace has become flooded with fraudulent products. Internet users should purchase only from reliable sellers and companies, only when they are totally sure that the website is legitimate. [33]

At the time of the pandemic, hackers were frequent with phishing attacks, and the number has the tendency in rising even after the pandemic ends. In order to protect users from such attacks, it is necessary that Internet users pay attention when opening emails and to review emails carefully with grammar and spell checking or any other suspicious language signs, as well as to beware when opening links or attachments from unknown sender. Malware, often used in the process of cyber phishing attacks, can be handled with cyber defence tools, such as various antivirus programs.

Special anti-malware measures for preventing data theft must be applied when it comes to working from home, which has become a reality everywhere in the world due to the coronavirus pandemic. If employees use computers and digital technology while working from home, employers should inform workers of all possible hazards, as well as take data security measures into account. Employees need to be provided with data security protection when working from home involves sending confidential data outside the company's premises. The employer will have to make sure that the systems enables secure transmission of such data, by establishing a solid information system with the necessary security measures, but also to advise employees that it is essential to be equipped with appropriate skills which make the employee aware of all potential problems. Employees should be provided with training in order to refresh their knowledge.

In addition to data and internet security, it is necessary to take into account the physical health of workers who work from home during a pandemic. Employees needs to be offered a variety of tasks in order to change body

position frequently so as not to work in the same body position for a long time. The work equipment must be set up to minimize body twisting or excessive stretching, and workers must be encouraged to take regular breaks, and from time to time to have an opportunity to stand up.

Employers who have enabled employees to work from home must pay attention in securing the data, through encryption of channel connecting remote machines to, monitoring of internet traffic and connections as well as to secure protocols to accessing professional assets and data. This is especially important for organizations, which have higher risk profile and have appetite for investing more in security, to adopt the following practices of data classification, data leak prevention, monitoring the user behaviour and even email encryption. The professionals should only store necessary information, to share credentials only with relevant parties, and even implement two-factor authentication. [34]

In addition to all the dangers lurking on the Internet due to cybersecurity violations, it is very important to ensure the privacy of teachers and students in the process of online learning and during organizing online classes. There are several important recommendations that should be adopted when conducting online classes, especially during video-enabled teleconferencing, such as: recommending when and whether to turn on the webcam, to remind teachers not to share teaching materials over an insecure network, to avoid sending emails to parents because this spreads the circle of communication and thus creates possible dangers to cybersecurity, etc. [35]

REFERENCES

[1] V.Vilić, "Isolation during covid-19 pandemic: a trigger for domestic violence", Yearbook no.3 HUMAN Rights Protection: the right to human dignity/ Editor:Zoran Pavlović – Novi Sad: Provincial Protector of Citizens- Ombudsman; Belgrade: Institute of Criminological and Sociological Research, 2020 (Novi Sad: Vojvodina Provincial Authorities Common Affairs Department). 739 str. str. 695-714

[2] RBC Corporate Governance and Responsible Investment Team - Data privacy and security in the time of COVID-19, May 11, 2020, https://www.rbcgam.com/en/ca/article/data-privacy-and-security-in-the-time-of-covid-19/detail, retrieved on 03.05.2021.

[3] M.Ristić, M. Stojanović, M. German Sirotnikova, A. Keller-Alant, H. Firat Buyuk, A.Vladisavljević, M. Gascón Barberá & M. Necsutu, „Pravo na informaciju i privatnost: Drugačije žrtve koronavirusa", BIRN, published 24.03.2020., https://balkaninsight.com/2020/03/24/pravo-na-informaciju-i-privatnost-drugacije-zrtve-koronavirusa/?lang=sr, retrieved on 03.05.2021.

[4] S. Janković & A. Durović, "Aplikacija za 'lov na izolovane' i dalje aktivna", published 27.03.2020., https://www.slobodnaevropa.org/a/aplikacija-za-lov-na-izolovane-ali-i-dalje-aktivne/30513232.html, retrieved on 02.05.2021.

[5] Garda World, Moldova: First case of COVID-19 confirmed March 8, published 08.03.2020., https://www.garda.com/crisis24/news-alerts/320631/moldova-first-case-of-covid-19-confirmed-march-8, retrieved on 05.05.2021.

[6] Human Rights Dimensions of COVID-19 Response, published on 19.03.2020., https://www.hrw.org/news/2020/03/19/human-rights-dimensions-covid-19-response, retrieved 05.05.2021.

[7] Ibid.

[8] Human Rights Dimensions of COVID-19 Response - Root out discrimination and stigma, protect patient confidentiality, published 19.03.2020., https://www.hrw.org/news/2020/03/19/human-rights-dimensions-covid-19-response#_Toc35446585, retrieved on 05.05.2021.

[9] Bitdefender - Tough on threats, light on your system, https://www.bitdefender.com, retrieved on 04.05.2021.

[10] Anti-malware Research: 5 Times More Coronavirus-themed Malware Reports during March, published on 20.03.2020, https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/, retrieved on 06.05.2021.

[11] J.Guzman, "Changing America: China rolls out facial recognition thermometers on buses amid coronavirus outbreak", published on 19.02.2020., https://thehill.com/changing-america/well-being/prevention-cures/483669-china-rolls-out-facial-recognition-thermometers, retrieved on 05.05.2021.

[12] S. Wray, "South Korea to step-up online coronavirus tracking", published on 15.03.2020., https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109, retrieved on 07.05.2021.

[13] Coronavirus tracking apps: How are countries monitoring infections?, https://www.dw.com/en/coronavirus-tracking-apps-how-are-countries-monitoring-infections/a-53254234, retrieved on 06.05.2021.

[14] Reuters: Israel approves cellphone tracking of COVID-19 carriers for rest of year, published on 20.07.2020., https://www.reuters.com/article/us-health-coronavirus-israel-surveillanc-idUSKCN24L2PJ, retrieved on 08.05.2021.

[15] Reuters: Israeli Supreme Court bans unlimited COVID-19 mobile phone tracking, published on 01.03.2021., https://www.reuters.com/article/health-coronavirus-israel-surveillance/israeli-supreme-court-bans-unlimited-covid-19-mobile-phone-tracking-idINKCN2AT25R, retrieved on 08.05.2021.

[16] Ustav Republike Srbije, Sl. glasnik RS br. 98/2006

[17] Zakon o elektronskim komunikacijama, Sl. glasnik RS br. 44/2010, 60/2013 - odluka US, 62/2014 i 95/2018 - dr. zakon

[18] Cybersecurity Considerations in a COVID-19 World, https://www.cosn.org/sites/default/files/COVID-19%20%26%20Cybersecurity%20-%20Member%20Exclusive.pdf, retrieved on 10.05.2021.

[19] The COVID-19 effect: Cybersecurity and data privacy, published on November 2020, https://www.bmogam.com/ca-en/investors/news-and-insights/the-covid-19-effect-cybersecurity-and-data-privacy/, retrieved on 07.05.2021.

[20] M.Ristić, M. Stojanović, M. German Sirotnikova, A. Keller-Alant, H. Firat Buyuk, A.Vladisavljević, M. Gascón Barberá & M. Necsutu, „Pravo na informaciju i privatnost: Drugačije žrtve koronavirusa“, BIRN, published 24.03.2020., https://balkaninsight.com/2020/03/24/pravo-na-informaciju-i-privatnost-drugacije-zrtve-koronavirusa/?lang=sr, retrieved on 03.05.2021.

[21] International Press Institute: Hungary seeks power to jail journalists for 'false' COVID-19 coverage, published on 23.03.2020., https://ipi.media/hungary-seeks-power-to-jail-journalists-for-false-covid-19-coverage/, retrieved on 08.05.2021.

[22] J.Spike, "Press Freedom: COVID Pandemic Adds to Pressure on Hungarian Media", published on 01.06.2020., https://www.voanews.com/press-freedom/covid-pandemic-adds-pressure-hungarian-media, retrieved on 05.05.2021.

[23] Odluka o zabrani izazivanja panike i nereda za vrijeme vanredne situacije na teritoriji Republike Srpske, Sl.Glasnik RS br. 26/2020

[24] Dnevni list DANAS od 14. aprila 2020., https://www.danas.rs/svet/vlada-rs-stavila-van-snage-uredbu-o-izazivanju-panike/, retrieved on 05.05.2021.

[25] J. Tidy, "Coronavirus: How hackers are preying on fears of Covid-19", published on 13.03.2020., https://www.bbc.com/news/technology-51838468, retrieved on 06.05.2021.

[26] The whole world knows where you're working right now - Don't leave your home office open to cyber criminals, https://www.policedsc.com/images/PDSC_TOP_TIPS_WORKING_FROM_HOMEv2.pdf, p.2, retrieved on 04.05.2021.

[27] Malpedia, https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla, retrieved on 08.05.2021.

[28] The whole world knows where you're working right now - Don't leave your home office open to cyber criminals, https://www.policedsc.com/images/PDSC_TOP_TIPS_WORKING_FROM_HOMEv2.pdf, p.2, retrieved on 04.05.2021.

[29] The whole world knows where you're working right now - Don't leave your home office open to cyber criminals, https://www.policedsc.com/images/PDSC_TOP_TIPS_WORKING_FROM_HOMEv2.pdf, p.2, retrieved on 04.05.2021.

[30] The whole world knows where you're working right now - Don't leave your home office open to cyber criminals, https://www.policedsc.com/images/PDSC_TOP_TIPS_WORKING_FROM_HOMEv2.pdf, p.2, retrieved on 04.05.2021.

[31] The whole world knows where you're working right now - Don't leave your home office open to cyber criminals, https://www.policedsc.com/images/PDSC_TOP_TIPS_WORKING_FROM_HOMEv2.pdf, p.2, retrieved on 04.05.2021.

[32] Coronavirus: Will our day-to-day ever be the same?, https://www.bbc.com/worklife/article/20201109-coronavirus-how-cities-travel-and-family-life-will-change, retrieved on 08.05.2021.

[33] FraudWatch International: COVID-19 has long term effects on cyber security, published on 27.03.2020., https://fraudwatchinternational.com/active-scams/covid-19-has-long-term-effects-on-cyber-security/, retrieved on 06.05.2021.

[34] P.Boyden, "Post COVID-19 Privacy Regulations – how will it affect us?", published on 29.05.2020., https://fraudwatchinternational.com/all/ipost-covid-19-privacy-regulations-how-will-it-affect-us/, retrieved on 08.05.2021.

[35] Cybersecurity Considerations in a COVID-19 World, https://www.cosn.org/sites/default/files/COVID-19%20%26%20Cybersecurity%20-%20Member%20Exclusive.pdf, retrieved on 10.05.2021.