



MONITORING OF DIGITAL RIGHTS VIOLATIONS

Analytical report

April 2020

I. General violations of digital rights (*violations affecting an unlimited number of individuals*).

1. Access to the Internet and online information.

- 1) As of April 2020, 240 websites remained blocked pursuant to two Decrees of the President of Ukraine of May 15, 2017¹ and May 14, 2018². This fact has been repeatedly highlighted in analytical reports following the Monitoring of Digital Rights Violations in Ukraine in 2019³.

The Coalition “For the Free Internet” prepared and published a legal analysis of the Decree of the President of Ukraine of 2018. Its conclusions are largely relevant to the first Decree as well⁴.

Key considerations are as follows:

- the sanction, as a way of restricting human rights and freedoms does not meet the constitutional standards and requirements and reflects an unrestricted discretion of the government;
- the sectoral nature of the sanction requires a positive vote in the Verkhovna Rada of Ukraine for a sanction to be enforced;
- the mechanism in the part of websites blocking does not comply with the national law and violates the fundamental constitutional rights of citizens;
- the practice of blocking hundreds of websites in the manner applied by the government does not meet the criterion "prescribed by law" in the light of international treaties and the European Court of Human Rights case law;
- such blocking does not meet the criterion of the "necessity in a democratic society" and is disproportionate to the defined legitimate aim.

It is a continuing violation and no improvements have been noted as of April 2020. On the contrary, the governmental authorities make repetitive statements about the need to extend the blocking of those web resources⁵.

¹ <https://www.president.gov.ua/documents/1332017-21850>

² <https://www.president.gov.ua/documents/1262018-24150>

³ <https://www.ppl.org.ua/monitoring/monitoring-cifrovix-prav>

⁴ <https://www.ppl.org.ua/yuridichnij-analiz-ukazu-prezidenta-pro-blokuvannya-sajtiv.html>

⁵ <https://www.rnbo.gov.ua/ua/Diialnist/4597.html>

- 2) Prohibition by the headmaster of the “Budokan” secondary school of oriental languages and martial arts to include the content from the distance learning program, broadcasted by 112, Zik and NewsOne channels (over the Internet as well) as a part of teachers' preparations for their own webcasted lessons, thematic presentations and on-line classes (he also did not recommend parents and pupils to watch the content of those channels for the distance learning purposes)⁶. Given that the Ministry of Education and Science of Ukraine listed these channels among the sources to be used during the All-Ukrainian online school⁷, specifically for teaching children of the 5-7th grades – this prohibition constituted the violation of digital rights, including the right to access information (restriction of access to information sources) and the right to education.

In sum, during the reporting period **3 violations of digital rights were spotted** in the form of restrictions on access to the Internet and information published online, covering 243 web resources.

2. Processing of personal data for a different purpose to that for which the persons have consented.

1) Map of compliance with the self-isolation regime from Kyivstar.

Kyivstar has mapped the self-isolation index, calculated by the company as a percentage of the population, which restrained oneself from moving around during the period of self-isolation⁸. This indicates that personal information is not processed for the purpose for which the customers consented.

2) Publication of a map spotting the indicative area of residence of patients with COVID-19, by the Zhytomyr Oblast State Administration⁹.

The creation of such a map would be impossible without processing the relevant personal data of patients with coronavirus disease (both about their health and their place of residence). Processing of such information for the purpose of its public dissemination without a person's consent is prohibited, it also does not pursue a legitimate aim.

Moreover, making public this type of information creates preconditions for social tension, suspicion, harassment of residents of a certain residential area, the spread of hate speech, and might incite violations of individual human rights.

3) Publication of a map spotting the indicative area of residence of patients with COVID-19, by the Dnipro City Council¹⁰.

This violation is similar to the above mentioned.

All in all, **3 (three) facts** of processing personal data for a different purpose to that for which the persons consented were recorded in the reporting period.

3. Internet and dissemination of rumors.

In March 2020, due to the announcement of a coronavirus pandemic the quarantine was introduced on the territory of Ukraine¹¹. In this context, many different kinds of messages,

⁶<https://www.facebook.com/BudokanLviv/photos/a.152703171801001/772921236445855/?type=1&theater>

⁷<https://mon.gov.ua/ua/news/o-1000-startuye-vseukrayinska-shkola-onlajn-rozklad-i-temi-urokiv-na-tizhden-posilannya-na-youtube-mon-de-translyuvatimutsya-uroki-dlya-vsih-klasiv>

⁸<https://kyivstar.ua/uk/covid2019-stat>

⁹<https://ms.detector.media/zakonodavstvo/post/24517/2020-04-16-chumni-kvartali-zhitomirska-oda-oprilyudnila-kartu-z-poznachkami-vulits-de-meshkayut-khvori-na-covid-19/>

¹⁰<https://ms.detector.media/zakonodavstvo/post/24566/2020-04-25-meriya-dnipra-opublikovala-na-saiti-kartu-z-poznachkami-de-viyavleno-zakhvorilikh-na-koronavirus/>

¹¹<https://www.kmu.gov.ua/npas/pro-zapobigannya-poshim110320rennyu-na-teritoriyi-ukrayini-koronavirusu-covid-19>

including false ones, were spread in social networks, in particular on Facebook. With a view to counteract fakes, the law enforcement agencies began to actively draw up protocols on administrative offenses under the Article 173-1 of the Code of Administrative Offenses (spreading false rumors), which led to the emergence of a new and, in some cases, ambiguous punishment practice for spreading rumors on the Internet.

For instance, according to the Security Service of Ukraine, 241 persons who had disseminated false information about the coronavirus got detected as of April 28, 2020¹². At the same time, in April 2020, 32 rulings in cases under the Article 173-1 of the Code of Administrative Offenses were found in the Unified State Register of Judgments. Out of these, the court made the following decisions:

- held that there had been an administrative offense and applied a fine of 170 hryvnias, charging a court fee of 420 hryvnias, 40 kopecks, – **in 9 cases**;
- ruled on the administrative offense and on the release of a person from liability due to the insignificance of the committed act, making a verbal warning only – **in 5 cases**;
- decided on the absence of the event and/or the legal elements of the administrative offense, in particular its objective side, and dismissed the proceedings **in 12 cases**;
- found it necessary to return the case file to the National Police for bringing the protocol on administrative offenses in line with the requirements of the Code of Administrative Offenses – **in 6 cases**.

Violations of digital rights have been detected in the first two cases due to:

- 1) incomplete establishment of the facts: often the courts do not establish the full text of the message, which led to the drawing up an administrative protocol. As a result, it is impossible to see from the court decision what information the court has analyzed (and whether it has made any analysis), whether it is accurate and can lead to panic or disturbance of public order.
- 2) lack of the proper body of evidence: often there is no evidence of intent to spread panic or disturb public order.
- 3) the lack of assessment of the disputed message by the court for its credibility.
- 4) the lack of justification for the intent to spread panic in the society or to disturb public order¹³.

A total of **12 (twelve)** cases of violations of general digital rights, related to the spread of rumors on the Internet, were detected in April.

To sum up, there were a total of 18 (eighteen) general violations of digital rights, of which: 3 (three) violations of digital rights appeared in the form of restrictions on access to the Internet and online information covering 243 web resources; **3 (three) facts** of processing personal data for a different purpose to that for which the persons consented, and **12 (twelve) facts** related to the spread of rumors on the Internet.

II. Individual violations of digital rights (*infringements affecting individual right-holders and with no direct impact on wide audience*).

1. Violations of the right to freedom of expression

¹² <https://ssu.gov.ua/ua/news/1/category/21/view/7517#.Vz25EtDr.dpbs>

¹³ Overview of the related case law and a detailed report will be published tentatively in July 2020

1) Declaration of information as false and the obligation to refute it without involvement of due defendants.

The Pechersk District Court of Kyiv in its decision in absentia of February 27, 2020 satisfied the claim for protection of business reputation and refutation of false information, brought by LLC "News 24 hours" against the head of the Main Department of Information Policy of the Presidential Administration of Ukraine. While declaring that the disputed information was disseminated by the Administration of the President of Ukraine, the court did not involve it in the case as a defendant, which gives grounds to doubt whether the circumstances of this case had been established in full.

Also, the court applied two methods of legal protection at once – refutation and removal of the disputed information from the website – without justifying the need for their simultaneous application¹⁴.

2) Filing excessive claims (UAH 5 million) and seizing all the defendant's property in order to secure the claim, which has a "chilling effect" on the freedom of speech

Specifically, on April 6, 2020, the Kharkiv District Court of Kharkiv oblast ruled to secure a lawsuit in the case of refutation of false information disseminated on a user's Facebook page and compensation of non-pecuniary damage of UAH 5 million. The court has arrested and banned any registration actions in respect of immovable property and vehicles of the defendant, as well as froze the assets, prohibiting the alienation of his share in the authorized capital of companies¹⁵. The filing of a lawsuit for a tangible amount – 5 (five) million hryvnias, as well as the satisfaction of the request to secure the lawsuit by seizing all the defendant's valuable property – has a "chilling effect" on the freedom of speech.

3) Rendering decisions on refuting the value judgments and orders to apologize.

By decisions of the Truskavets City Court of the Lviv oblast of 05.03.2020 in cases No. 457/991/18 and No. 457/1004/18, the editor-in-chief of the newspaper Dzherela Truskavtsya and the Limited Liability Company "The editorial board of the newspaper "Dzherela Truskavtsya" were ordered to publish on its website the refutation message with an apology to the plaintiffs (apology, as a way of legal protection, is not prescribed by the legislation of Ukraine and is not a refutation), as well as to refute not only facts but also value judgments¹⁶.

4) Attacks on journalists and bloggers, inefficient investigation of these cases, in particular:

a) In almost 2 (two) years, the pre-trial investigation officials have not taken all necessary steps to prosecute the perpetrators of the attack on the journalist (blogger). This might reflect the failure to ensure an efficient investigation in the case, so an application to the ECtHR is being prepared¹⁷.

For instance, Mr Vsevolod Novokhatko, editor of the online media "Zakon Odyn Dlya Vsikh", was attacked on May 24, 2018. This case has not been investigated yet, several decisions have been made to close it, which have been overruled by the courts.

b) A security guard of the Illinsky Monastery of Ukrainian Orthodox Church of the Moscow Patriarchate attacked Mr Vladislav Shvets, a photojournalist with the "Ukrainian Information Service", on April 17, 2020, in Odesa. The journalist was making a coverage of

¹⁴<http://reyestr.court.gov.ua/Review/88778487>

¹⁵<http://reyestr.court.gov.ua/Review/88714542>

¹⁶ <http://reyestr.court.gov.ua/Review/88941545> and <http://reyestr.court.gov.ua/Review/88941130>

¹⁷<https://helsinki.org.ua/articles/yak-politsiia-ta-prokuratura-dnipra-ta-oblasti-vzhe-dva-roky-sabotuiut-rozsliduvannia-napadu-na-aktyvista/?fbclid=IwAR3xYO3osdCwnyofprUhfqRLtSMRNHZ6XkbqMnUHR70L2qguJk4KnGzm0mU>

the Easter preparations. In his turn, the investigator of the National Police accepted the appeal on obstruction of professional journalistic activity¹⁸.

c) During a live streaming in front of the Cabinet of Ministers of Ukraine on April 29, 2020, police officers beat up and broke the equipment of Hromadske TV journalist Bohdan Kutieпов, who was covering together with his colleague Nikita Mekenzin a rally of entrepreneurs opposing the quarantine restrictions¹⁹.

All in all, **6 (six) cases** of violation of the right to freedom of expression in the digital environment were spotted in April 2020.

2. *Privacy and Data Protection:*

1) **Selling personal data.**

a) As the Secret Service of Ukraine reported, a resident of Ivano-Frankivsk was selling information from the databases²⁰ of the State Customs and Border Services of Ukraine, namely the information on border crossings of Ukrainian citizens and foreigners, of vehicles, and the period of their stay abroad. A criminal proceedings was opened on the grounds of a crime under part 2 of the Art. 361-2 of the Criminal Code of Ukraine – an unauthorized selling or sharing of the classified information, materials were submitted to the court²¹.

b) In Telegram some bots selling personal data of customers, allegedly to Privatbank, have been detected. The bank appealed to the National Police in because of the bots activity²².

2) **Theft and “leakage” of personal data.**

a) The press service of the Marriott International hotel chain made a statement on the possible data theft of over five million of its customers, including their names, addresses, phone numbers, emails, birthdays, as well as information about their benefits and participation in the loyalty and partnership programs²³.

b) Publication of correspondence of Mr Volodymyr Pavlenko, Deputy Head of the Agency for Search and Management of Assets (ARMA) without his consent²⁴.

3) **Disclosing personal data through negligence**

The State Employment Service of Ukraine sent out to its applicants a password to enter their e-cabinet in a letter with open addresses²⁵. Now anyone can visit e-cabinets of those who did not change their passwords right after.

In sum, **5 (five) cases** of violation of the right to privacy and data protection took place in the digital environment during April 2020.

¹⁸https://usionline.com/2020/04/17/v-odesse-ohrannik-tserkvi-napal-na-zhurnalistku-usi-foto-video/?fbclid=IwAR3jwHnqwKdNkToGfwdc50bjaScImUPv3jL8_Y8PzRnRvz2vbBr2eIoLYJO

¹⁹<https://hromadske.ua/posts/priberi-abo-zlamayemo-policiya-napala-na-zhurnalista-hromadske>

²⁰ Since it is not clear from the Secret Service message whether it involved selling of the entire database or only some piece of information concerning particular individuals or legal entities, whether this violation is qualified as an individual violation of digital rights.

²¹<https://ssu.gov.ua/ua/news/1/category/21/view/7427#.VoItFNTe.dpbs>

²²<https://ain.ua/2020/04/27/v-telegram-zarabotali-boty-kotorye-po-nomeru-vydayut-inn/>

²³<https://ua.korrespondent.net/business/companies/4211793-velyka-merezha-hoteliv-zaiavyla-pro-vyitik-danykh-klientiv>

²⁴<http://nashigroshi.org/2020/04/24/pavlenkohey-t-zlyv-perepysok-zamholovy-arma-i-yoho-komentari-shchodo-tsoho/?fbclid=IwAR2QTTONpcM3saCEDlidFHUQH8FGn5-eXp4wdK3uZ3gbUpge7HXRccR-fCY>

²⁵<https://internetua.com/centr-zanyatosti-raskryl-licsnye-dannye-zayavitelei>

<https://ms.detector.media/kiberbezpeka/post/24595/2020-04-30-cherez-neobachnist-derzhavnii-tsentr-zainyatosti-rozkriv-osobisti-dani-zayavnikov/>

A total of 11 (eleven) individual violations of digital rights were spotted in April 2020, of which: **6 (six)** cases of violation of the right to freedom of expression and **5 (five)** violations of the right to privacy and data protection in the digital environment.

III. Potential threats to free speech and the right to privacy on the Internet in Ukraine:

- 1) **Website blocking.** On April 20, 2020, the Ministry of Reintegration of the Temporarily Occupied Territories of Ukraine shared a statement that Roskomnadzor had blocked its website upon the request of the Prosecutor General's Office of the Russian Federation.

Along with this, it is still unknown whether the website of the Ministry of Reintegration is blocked only on the territory of Russia or also on the temporarily occupied territories of Ukraine. Therefore, this case is currently included in the list of potential threats²⁶. The reason behind this blocking was "a piece of news about the covering up of COVID-19 patients in the Crimea and Donbas."²⁷

- 2) **The use of the smartphone application "Diy vdoma" ("Act at home")** for monitoring citizens' compliance with the observation and self-isolation regimes – poses a threat of violation of digital rights, as the principles of personal data processing defined by Article 6 of the Law of Ukraine "On the Personal Data Protection" are not fully respected even with the law on data processing and the resolution of the Cabinet of Ministers of April 22 in place. Specifically, there is no transparency regarding the procedure for data transmission, the volume of data is not clearly defined, namely when it comes to the "brief information on the state of health" passed to the Ministry of Internal Affairs, etc. The latter fact also does not allow to fully assess whether the requirements that the composition and content of personal data must be relevant, adequate and not excessive in relation to the specified purpose of their processing²⁸.

Moreover, users of this mobile application have repeatedly complained about the existence of technical problems associated with its operation: false recording of violations of self-isolation in the absence of such incidents, lack of sound messages, which prevents timely response and generates artificial "violations" of self-isolation, as well as inadequate technical support for the work of the application, problems with feedback, etc²⁹.

- 3) **Attacks on websites and other web resources.** There was a massive DDoS attack on electronic services of the Kyiv City State Administration. This has put significant pressure on the system and external communication channels, which in turn has created a potential threat of temporary restrictions on access to e-services or city websites³⁰.
- 4) **Spread of fake news.** In April 2020, **27 reports on multiple facts of spreading fake news** were spotted. They pertained mainly to the coronavirus issue (see, in particular, cyber police reports³¹, as well as information on the spraying of disinfectants from helicopters³²,

²⁶ It should be noted that the Government of Ukraine does not bear responsibility for this violation and, therefore, it is not included in the relevant statistics. However, this is the first case of blocking the website of the Ukrainian government by another state, and therefore it needs close attention.

²⁷ <https://mtot.gov.ua/ua/genprokuratura-rf-zablokuvala-sat-minreintegracii-ukraini>

²⁸ <https://dslua.org/publications/chy-zahrozhue-vykorystannia-diy-vdoma-tsyfrovym-pravam/>, also: <https://dslua.org/publications/ne-chas-dlia-zghody-shcho-ne-tak-iz-novym-antivirusnym-zakonom/> and <https://dslua.org/publications/kabmin-detalizuvav-umovy-zastosuvannia-diy-vdoma/?fbclid=IwAR1cELx9pTJx7P0evhjCjZwtymIKGIewqDkUBeKdc5hxf3sK-x5AgvypbDE>

²⁹ https://play.google.com/store/apps/details?id=ua.gov.dii.quarantine&fbclid=IwAR0j7g_XZ2H8tUrOebiYEI2wdvxonJDYci1GITV8BkSqqYrOKfUapuOkNo

³⁰ <https://kyivcity.gov.ua/news/na-elektronni-servisi-kmda-zdiysnyuyetsya-kiberataka/>

³¹ <https://cyberpolice.gov.ua/news/z-pochatku-karantynu-vyavleno-faktiv-rozpovsyudzheniya-fejkiv-perevireno-povidomlennya-shhodo-mozhlyvyx-shaxrajstv-u-tomu-chysli-pry-onlajn-kupivli-zasobiv-indyvidualnogo-zaxystu-5687/>

³² <http://www.reyestr.court.gov.ua/Review/88537270>

the creation of fake pages and the spread of false information about the EU and Ukraine³³ during the pandemic, etc.)³⁴.

- 5) **Processing of users' data without their consent.** According to media reports, Facebook uses a microphone for listening to its users aiming to further sell them more targeted advertising³⁵. Meanwhile, Twitter announced it would collect more information about its users to share with advertisers, and removed from its mobile app an option that allowed users to control what personal data could be sent to the company's business partners³⁶. These cases reveal the collection and processing of personal data of social network users without their consent, and thus the potential opportunities for violation of their right to privacy and protection of personal data. As far as these social networks are also used in Ukraine, there is a risk of violating the right to privacy.
- 6) **Software vulnerabilities that could violate the right to privacy:**
 - a) The media reveal a number of serious vulnerabilities found in the security system of Zoom program, leading to leakages of user data, theft of passwords from Windows user accounts, etc.³⁷
 - b) Twitter also reported some vulnerabilities for this social network users who use the Firefox browser (after closing Twitter or logging out of it, the user's personal files remained in the browser's cache and could be accessed by anyone)³⁸.
 - c) Software developers have discovered a vulnerability in the TikTok service that allows you to replace any video on a third person's page³⁹.
- 7) **Internet fraud.** Fraudsters offer to leave an application and watch some video, but instead install a malicious program on your computer or phone that allows you to steal personal data and access a person's bank account⁴⁰.
- 8) **Distortion of information about the number of views.** According to media reports, the Russia Today TV channel falsifies the number of views of its videos on YouTube and buys comments from bots under the videos. This leads to distortion of information about the website visits and can potentially violate digital rights through manipulation of information⁴¹.
- 9) **Risks posed by the neural network.** Hlab.AI company has announced that it had managed to develop a neural network allowing to identify people who do not wear protective face masks⁴². This poses a potential threat to the right to privacy and personal data protection.

³³<https://www.eurointegration.com.ua/news/2020/04/1/7108223/>

³⁴ These facts are listed as potential threats to digital rights, because on the basis of statistic data solely without a meaningful analysis of reports (including courts) it is impossible to establish the presence or absence of violations.

³⁵<https://internetua.com/v-facebook-priznali-csto-proslushivauat-polzovatelej>

³⁶<https://internetua.com/twitter-teper-peredaet-reklamodatelyam-bolshe-dannyh-o-svoih-polzovatelyah>

³⁷<https://www.buzzfeednews.com/article/pranavdixit/google-bans-zoom>, <https://mind.ua/news/20209799-google-zaboroniv-svoyim-spivrobotnikam-vikoristovuvati-zoom>, <https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/>

³⁸<https://internetua.com/twitter-sohranyal-licsnye-soobsxeniya-polzovatelei-v-keshe-brauzera>

³⁹<https://internetua.com/uyazvimost-v-tiktok-pozvolyaet-podmenyat-video-na-csujih-stranichah>

⁴⁰<https://www.obozrevatel.com/economics/fea/dostatochno-zajti-v-internet-moshenniki-v-razgar-koronavirusa-ostavlyayut-ukraintsev-bez-kopejki.htm>

⁴¹<https://ms.detector.media/manipulyatsii/post/24442/2020-04-03-kanal-rt-nakruchue-milioni-pereglyadi-v-youtube-cherez-pornosaiti-rozsliduvannya/>

<https://navalny.com/p/6325/?fbclid=IwAR3qQ2CpsGNS6JFgYoGf44tOSqgm8ExJzyFms6mVNvSUwpJS7B45zZf87E>

⁴²<http://hlab.ai/covid-mask-detection>

10) **Tracking users of social networks.** An attempt by Facebook to arrange mass surveillance of its users possessing iPhones has been revealed⁴³. For this purpose, the company tried to purchase special spyware from the Israeli company NSO Group.

Such actions potentially put the human right to privacy and personal data at risk.

11) **Use of social networks, applications, as well as certain products of Internet giants, namely by Apple and Google, for counteracting the coronavirus pandemic.**

According to mass media, Facebook will monitor the movement of users to counter the spread of COVID-19⁴⁴, whereas Apple and Google will join their efforts in developing software that might help reduce the chances for the disease spread⁴⁵. In addition, the Kyiv City State Administration announced the potential use of the Telegram application for remote monitoring of Kyiv residents' compliance with the self-isolation regime⁴⁶.

This might potentially violate the digital rights of individuals, especially when it comes to the collection, storage and use of their personal data.

12) **Sending phishing messages** that poses a threat to digital security.

Google has reportedly blocked 18 million phishing emails about coronavirus allegedly sent to its users by the World Health Organization (WHO)⁴⁷.

In sum, in April 2020, 12 (twelve) potential threats to the freedom of speech and the right to privacy on the Internet were identified in Ukraine.

Summarizing the above, it is worth noting that the monitoring of digital rights violations in Ukraine in April 2020 revealed:

• **18 (eighteen) facts of the general violation of digital rights, in particular:**

- 3 violations of digital rights in the form of restrictions on access to the Internet and online information covering 243 web resources;
- 3 facts of processing personal data of persons for a different purpose to that for which consent was given;
- 12 facts related to the spread of rumors on the Internet.

• **11 facts of individual violation of digital rights, specifically:**

- 6 cases of violation of the right to the freedom of expression in the digital environment;
- 5 cases of violation of the right to privacy and data protection in the digital environment.

Also, **12 potential threats** to the freedom of speech and the right to privacy on the Internet have been identified in Ukraine.

⁴³<https://internetua.com/facebook-pytalas-kupit-shpionskoe-po-dlya-slejki-za-polzovatelyami-iphone>

⁴⁴<https://www.segodnya.ua/world/usa/big-brother-facebook-budet-sledit-za-peremeshcheniem-polzovateley-v-ramkah-borby-s-pandemiy-koronavirusa-1426746.html>, <https://internetua.com/facebook-predlagauat-ispolzovat-dlya-poiska-zarajennyh>

⁴⁵<https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>, <https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/>

⁴⁶https://kyivcity.gov.ua/news/u_stolitsi_zapustili_Telegram-bot_dlya_dstantsiyonogo_kontrolyu_za_dotrimannyam_kiyanam_i_rezhimu_samoizolyatsi/

⁴⁷<https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond>