Criminal law treatment of deviant behavior in media and social networks

Yulia Gracheva

Professor, Chair of Criminal Law, Kutafin Moscow State Law University, Doctor of Juridical Sciences. Address: 9 Sadovo-Kudrinskaya Street, Moscow 125593, Russia. E-mail: uvgracheva@mail.ru

Sergey Malikov

Professor, Chair of Criminal Law, Kutafin Moscow State Law University, Doctor of Juridical Sciences. Address: 9 Sadovo-Kudrinskaya Street, Moscow 125593, Russia. E-mail: s.v.malikov@yandex.ru

Alexander Chuchaev

Professor, Chair of Criminal Law, Kutafin Moscow State Law University, Doctor of Juridical Sciences. Address: 9 Sadovo-Kudrinskaya Street, Moscow 125593, Russia. E-mail: moksha1@rambler.ru

Abstract

It would be difficult to imagine modern society without information and telecommunication networks, including media and social networks that promote the development of the economy, education, medicine, etc. Media and social networks are an important means of communication and especially so during the coronavirus lockdown; however, the more people are involved in cyberspace, the more crimes are committed there. The subject of this study is deviant behavior on media and social networks with the objectives of identifying the main types of deviant behavior, ascertaining the techniques used to impair public relations protected by criminal law, assessing the existing measures in criminal law that prevent deviant behavior on the internet, and proposing new measures that may be necessary. General scientific (dialectical, logical, systematic) and special legal (comparative legal, formal legal, legal modeling) methods are applied. More than 80% of cybercrime in Russia involves theft using modern social engineering technology for phishing. Although the Supreme Court of the Russian Federation has recommended otherwise, these thefts are treated as a different class in the theory of criminal law and judicial practice. One of the ways to achieve uniformity in law enforcement is to exclude special types of fraud from the Criminal Code of the Russian Federation. Another common way of taking possession of someone else's property is to use a computer program to freeze a system until a certain amount of money has been transferred to a particular account. A gap in the treatment of such acts by criminal law is identified and ways to eliminate it are proposed. The 2020 pandemic highlighted the role of internet in spreading various pieces of fake news; Federal Law No. 100-FZ of April 1, 2020, which supplemented Articles 207.1 and 207.2 of the Criminal Code, was an effective

and timely response. Media and social networks are often used as a platform for inciting, preparing and/or organizing the commission of a crime or other offenses. The study of cyberterrorism shows that there is no need to introduce an independent standard for such acts. Cybercrime also includes attacks on privacy, and the article explores internet harassment in detail by delineating different types of it and the legal response to them. A proposal to amend the wording of Article 137 of the Criminal Code is judged sound.

Keywords

media and social networks; deviation; criminal liability; fakes; phishing; cyberbullying; computer fraud; privacy; cyberterrorism.

Acknowledgments: The work was supported by the RFBR (research project No 18-29-16158)

For citation: Gracheva Yu. V., Malikov S.V., Chuchaev A.S. (2021) Criminal Law Treatment of Deviant Behaviour in Media and Social Network. *Legal Issues in the Digital Age,* no 1, pp. 123–144.

DOI: 10.17323/2713-2749.2021.1.123.144

Introduction

A number of factors make committing crimes in the digital realm tempting. First, its illusion of anonymity and therefore impunity removes the fear of punishment and increases the likelihood of unlawful behavior. Second, the transnational aspect of such criminality together with online access from anywhere in the world means that where a crime is committed may have nothing to do with where the perpetrator is; preparing for a crime and committing it can be coordinated among participants from different parts of the world. Third, over 4.5 billion people are in cyberspace.[1] Fourth, artificial intelligence may be used to commit crimes [Van der Wagen W., Pieters W., 2015: 578]. Fifth, exchange of information is practically instantaneous. Sixth, any necessary information can be collected without calling attention to oneself; this could even include material about potential targets for acts of terrorism and the persons who could carry them out. Seventh, the financial system for digital accounts is uncontrolled, and the transactions that underwrite crimes can be executed anonymously. Finally, detecting and investigating these crimes is difficult and may lag far behind the time when they are committed.

[1] Interpol-Europol 8th Cybercrime Conference: Half of humanity at risk. Available at: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-Europol-8thCybercrime-Conference-Half-of-humanity-at-risk (accessed: 2 February 2021)

Some distinguishing features of deviant behavior in the digital realm are: use of information and telecommunication networks, and in particular media and social networks, which is typically accompanied by illegal access to electronic information; the creation, use and distribution of malware; and violations of the rules governing use of storage, of processing or transmitting electronic information and of information and telecommunication networks.

Over 80% of Russian cybercrime in 2019 involved some form of theft; more than 8% involved illegal sales of narcotics (Article 228.1 of the Criminal Code of the Russian Federation (further, CC RF); and about 1% consisted of crimes involving electronic information. Ministry of Internal recorded 508 personal privacy violations (Art. 137 of the CC RF); 469 crimes related to extremism (Art. 205.2 and 208); 232 violations of copyright and related rights (Art. 146); and 25 suicide-related incidents (Art. 110 and 110.1) [Kirilenko V.P., Alekseev G.V, 2020: 900]. As is the case in all European countries, 80% of cybercrime is prompted by motives of self-interest.

It seems important to identify the basic types of deviant behavior on the internet, understand the hazard they present to society, judge how they fit into the existing legal and regulatory framework, and propose pertinent solutions if there are lacunae. A combination of general scientific and specialized legal research methods will be used to these ends.

1. Phishing — theft or computer fraud?

A substantial number of acts detrimental to society which are committed through social networks involve fraud [Solov'ev V.S., 2016: 60]. Phishing, which is one of the widespread techniques for social engineering, is used to commit fraud by gaining access to confidential user information — logins and passwords. If an email sent as part of a phishing attack contains a link to a counterfeit webpage that precisely mimics the form and content of an official interface and requires entering confidential information (a debit card number, PIN code, etc.),[2] then that theft of property is subject to criminal liability for theft of a bank account (or theft of electronic funds) under Art. 158(3)(d) of the CC RF.

Phishing emails may contain various kinds of programs (trojans) that are installed without permission on the victim's computer, smartphone or other high-tech device if the e-mail is read and the links in it are followed.

[2] How to Recognize and Avoid Phishing Scams. Available at: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (accessed: 2 February 2021)

All the recent bank trojans written for Android are able to divert money automatically.[3]

Some legal scholars of the matter maintain that this method for misappropriating funds has not been properly addressed in the CC RF, even though there are such points as Art. 158(3)(d) and Art. 159.3 and 159.6. They propose supplementing the Code with a separate "form of theft involving a new way of committing it by employing computer technology" [Inogamova-Hegai L.V., 2019: 55]. That proposal might have merit if the legislation had not provided differentiated liability for theft that hinges upon the method use to misappropriate someone's property (Art. 158–162). However, in accordance with the rules for classification under general and special standards, liability would be incurred by committing an act specified by a special standard (for the matter in question that would be Art. 158(3)(d) and Art. 159.3 and 159.6), which renders such proposals pointless. Finally, the legislature has in essence already carried out a related proposal by passing Federal Law of 29 November 2012 No. 207-FZ "On amending the Criminal Code of the Russian Federation and certain legislative acts of the Russian Federation"[4] which inserted Art. 159.6 "Fraud in the field of electronic information" into the CC RF. Despite its title, the crime that Art. 159.6 addresses is not fraud but a separate type of theft with its own methods for misappropriating property or the right to it [Bolsunovskaya L.M., 2016: 15]. Those methods include inscription, deletion, blocking and modification of electronic information or other interference with the functioning of storage devices, with processing and transmission of electronic information, or with information and telecommunication networks. As justification for our position that Art. 159.6 of the CC RF addresses a separate type of theft, we may first cite the first para of the Resolution of the Supreme Court of the Russian Federation of 30 November 2017 No. 48 "On judicial practice in matters of fraud, misappropriation and embezzlement".[5] Its list of the articles of the Criminal Code of the RF, which pertain to fraud omits Art. 159.6. Then, the method of misappropriation of property that distinguishes fraud from other kinds of theft is deception or abuse of trust which causes the victim to transfer their property or the right to it, that is, "there must be a victim of 'deception'" [Kibal'nik A., 2018: 67]. That deception is lacking in the case of computer

[3] Chernykh E. Cybercrime and our telephones. Available at: http://crimescience.ru/?p=9980 (accessed: 2 February 2021)

[4] Collected Laws of the Russian Federation. 2012. No. 49, item 6752.

[5] Bulletin of the Supreme Court of the Russian Federation. 2018. No. 2.

fraud because the victim is unaware of the method for misappropriating the crime's target object [Lopashenko L.A., 2015: 507].

This issue came up when a person identified as Z., who was employed as a sales consultant at the Volga branch of Togliatti regional office of the Megafon mobile phone chain, was convicted under Art. 159.6(1) of the CC RF of modifying the electronic information in the SBMS program used to serve mobile phone subscribers. Z. has transferred illegally funds from personal accounts that belonged to Megafon Company. This computer fraud resulted in theft of 500,699.97 rubles.[6]

The materials in this criminal suit make clear that there was no deception of the victim that would have caused them to independently transfer funds to the guilty party. Furthermore, the courts of the first and appellate instance found no evidence in Z.'s acts of the crime specified in Art. 272 of the CC RF. The court of first instance concluded that Z.'s criminal acts were fully consistent with the offense specified in Art. 159.6 (1). The illegal access to electronic information that Z. obtained for the purpose of carrying out the criminal intent to divert funds from Megafon consisted of acts that constituted the objective aspect of Z.'s fraud as specified in Art. 159.6 (1).[7]

The bodies charged with preliminary investigation of Z.'s acts were commissioned under Art. 272(3) and 159.6(1), which is consistent with the elucidation contained in para 20 of the Decision of the Plenum of the Supreme Court of the RF of 30 November 2017 No. 48. The presidium of the Samara Oblast Court called attention to that circumstance when it responded to the cassation appeal of the victim and the prosecutorial presentation by referring the case for a new trial.

There are two points of interest in the verdict rendered. The first is that not all legal scholars and law enforcement agencies find it obvious that those acts meet the criteria for multiple offenses in accordance with the relevant sections of Art. 159.6. and 272–274 of the CC RF [Kibal'nik A., 2018: 67].[8] They would maintain that computer crimes are a method of committing fraud involving electronic information and that, therefore, those acts were not multiple. The second is that it would be difficult to agree that the acts meet the criteria of Art. 159.6(1) of the CC RF because there is no

[6] Decision of the Presidium of the Samara Oblast Court. 14 February 2019 No. 44U-36/2019, 44U-37/2019 // SPS Consultant Plus.

[7] Ibid.

[8] Verdict of Kaluga Regional Court. 9 August 2017. Case of B. In: Criminal jurisdictional activity under digitalization. Moscow, 2019, p. 114.

victim of deception, and it is no less difficult to accept the existing standard and the explanations of the practices for applying it provided by the Plenum of the Supreme Court of the RF.

Distinguishing between several special types of fraud and theft is a problem that has come up both in theory and in practice, and it has not been solved by the passage of Federal Law of 23 April 2018 No. 111-FZ "On amending the Criminal Code of the Russian Federation" which inserted para. 3 into Art. 158 of the CC RF and para 3 and subparagraph d into Art. 159.6 of the CC RF (theft and fraud, respectively, with respect to money "from a bank account and equally with respect to electronic funds") and clarified the title and content of Art. 159.3(1) of the CC RF as fraud by means of electronic execution of payment.[9] Our view is that this in fact blurred the distinction between theft from a bank account (Art. 158(3) (d) and fraud by means of electronic execution of payment (Art. 159.3) and computer fraud (also Art. 159.6). Some authors maintain that it has been difficult to find characteristics that would set theft from a bank account apart from general criminal fraud employing information and communication technologies and electronic execution of payment (Art. 159) [Russkevich E., 2019: 60]. If a perpetrator took possession by any means of the debit card and personal information of a victim and, for example, withdrew cash from an ATM and then made a wire transfer from the victim's card to someone else's account, that act would certainly meet the criteria of Art. 158(3)(d) of the CC RF. Ivan Klepickij takes a diametrically opposed position that this would be an instance of the crime specified by Art. 159.3. "The current version of the law does not require for the application of Art. 159.3 that there be a victim of deception, and the manner of committing the crime is likewise not specified" [Klepickij I.A., 2021: 357]. His position has at times been upheld in judicial practice. For example, a person who found a wallet with two bank cards and spent 12,984.31 rubles via contactless payments was convicted under Art. 159.3.[10] However, the Cheryomushki District Court of Moscow arrived at opposite conclusion in its verdict that Art. 158(3) (d) applied to the actions of an automobile driver who transferred funds to his own bank card from a mobile phone with its mobile banking interface still open that someone had left in a rear passenger seat compartment.[11]

[9] Collected Laws of the Russian Federation. 2018. No. 18, item 2581.

[10] Verdict of the Graivoronsky District Court, Belgorod Oblast. 15 July 2019. Case No 1-40/2019.

[11] Verdict of the Cheryomushki District Court of Moscow. 15 July 2019. Case No 1-387/2019.

The same classification should apply to manipulation involving electronic information through which a person gains access to someone's bank account (by social engineering, for example) and then arranges wire transfers of funds from the victim's account to their own or to another person's. Clearly cases of this kind should incur criminal liability not only for theft (Art. 158(3)(d) but also for crimes involving electronic information (Chapter 28 of the CC RF). The classification would be no different even when "manipulation involving electronic information (inscription, modification, etc.) does not result simply in movement of funds, but also when it disrupts normal operations in the information and communications infrastructure (such as blocking a personal user account in a system for providing remote services)" [Russkevich E., 2019: 61].[12] In these situations, the method used to misappropriate someone's property is unchanged and remains concealed.

Art. 158(3)(d) of the CC RF and that article as a whole, which together prescribe liability for computer crime, should also apply to acts of a perpetrator who uses a trojan computer program to obtain remote access to a system (a personal computer, mobile banking, etc.) and then to install programs that control the keyboard and mouse in parallel with the system's operator in the event that the illegitimate access to information has been used to misappropriate someone's property.

It follows that neither Art.159.6 nor Art. 159.3 cover theft through electronic execution of payments or involving electronic information as a way to seize someone's property because any deception or abuse of trust which causes the victim to "voluntarily" give that property away is absent. The proposal in this connection would be, first, to classify theft of another person's property according to legislation that delineates the forms of theft. This would make Art. 159.6 superfluous. The second part of the proposal would be to exclude any special content of fraud from the CC RF. Although this is not a new idea, it has become all the more pressing. It follows that retaining Art. 159.6 is inadvisable, first, because it does not solve the problem of one alternative for theft (Art.158(3)(d) competing with another in the section on theft involving electronic information. Second, the existence of special criteria should be justified by broader or narrower impositions of liability for the crimes that are established by them. However, the penalties for committing the acts specified by Art. 158(3)(d) and 159.6 debates over the necessity of criteria for the entire range of fraud involving electronic information and computer crimes.

[12] Russkevich maintains that this would be an instance of fraud involving computerized information.

2. Extortion via the internet: Gaps in regulation by criminal law

Ransomware is a type of computer program (trojan) contained in phishing emails. The program will block the operation of a computer and demand transfer of a certain amount of money to an account such as an electronic wallet as a condition for restoring the functionality of the system. It will also threaten to erase information kept on the computer if the demand is not met. These program codes are not designed to damage computers as such or their parts, but instead to erase information located in them. Acts of this kind incur cumulative liability: under Art. 272(2) (motivated by gain) or 272(4) if the consequences are grave or if there is a threat of such consequences; and under Art. 273 because creating and deploying harmful programs in not covered under Art. 272. Liability under Art. 273 is necessarily incurred whether the perpetrator wrote the harmful program or obtained it ready for use; this is because a socially hazardous act in Art. 273 may take alternative forms as creation, dissemination and use. This position has been confirmed by judicial practice.[13]

A demand that money be transferred with a threat to erase information (databases) cannot as such be classified under Art. 163 even though it is intended to misappropriate another person's property. Extortion is defined as a demand for the transfer of someone's property under threat of violence or of destruction or damage to someone's property, as well as threat of dissemination of information harmful to the victim's reputation, etc. According to Art. 128, in which ownership rights are defined in relation to property, information and databases are not considered property although they may be subject to civil rights [Danilov D., 2018: 37–42]. The fact that Art. 163 makes no reference to commission of a crime by threatening to erase information and thus hampers proper recognition of such acts by criminal law constitutes a problem, which must be eliminated by agenda to Art. 163(1) of the CC RF so that this kind of threat is specified.

3. Fakes on social networks

In February and March 2020 an intensive campaign of fakes concerning the coronavirus infection (COVID-19) was launched. It was intended to induce fear and panic in the populace, to give the impression that the

[13] For example, by the Appellate Decision of the Moscow City Court of 27 November 2020 in case No. 10-16199 // Consultant Plus.

country's leaders could not deal with the outbreak and were concealing important information, and to compromise and discredit law enforcement agencies, etc. As the World Health Organization acknowledged, a true "pandemic of fake news" or "infomedia" came along right after COVID-19 had taken off, and it spread across the planet even faster than the virus itself. Its main "carriers" were mobile platforms and, above all, the popular messaging service WhatsApp.[14]

The pandemic of fakes "blanketed" Russia too. The governor of Yamal had to intervene in order to debunk one of these fakes. On local networks rumors persisted that someone in the top management of a gas producing company went to Italy and, "didn't tell anyone about it or stayed in quarantine, and everyone in the town was exposed, which caused a coronavirus outbreak". Within a week that story seemed almost official. A fake circulated at about the same time in Ufa stated that a thousand graves were being prepared somewhere in the vicinity to accommodate coronavirus deaths. In the town of Chebarkul in Chelyabinsk oblast one woman claimed in all seriousness that troops were dispatched to the city to suppress "food riots".[15]

To prevent mass dissemination of fakes that would cause panic and disturb public order, Federal Law of 1 April 2020 No. 100-FZ "On amending the Criminal Code of the Russian Federation and Articles 31 and 151 of the Criminal Procedural Code of the Russian Federation" was passed. It supplemented the CC RF with Art. 207.1 "Public dissemination of intentionally falsified information about circumstances that constitute a threat to the lives and safety of citizens" and 207.2 "Public dissemination of intentionally falsified information that leads to grave consequences".[16] This law came into force 1 April 2020.

Presidium of the Supreme Court of Russia has explained that fakes related to COVID-19 fall under Art. 207.1 because "spreading infection by the novel coronavirus (COVID-19) within the Russian Federation has currently and may in the future result in human suffering, harm to human health, substantial material losses, and disruption in the living conditions of the populace...."[17]

---

[14] Available at: https://rg.ru/2020/04/16/voz-obiavila-o-pandemii-fejkov.html (accessed: 23 April 2020)

[15] Available at: https://rg.ru/2020/04/18/reg-urfo/advokat-rasskazal-chto-zastavliaet-liudej-rasprostraniat-fejki-o-koronaviruse.html (accessed: 23 April 2020)

[16] Rossiyskaya gazeta. 3 April 2020.

[17] Review of selected issues in judicial practice as they concern application of legislation and measures to combat the spread of the novel coronavirus (COVID-19) within the Russian Federation. No. 1 // Consultant Plus

The actions of individual persons are evidence of criminally punishable acts under Art. 207.1 of CC RF in the event that they constitute public dissemination of seemingly trustworthy accounts of intentionally falsified information about circumstances that present a threat to the lives and safety of the populace, including about the circumstances associated with the spread of the novel coronavirus (COVID-19) within the Russian Federation or circumstances associated with the protective measures, techniques and methods adopted to ensure the safety of the populace in those circumstances. If spreading such falsehoods constitutes an actual hazard to society and harms public safety and order, then criminal liability is incurred.

Socially significant information may also include information about the circumstances that constitute a threat to the lives and safety of the population and/or about the protective measures and methods adopted in order to ensure the safety of the population and territory in such circumstances.[18]

If fakes result in someone's death or harm to their health, then the acts would fall under Art. 207.2.

Various social networks are typically involved in disseminating such information, as review of both Russian and international practices will show.

Social networks are monitored on a daily basis in order to prevent the spread of such information. The materials that turn up are vetted, and if any information about circumstances that constitute a threat to the lives and safety of the populace is intentionally falsified, then Roskomnadzor will block it. For example, internet monitoring discovered a report alleging that those who died of the coronavirus were being removed by night from an observation center in Krylatskoye. Official information, however, stated that the observation center was being used to quarantine healthy people who had to leave self-isolation because of contact with someone infected. The Moscow City prosecutor followed up with an investigation concerning the fact of publication. The materials were turned over to the Investigative Committee for a determination of whether to lodge a criminal suit under Art. 207.1.[19]

A video clip with the headline "COVID-19 is transmitted by testing" on YouTube was discovered. The originator claimed that "the coronavirus was developed in the laboratory from a virus in bats, which was not transmissible between humans. It is carried to human beings by the testing

[18] Ibid.

[19] Available at: https://rg.ru/2020/04/18/genprokuratura-obnaruzhila-resursy-rasprostraniaiushchie-fej-ki-o-koronaviruse.html (accessed: 23 April 2020)

because 15–20% of tests are infected. Air-borne particles do not transmit it." The Prosecutor General found that the video stating that infection is the result of testing could convince people to reject testing and delay getting prompt assistance for severe infection. The originator of the clip was charged with a crime specified by Art. 207.1. On the official site devoted to combating coronavirus infection, information is posted about how it is transmitted by air-borne particles. This and other circumstances confirm the dissemination of intentionally falsified information.

4. Incitement to crime via media and social networks

Another risk arising from media and social networks is their use as platforms for inciting, preparing and/or organizing crime or unlawful acts.

On 23 and 31 January 2021 unlawful demonstrations showed evidence of using the internet, the social networks TikTok, VKontakte, Facebook, Twitter, Instagram, and the YouTube service to organize public disorder, spread slander, and persuade minors to commit acts that, at minimum, would constitute a hazard to their lives.

In the middle of that week Roskomnadzor required social networks to suppress solicitations to participate in the demonstrations. The Prosecutor General in turn insisted on imposing a complete ban on access to the websites that published such solicitations.[20]

It was observed that the irregular opposition in this instance turned to schoolchildren and not merely to secondary school students, but also younger children, and that it provided them with detailed instructions on how to behave at the demonstration, including extracting the SIM cards from telephones taken to the demonstration.

Roskomnadzor reported that moderators at VKontakte and YouTube deleted about 50% of total unlawful content that came to their attention. The TikTok app removed 38% and Instagram 17% of such data. Criminal cases under Art. 151.2(2)(c) of the CC RF (inciting minors on information and communication networks to commit acts that present a threat to their lives) were opened. In addition, the acts of the organizers and individual participants of unauthorized demonstrations could be charged under Art. 212.

Several researchers have found that al-Qaida, for example, is relying much more frequently on the digital communication platforms of Tele-

[20] Available at: https://rg.ru/2020/04/18/genprokuratura-obnaruzhila-resursy-rasprostraniaiushchie-fejki-o-koronaviruse.html (accessed: 23 April 2020)

gram and Signal. Jihadists prefer Twitter and Facebook to spread ideological propaganda. Cyberextremists rely heavily on the apps and programs of WhatsApp, Threema, Kik, Wickr and SureSpot to exchange messages.[21] As one example, a person identified as S. was convicted under Art. 205.2(2) of the CC RF of using the internet to call publicly for terrorist activities and publicly justify terrorism. The court acquitted S. of the charge of terrorist propaganda. The Judicial Collegium for Servicepersons changed that verdict and found that S.'s actions came under Art. 205.2(2) as public calls for terrorist activities, public justification of terrorism, and terrorist propaganda committed via the internet.

The court of first instance acquitted S. of terrorist propaganda on the grounds that the actions of the accused were not systematic in nature. However, that court's conclusion stands in contradiction to the materials introduced in the case and hinges upon an incorrect application of criminal law. By note 1.1 under Art. 205(2), terrorist propaganda is activity which disseminates materials and/or information aimed at indoctrinating a person with terrorist ideology, convincing them of its appeal or of the acceptability of terrorist action.

The hearings established that S. had three times posted for public viewing on his personal VKontakte page images, photographs and his comments on them which, according to the findings of experts, used psychological and linguistic techniques to incite violent acts (commission of acts of terrorism) against those who do not adhere to Islam; and in a second comment there were also justifications and approval of terrorist actions (armed jihad, and in particular as part of an international terrorist organization) as correct and objects for support and emulation.

The experts found also that material in the second comment affirmed the supreme importance of the pursuit of death by Muslims, approved of Muslims who had died in jihad, glorified the role of shahids, disapproved of non-Muslims, and spoke of the supreme value of fighting against "unbelievers" and the need to raise children within the traditions of that fight.

The acts of S. referred to in the verdict, the form and content of publications posted and openly accessible on the internet, his persistent intent to disseminate materials of a terrorist nature, and the testimony of witnesses concerning S.'s calls for acts of terrorist and public justification of terrorism — all these in sum show that he not only made public calls for acts of

[21] Is technology helping or hindering the fight against terrorism? Available at: https://wp.nyu.edu/dispatch/2017/12/15/is-technology-helping-or-hindering-thefight-against-terrorism/ (accessed: 15 March 2020)

terrorism and publicly justified terrorism, but that he also disseminated materials intended to inculcate an ideology of terrorism and a conviction that terrorism is appealing or that acts of terrorism are justified, which is to say that he engaged in terrorist propaganda.[22]

Terrorist propaganda, recruiting and training supporters, radicalizing a community, soliciting contributions, collecting information, arranging communication, and planning definite terrorist attacks through use of the internet are a hybrid form of cyberterrorism. In its pure form, it means actual attacks that usually target the critical information infrastructure of the Russian Federation in order to achieve political, religious or ideological objectives.

Some legal scholars regard the dissemination via internet of intentionally falsified information about impending terrorist acts as cybercrime (Kuleshova G.P., Kapitonova E.A., Romanovskij G.B., 2020: 161). In September 2017 there was an instance in Russia of dissemination of deliberately falsified reports of impending terrorism. It targeted the information databases of state institutions and caused damage appraised at over 300 million rubles. FSB Director Alexander Bortnikov reported that the four perpetrators were Russian citizens located abroad.[23] The media reported a version of events in which foreign special services had commissioned the attack to test a new method for hybrid warfare. In October 2018 the United Kingdom openly threatened Russia with a cyberattack on Moscow's electricity grid in the event of any aggression carried out against NATO or its allies.[24] Russia's special services have regarded acts of this kind as state terrorism.

Cyberterrorism has lately been the focus of increased attention. In the US and Western Europe cyberterrorism has mostly political connotations. Those countries peddle the notion that Russia, China and Iran pose a cyberthreat and promote the ideology that a cyberspace offensive against those countries must be mounted.

Criminal law studies on these topics are engaged in debate about how to increase liability for use of the internet to carry out terrorism. As always,

[22] Appellate Decision No. 225-APU19-1. Review of the judicial practice of the Supreme Court of the Russian Federation No. 1, 2020 // Bulletin of the Supreme Court of the Russian Federation. 2020. No. 10.

[23] Damage from telephone terrorism in Russia cost 300 million rubles. Available at: https://ria.ru/defense_safety/20171005/1506292428.html (accessed: 23 April 2020)

[24] UK war-games cyber attack on Moscow. Available at: https://www.thetimes.co.uk/edition/news/uk-war-games-cyber-attack-on-moscow-dgxz8ppv0. (accessed: 23 April 2020)

opinions differ. One writer, for example, has proposed increasing the liability stipulated in Art. 205(2) for committing acts of terrorism by hacking into computer systems [Chekunov I.G., 2012: 43]. Others reject that suggestion on the grounds that the existing features of criminal law for counteracting cyberterrorism are sufficient [Kuleshova G.P., Kapitonova E.A., Romanovskij G.B., 2020: 163].

The latter position has merit, first, because a reading of Art. 205(1) of the CC RF indicates that it applies liability both for carrying out bombings, arson, etc. and also for the threat to do so. The mere threat is a less dangerous act than in fact setting off an explosion or arson; hence, an act of terrorism of that kind would incur penalties that are closer to the minimum prescribed in Art. 205(1). In such instances, circulating the threat via the internet does not require establishing that as a criterion and can be taken into consideration when a penalty is imposed under the sanction.

Furthermore, certain passages, such as some in Art. 205.2, have such a criterion.

5. Personal privacy in media and social networks

Media and social networks have become a convenient platform for carrying out internet harassment. In one fashion or another, harassment has affected half of all children. Adolescents who have been victims of harassment on the internet have usually been subjected to it beforehand in real life so that virtual harassment often exacerbates actual violence.

Along with adolescents, victims include public figures (actors, sport stars, people in show business, etc.) and former partners.

Internet harassment (cyberbullying) is defined as deliberate insults, threats, defamation or disclosure of compromising information to others by means of modern channels of communication and usually for an extended length of time. Along with "cyberbullying" such other terms as "internet mobbing" and "cyber-mobbing" for this phenomenon have been derived from English.

All forms of internet harassment share the following characteristics:

They are carried out online via information and communication channels, or via mobile phones through transmission of obscene video and audio clips, text messaging, or annoying calls. This enables: a) round-the-clock interference with privacy (attacks do not cease after the school or work day); b) unlimited geographic reach, which allows an unlimited audi-

ence and immediate dissemination; c) practical anonymity for the source of the messages or images that are transmitted electronically.

They are a form of persecution, i.e. illegal restriction of the right to life, health, free choice of residence, freedom of movement, etc., as well as a cause of moral damage, psychological trauma, and impairment of honor and dignity by insults, bullying, persistent slander, etc.

They are carried out for a long time as systematic acts characterized by some kind of harassment — circulating deliberate falsehoods (rumors and gossip) about a person, ridicule and provocations, direct insults and intimidation, shunning (boycotts and demonstrative disregard), attacks that impair the honor and dignity of a person and cause material or physical harm.

The victim typically does not know who is behaving aggressively because the perpetrator conceals their identity from the victim and can operate anonymously, which provides a feeling of impunity and often prolongs the attack. The victim's ignorance of the identity of the persecutor can contribute to feeling bullied, intimidated and upset.

"Internet bullying" is a phrase that refers first of all to cyberstalking, which consists of acts that disrupt personal privacy through persecution (telephone calls, emails, surveillance, etc.), persistent molestation, direct and indirect threats, gross insults and harassment. The case of a person referred to as G. is indicative in this regard. G. was accused of intentionally inflicting grievous bodily harm (Art. 111(2)(h) of the CC RF) and issuing death threats (Art. 119). When G. learned that his wife wanted a divorce, he stalked her, frequently threatened her and once took her to a forest where he placed a knife at her throat and demanded that she tell him about her relations with other men. She brought this to the attention of the police, but they would not issue criminal charges because tangible evidence of her husband's crime was lacking (although the fact that the accused had placed a knife at her neck might have been sufficient, even in the absence of any other evidence, for the applying Art. 119) [Yurchenko I.A., 2021: 179]. Prompt application of criminal law to G.'s deviant behavior might have prevented him from committing a more serious crime; he would not have cut off the victim's hand.

One type of cyberstalking is molestation carried out for sexual motives, which is usually termed harassment and is often practiced by supervisors against their subordinates. In Russian criminal law, these acts may be evidence of the crime specified by Art. 133.

Cyberbullying may take the form of public disclosure of personal information often referred to as outing or trickery in English. This involves

revealing personal information, intimate photographs, information about state of health or finances, as well as acts meant to humiliate or blackmail someone such as a former partner, etc. District Court in Ulyanovsk City found a person referred to as N. guilty of posting on internet files entrusted to him by a person referred to as G. These files contained G.'s personal information including personal secrets along with videos and intimate photographs of her. N. had vengeful motives for circulating those materials without G.'s consent because she had broken off relations with him.[25]

A person referred to as A. was convicted of two types of cyberstalking — sexual harassment (harassment in the primary sense) by means of disclosure of personal information (outing and trickery) – under Art. 133(1) and 137(1). While living with his girlfriend, he used a mobile phone and webcam to record images and videos without her consent of their sexual encounters. After their relationship dissolved, he began to blackmail the victim by threatening to circulate the material he had gathered unless she would resume sexual relations with him. As proof that his threat was serious, he posted photos that were in his possession on a social network.[26]

In early 2021 world witnessed internet harassment of US President Donald Trump. The top management of the major social networks in the USA decided that further posting on their platforms in his capacity as president would constitute a risk of violence. After blocking Trump, those services also blocked a large number of his supporters. Twitter, Facebook, Instagram, Reddit, Discord, TikTok, Twitch, Snapchat and YouTube all took part in this unprecedented campaign. Amazon denied hosting on its servers to the Parler network, which was popular with Trump's supporters, and it became inaccessible to users as a result. In response Trump declared, "You can't silence us!" and announced the creation of his own internet platform. The popularity of Telegram soared in this environment to become the second most downloaded app in the United States.

This kind of cyberbullying is considered social isolation or exclusion, i.e., refusal to maintain contact both commercially and informally, which may mean blocking a contact, excluding an instant messenger group, or a gaming community or other community (or communities), etc.

Social isolation of Donald Trump's network brings two problems to the fore. First, there is the question of the legitimacy of censorship and limits

[25] Judicial and regulatory acts of the Russia. Available at: https:// sudact.ru / regular/court/ reshenya-leninskii-raionnyi-sud-g-ulianovska- ulianovskaia-oblast (accessed: 10 February 2021)

[26] Available at: https://pravo.ru/ news /view/118866 (accessed: 10 February 2021)

on freedom of speech. Second, the largest IT corporations are now in fact political powers whose activities demand regulation by law. The resulting conflict has also been seen as evidence of the culture war that has sundered American society.[27]

Yet another type of cyberbullying is an open threat of physical violence, also called a cyberthreat; it consists of a direct or indirect threat to kill someone or inflict bodily harm. In Russian law these acts fall under Art. 119 of the CC RF as death threats or threats to inflict severe injury.

Among the acts classified as internet harassment, there are those that denigrate someone's honor, dignity or business reputation, such as:

blackening a victim's reputation, spreading rumors, or denigration; deliberately presenting them in a negative light by posting photos or videos on the internet (on websites, forums, and newsgroups) or by email. The motive behind these acts may be to disrupt friendly or partnership relations or to take revenge on a former friend;

use of fictional names or impersonation; this includes deliberately impersonating another person by using their password and login to commit antisocial acts, such as insults or humiliation, that will be attributed to the victim.

Ridicule, mockery, provocation or trolling online.

Insults or flaming; this type is characterized by openly making offensive comments, vulgar references and remarks online.

A person referred to as B. was found guilty of ten insults directed at a judge of the Saint Petersburg City Court, obstructing investigation of the case, and inflicting bodily harm on the investigator. The court found that for seven months B. had repeatedly called the judge on a landline telephone and had left various kinds of voicemail including offensive ones. The perpetrator wanted to take revenge on the judge for deciding against her in a civil suit. The investigation classified the matter as commission of ten criminal acts specified by Art. 296(1) of the CC RF and ten more criminal acts specified by Art. 130(1). During the investigation, the public prosecutor dropped the charges under Art. 296(1) because it was found that threats as such were not made, although there was foul language did not have any definite meaning.[28]

[27] Available at: https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D0%B8%D1 %80%D0%BE%D0%B2%D0%BA%D0%B0_%D0%94%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%B4%D0%B0_%D0%A2%D1%80%D0%B0%D0%BC%D0%BF%D0%B0_%D0%B2_%D1%81%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D1%85_%D1%81%D0%B5%D1%82%D1%8F%D1%85 (accessed: 2 February 2021)

[28] (Accessed: 12 February 2021)

Study of the types of cyberbullying outlined shows, first, that there is no single standard in Russian law that prescribes liability for internet harassment. Second, several categories of internet harassment incur administrative liability: insults (Art. 5.61 of the Code of the RF on Administrative Offenses [further COA RF]), assault and battery (Art. 6.1.1 of the COA RF), disorderly conduct (Art. 20.1 of the COA RF). Other types incur criminal liability: assault and battery (Art. 116 of the CC RF), assault and battery by a person subject to administrative penalties (Art. 116.1 of the CC RF), threatening death or infliction of grave injury (Art. 119 of the CC RF), coerced sexual acts (Art. 113 of the CC RF), violation of personal privacy (Art. 137 of the CC RF), breach of the confidentiality of correspondence, telephone conversations, postal, telegraph or other messages (Art. 138 of the CC RF), unlawful access to special technical equipment intended for clandestinely obtaining information (Art. 138.1 of the CC RF), violation of domestic privacy (Art. 139 of the CC RF), extortion (Art. 163 of the CC RF), unlawful access to computerized information (Art. 272 of the CC RF), and the creation, use or distribution of harmful computer programs (Art. 273 of the CC RF).

Finally, several kinds of harassment and internet harassment fall outside the scope of the law, such as periodic telephone calls and SMS texts, surveillance by an obstinate admirer, threats expressed on social networks by fanatics, etc. even though these may be precursors to a grave or extremely grave crime. Then too, some kinds of harassment and internet harassment receive no independent recognition in criminal law. Nevertheless, when they are long-term, systematic and intrusive, they provoke mental anguish that may harm health or lead to suicide.

To address this, some writers suggest following international practice by incorporating a criterion for persecution analogous to foreign ones into the Russian Criminal Code [Barysheva K.A., 2017: 347–350]. For example, §238 of the German Criminal Code prescribes liability for a perpetrator who persistently stalks a person as follows:

Whosoever unlawfully stalks a person by:

seeking proximity to them;

trying to establish contact with them by means of telecommunications or other means of communication or through third persons;

abusing their personal data for the purpose of ordering goods or services for them or causing them to make contact with the perpetrator;

threatening them or a person close to them with loss of life or limb, damage to health or freedom, or

committing similar acts;

thereby seriously infringes their lifestyle shall be liable to imprisonment not exceeding three years or a fine [Golovnenkov P.V., 2021: 346].

Criminal liability becomes more severe in the event that the crime subjects the victim, their relatives or others close to the victim to mortal danger or causes them grave injury or death. The offenses then incur imprisonment for up to ten years.

Complex criteria for stalking are also found in the criminal law of the USA and the United Kingdom.

In 2013 New Zealand passed a law that imposes criminal liability for cyberbullying. A person who is guilty of sending intimidating, racist, sexist or any other message that causes "serious emotional distress" may be punished by imprisonment for two years. In addition, the law distinguishes encouraging suicide as a separate category of crime, which is punishable by imprisonment for up to three years.[29]

Criminal law in other countries designates harassment a crime in the USA and Japan, while revenge porn is a crime in Israel, the USA and the UK, etc.

Introducing liability for harassment (extortion, stalking, bullying, etc.) would, first, not solve the problem of law enforcement and, second, would cause problems in making distinctions between the criteria for crimes that are already present in Art. 110, 110.1, 133, 137 and 138 of the CC RF among others.

It would be more effective to revise the existing criminal law standards in a carefully considered way, and several such proposals have already been made [Yurchenko I.A., 2018: 56].

There is another opinion on this matter. Pavel Golovnenkov in his commentary on §238 of the German Criminal Code notes that several kinds of unlawful persecution by applying psychological pressure to a person (under certain conditions) are punishable under general criteria intended to protect bodily security and personal freedom (for example, personal freedom in §240 of the Code, threats in §241, inflicting bodily harm in §223 and others) and under the provisions of §4 of the Law on Protection of Civil Rights from Acts of Violence and (Unlawful) Harassment (*Gesetz zum zivilrechtlichen Schutz vor Gewalttaten und Nachstellungen* [*Gewaltschutzgesetz — GewSchG*] of 11 December 2001, BGBl. 2001 I S. 3513). Law enforcement practice has indicated that, in order to effectively combat infringements of

[29] Available at: http://sanktpeterburg.bezformata.com/listnews/novoj-zelandii-kiberbulling-stal/35038126/ (accessed: 30 January 2021)

personal human rights by lengthy unlawful harassment carried out in a variety of ways, as well as to mitigate the potential for danger that may lie behind such behavior, the Criminal Code had introduced § 238 which sets separate criteria that cover to the fullest extent possible the entire range of criminal acts in the matter (BT-Drs. 16/575, S. 1; 16/1030, S. 1). The benefit that the law protects in this case is the freedom of the individual to exercise their preferences and carry out their personal activities in their own way of life. Furthermore, provisions of §238 (para 2 and 3) protect a potential victim's physical security and life from unlawful harassment (see BT-Drs. 15/5410 S. 6, 16/1030 S. 6) [Golovnenkov P.V., 2021: 347 ff].

Conclusion

The allure of committing crimes via the internet arises from a number of circumstances: the illusion of committing a crime anonymously; the transnational nature of those crimes; the presence of over 4.5 billion persons in cyberspace; the opportunity to commit crimes using artificial intelligence; immediate information exchange; the concealment afforded by the internet for preparation to commit a crime; the uncontrolled financial system, digital accounts and anonymous transactions that can underwrite crimes; and finally the difficulty in detecting and investigating such crimes, which results long-delayed responses. Deviant behavior online is characterized by use of information and communication networks including media and social networks, which is usually accompanied by unlawful access to computer information; the creation, use and dissemination of harmful software; and also improper use of storage, processing or transmission of electronic information and of information and telecommunication networks.

Theft by phishing accounts for over 80% of Russian cybercrime committed by means of modern social engineering technology. Although it runs counter to the recommendations of the Plenum of the Supreme Court of the RF, these crimes are given various interpretations. One way to make law enforcement more consistent is to exclude special categories of fraud from the CC RF and classify such crimes under 158(3)(d) as theft from a bank account or theft of electronic credits under Art. 272, 273 and 274.1.

A common way to seize someone else's property is to use software that makes a system inoperative and demand sending money to a certain account in return for restoring functionality. There is a gap in criminal law's recognition of such acts, and the proposal is to supplement Art. 163(1) to address tries to destroy information.

While media and social networks are regularly used to disseminate fakes, to prevent mass dissemination of fakes that would cause panic and disturb public order, Federal Law of 1 April 2020 No. 100-FZ was adopted to supplement the CC RF with Art. 207.1 "Public dissemination of intentionally falsified information about circumstances that constitute a threat to the life and safety of citizens" and Art. 207.2 "Public dissemination of intentionally falsified information that leads to grave consequences".

Media and social networks have become a platform for inciting, preparing and/or organizing crime or other offenses. The polemics surrounding cyberterrorism were found to be indicative of the debate about increasing liability for use of internet for committing a crime. The position arrived at rejects any agenda to the CC RF. Art. 205(1) stipulates liability for setting off an explosion, arson, etc. as well as for the threat to do so. A threat is a less dangerous action than an actual explosion or arson; if an act of terrorism consists only of the former, then it should incur a punishment toward the minimum provided in Art. 205(1). Hence, disseminating a threat via the internet would not require inclusion in the law as a distinct classification and could be taken into account in applying a sentence within the range of punishments.

Internet harassment is widespread in cyberspace. One type that has not been properly addressed by the law is cyberstalking, which consists of violations of personal privacy (telephone calls, e-mails, surveillance etc.). When they are long-term, systematic and intrusive, they constitute mental harassment that may harm health or lead to suicide, force the victim to alter their accustomed way of living and in some cases are precursors to grave or extremely grave crime. Some legal experts proposed addressing this by inserting a separate article into the CC RF in order to stipulate the liability for cyberstalking. Other writers make the more persuasive case that agenda to the Art. 137 should be made in order to provide the criteria, that would permit making a distinction from the criteria for crimes that are already stipulated by Art. 110, 110.1, 133 and 138 among others.

The state should provide a national corpus of law mandating that internet service providers monitor malicious traffic and block it.

References

Barysheva K.A. (2017) Kiberstalking as a new form of criminal action. In: Ugolovnoe pravo: strategiya razvitiya v XXI veke. Moscow: RG-Press, pp. 347–350 (in Russian)

Bolsunovskaya L. M. (2016) The criminalization of a computer information fraud in the Russian law. *Biblioteka kriminalista*, no 3, pp. 15–20 (in Russian)

Chekunov I.G. (2012) The cybercriminality: term and classification. *Rossijskij sledovatel'*, no 2, pp. 37–44 (in Russian)

Danilov D. (2018) The qualification of Dos-attacks produced by profit interests. *Ugolovnoe pravo*, no 6, pp. 37–42 (in Russian)

Golovnenkov P.V. (2021) The German Criminal Code (Strafgesetzbuch (StGB). Tanslation and comments. Potsdam: University Press, 489 pp. (in Russian)

Inogamova-Hegaj L.V. (2019) The qualification of cybercrimes. In: Ugolovnoe pravo: strategiya razvitiya v XXI veke…. Moscow: RG-Press, pp. 52–55 (in Russian)

Kibal'nik A. (2018) The qualification of a fraud according to recent decision of the Supreme Court of the Russian Federation. *Ugolovnoe pravo*, no 1, pp. 61–67 (in Russian)

Kirilenko V.P., Alekseev G.V. (2020) The garmonization of the Russian anti-criminal legislation with legal standards of the European Council. *Vserossijskij kriminologicheskij zhurnal*, no 6, pp. 898–913 (in Russian)

Klepickij I.A. (2021) New *economic criminal law*. Moscow: Prospekt, p. 984 (in Russian)

Kuleshova G.P., Kapitonova E.A., Romanovskiy G.B. (2020) Legal basis of fight against cyberterrorism in Russia and abroad. *Vserossijskiy kriminologicheskij zhurnal*, no 1, pp. 156–165 (in Russian)

Lopashenko N.A. (2015) Legal reform of a fraud: forced questions and forced answers. *Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta*, no 3, pp. 504–513 (in Russian)

Russkevich E. (2019) Division of a theft from bank account from adjacent forms of crimes. *Ugolovnoe pravo*, no 2, pp. 59–64 (in Russian)

Solov'ev V.S. (2016) Criminality in social cells of Internet. A study of judicial practice. *Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta*, no 1, pp. 60–72 (in Russian)

Van der Wagen W., Pieters W. (2015) From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology*, no 3, pp. 578–595.

Yurchenko I.A. (2021) *The crimes against information security.* Moscow: Prospekt, 208 pp. (in Russian)

Yurchenko I.A. (2018) Stalker as an object of criminal liability. *Vestnik Universiteta O.E. Kutafina*, no 12, pp. 53–56 (in Russian)