Criminal Exploitation of Information and Communication Technologies: Riots

Received: 31 February 2023; Accepted: 6 March 2023 *Research Article*

Murad M. Madzhumayev
Department of Criminal Law, Criminal Procedure and Criminalistics of Law Institute
Peoples' Friendship University of Russia (RUDN University)
Moscow, Russian Federation
murad.mad@outlook.com
0000-0003-3332-2850

***Abstract*—The availability, reliability, security of information and telecommunication networks and systems constitute crucial pillars for enhancing standards of living, employment, business and civil society organizations, augmenting their activities and realizing the economic potential of the nation.**

The paper addresses the implications of information and communication technologies (ICTs) in the organization, coordination, and perpetration of violent unrest. With global trends in ICT developments and the digital population of the world in mind, it analyses their significance in certain phases of unrest.

The results and conclusions stated in the article are reached based on philosophical and ideological, general scientific and special scientific methods and approaches of research: dialectical, formal-logical (analysis and synthesis, induction, and deduction), synchronous comparative legal method and others.

An examination of the use of ICTs during a violent riot emphasizes the following variations of their utilization: a) informational interaction, communication, incitement; b) mobilization of crowd; c) organization of riots; d) allocation of roles; e) coordination.

As of today, an imminently significant challenge arises out from the criminal liability of internet service providers. The dissemination of information on the Internet involves, in addition to the author himself, other entities, in particular the owner of the network information resource, the owner of the server, etc.

Accordingly, the liability of ISPs for failure to restrict access to information containing advocacy, incitement, recruitment or other involvement in the commission of acts of mass unrest on the part of Internet users arises only if they are aware of the social danger of not restricting access to such information, anticipate the dangerous consequences of mass unrest as a direct consequence of such failure and, in so doing, knowingly direct their intellectual and physical efforts towards it.

Keywords—information and communication technologies, riots, organization of riots, incitement to riot, intermediary liability, internet service providers, mob assembly.

I. INTRODUCTION

Security is essential in all aspects of everyday life: technical, biological, political, economic, social, territorial, and so on. It is critical not only to accurately describe this idea, concept, and its derivatives, but also to appropriately use them for their intended purpose.

From this perspective, the state of security can be defined as the defense capability from internal and external threats targeted at national interests, i.e. ensuring the rights and legal interests of individuals, society, the state, and the sustainable development of urban and human settlements.

All communication networks, databases, and information sources have so far been integrated to form cyberspace [1].

Under the context of cybersecurity, it is feasible to identify both the vulnerability posed by this new place/space and the behaviors or processes aimed to make it (more) safe [1]. It is a combination of actions and methods, both technological and non-technical, aimed at safeguarding the bioelectrical environment and the data it stores and conveys from all potential dangers [1]. This very desirable outcome has yet to be realized.

This paper reveals precisely the non-technical measures of cyber security.

Delinquency, crime are de facto objective phenomena in the course of which human behavior unfolds in the spatial and temporal aspects of the interaction of the individual (motor and mental activity) with the environment. It affects the combination of subjective and objective factors (phenomena and processes) of that reality [2]. The offender, the victim of a crime (the object of assault); the circumstances of its commission; as well as the real-life situation of a crime comprise a crime mechanism, the essence of which is expressed in the functional-activity qualities of the system of these elements and the regularity of their interaction [2].

Often criminals exploit objects and realities in the course of their criminal acts. Rationale behind this may be the desire of the offender to simplify the commission of the crime, or rather to gain a mechanical/machine advantage in the commission of the crime.

II. THE INFORMATION SOCIETY

The information society is an environment that generates publicly available information and/or knowledge that individuals can use and/or share with the aim of pursuing their own sustainable enhancement potential to improve their standard of living within legal limits.

There are several definitions of the information society in the specialist literature, based on its key features. The most important three of them will be given here.

Y. Masuda, a Japanese sociologist, who is credited as one of the founders of the concept in question, argues that in the information society the central function will be digital values, while material values will remain in the periphery [3]. The fundamental nature of the infrastructure of "computopia", as he called the information society, applies to the main source of information production. Information utility illustrates the predominance of knowledge capital over material capitals [3].

On the contrary, D. Bell, the American sociologist referred to the information society as the "post-industrial society". He described theoretical knowledge as its fundamental nucleus. The codification of theoretical knowledge, he argued, was a source of innovation and social change [4].

An alternative approach was adopted by F. Webster, who defined the information society by classifying it into groups: the technological aspect; the economic aspect; the work-related aspect; the spatial aspect; and the cultural aspect.

The scale of technological innovation is considered an indicator of the formation of the information society, which should lead to social transformation because of the significant impact on society [5].

The economic dimension represents the intensification of the value of information activity in the economy. A positive index in the gross national product of the information business will determine the logical conclusion of the achievement of the information economy [5]. In the employment-related parameter, the information society indicator is the predominant number of people working in the information field. The emergence of white-collar workers to replace manual work, the growth of employment in the service sector and the decline in production are clear evidence of this [5]. In the spatial criterion, the fundamental emphasis is on information networks, and they can subsequently influence the organization of time and space. Tools functioning on the national, transnational, and global level, equipping the "ring of information highway" in the presence of appropriate techniques allows us to imagine a "conductive society" [5].

Television, radio stations, cinematography, books, magazines, posters, billboards, shop window signs, personal computers, audio accessories, Internet access and hand-held computers demonstrate the uninterrupted spread of this field, which allows us to speak of information in a cultural dimension. At the same time, these factors can be considered as tools of the information society. The presented points to the media-loaded society in which we live, and the new media all surrounds us [5]. Throughout the Age of Enlightenment, the public sphere was linked to the development of bourgeois literature. While by the twentieth century the media had taken the place of bourgeois literature [6]. In the 21st century, the autonomous citizenry was conceived as the ideal of an enlightened citizen, digitally networked and discussing issues of collective interest [7]. It can be assumed that the traditional public sphere tends to move to the Internet, evidence of which is the plurality and opposition of the digital arena to the "central public sphere" dominated by state, corporate and establishment power. This inclination towards an alternative public sphere can be explained by the open and free communicative nature of the digital public sphere, which is represented or supported online from websites to social networking sites, weblogs, and microblogs [8].

III. The Public Legal Sphere (Digital Population)

Staying inseparable from the public sphere since its early conceptualization, the media play a central role in public debates, both in more traditional forms and in new forms enhanced by digital technologies. The transformation of the media paradigm introduces clear changes both in media practices and in the role of citizens/consumers/producers. New media, in particular the Internet, pose new theoretical, methodological, and practical challenges to the shaping of the digital public sphere. Traditional spaces dedicated to public debate are confronted with different forms of socialization, with networked organizations and new channels of information dissemination and exchange that actualize "old" issues in terms of power, control, and citizen participation in public life [9].

The theoretical literature defines 'herding instinct' as referring to situations where people with private, incomplete information consistently make public decisions. Consequently, the first few decision-makers disclose their information and subsequent decision-makers may follow a set pattern, even if their private information suggests that they should deviate from it [10]. This 'information cascade' can occur in perfectly rational people when the information implied by early decisions outweighs the private information of any individual. Anderson and Holt conducted a laboratory study in 1997 in which they calculated the possibility of one person's signals and predictions influencing the decisions of another [11]. An information cascade is a sequence of decisions in which individuals optimally ignore their own preferences and mimic the choices of others ahead of them [12, 13].

The evolution of social media platforms such as Twitter, Facebook, WhatsApp has changed the information cascade process. Due to easy accessibility, especially via smartphones, a large number of people have joined these social media platforms. Moreover, these platforms have become the main source of information dissemination or cascade. Important news about disasters, riots, epidemics, political issues are often spread through these platforms and thus, within a short time, specific information reaches a large number of people.

Accessibility, operational security of information telecommunication networks and systems is crucial to the sustainable improvement of standards of living, working, business organization and civil society. The objects of digital legal relations under law include information in the form of digital data and information objects with digital data (information and communication technologies) [14].

Figure 1 illustrates that the development of ICT, especially mobile phones, has been more dynamic and faster than the introduction of other communication technologies. There has been a rapid preference for mobile networks and devices as the primary means of communication, including access to the World Wide Web. Today, mobile networks cover almost 95% of the planet. Meanwhile, mobile broadband networks with higher quality Internet connectivity cover about 80%.

Mobile networks now cover more than 95% of the Earth's land area, and mobile broadband networks, which provide much better Internet connectivity, cover about 94% [15]. By the end of 2022, more than half of the world's population (65%) was using the Internet, with the proportion of young people (aged 15-24) increasing to more than 75% (Internet users in 2005-2022 shown in Figure 2) [15]. The global progressive trend in ICT diffusion and growth of Internet users allows us to speak of a digital population of planet Earth and/or individual countries.

Today's realities involve both positive and negative aspects of the use of ICTs. On the negative side, there is an increasing trend of crimes involving the use of such tools. Their use is increasingly popular with terrorist, organized crime, and extremist groups as a means to influence government policy and/or decisions.

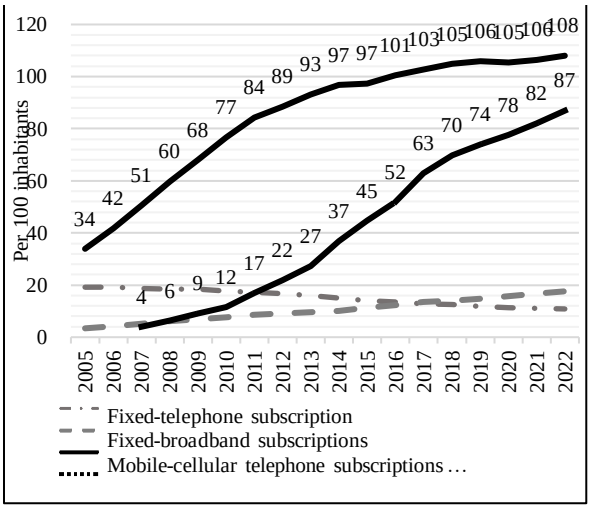

Fig. 1. Global trends in ICTs in 2005–2022 (Per 100 inhabitants)

Source: Measuring digital development Facts and Figures 2022. United Nations International Telecommunication Union (ITU)

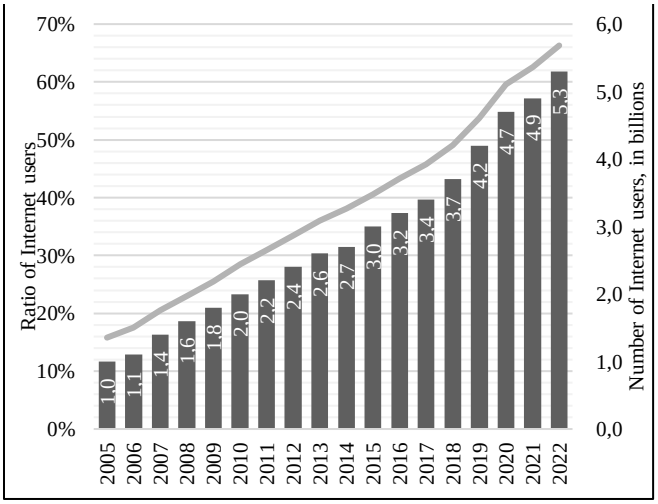

Fig. 2. Individuals using the Internet in 2005–2022 (%)

Source: Measuring digital development Facts and Figures 2022. United Nations International Telecommunication Union (ITU)

IV. The Criminal Utilization Of The Attributes Of The Information Society (ICTs): Riots

The events of the last decade in various countries around the world demonstrate the high efficiency of the impact of information and communication technologies on the consciousness of the general public in order to aggravate mass disturbances. The events of the "Arab Spring", the "colour revolutions" (e.g. in former Eastern Bloc countries), the riots in Minneapolis with subsequent spread to other US cities, etc., are illustrative in this regard. Among other things, one should also note the tactical methods used by the non-systemic opposition in a number of countries, in which public calls for "peaceful" rallies are posted online, with the initial intention to inflame and aggravate the situation.

In assessing the perspectives for exploiting ICTs during a riot, the following areas of use can be identified:

a) Information interaction, communication, appeals;

b) Mobilising people (rioters);

c) Organising the riots;

d) Allocation of roles;

e) Coordination in confrontation with law enforcement agencies;

f) Coordination in achieving the final objective.

When public discontent with certain social problems arises, ICTs facilitate the exchange of information, communication and even calls for specific (not always legal) actions.

A wide range of circumstances can serve as catalysts for social unrest. For example, inappropriate or otherwise lawful police action; unemployment; poor housing conditions; inadequate education; inadequate recreation facilities and programs; ineffective political power structures and recourse/appeal mechanisms; discrimination against people of another race; unfair administration of justice; inadequate federal programs; unacceptable municipal services; and low levels of social protection [16].

Traditional media often do not capture the essence of citizens' collective activism. Moreover, the respective structures restrict access to some websites and communication resources [17]. As an alternative, ICT provides an opportunity to overcome such media structures, ensuring the dissemination of information without 'filters' and censorship.

Mass mobilizations can take hours, days, weeks to months and involve large numbers of citizens. A popular mobilization mechanism involves individuals becoming involved in collective wrongdoing [17, 18, 19,]. In addition to the latter, both social movements and informal structures (such as activist associations) may be involved. At the same time, mass mobilization has a certain impact on public opinion through the concentration of attention and the involvement of the population [20]. A characteristic feature of this phenomenon is its disruptive component.

ICTs reduce the cost of publicizing necessary information about social movements in a short period of time, thereby increasing the number of active participants [21]. There is no doubt that these properties of ICT contribute to the organization of mass disturbances [22]. Decentralized, non-hierarchical organizational structures can be modelled using these technologies.

With the use of ICT tools, organizers can outline tactical plans for determining the form of implementation of collective action and the allocation of roles to participants in a mobilized crowd. The allocation of functional roles among the participants in a crowd takes place at the stage of preparation for the commission and/or implementation of acts of mass disorder as part of the criminal intent. Moreover, this may be accompanied by conditional discipline, active organizing activities, and an elaborate (if necessary) system of supplying the means and implements for the commission of the crime.

In order to ensure public order and public security at all public events, regardless of whether they are authorized or unauthorized, they are usually accompanied by representatives of law enforcement agencies. There is a high risk of confrontation between participants in unauthorized

assemblies and law enforcement officials. Depending on the objectives of such actions, the organizers may follow several scenarios:

a) They are not interested in a violent confrontation with representatives of law enforcement agencies and therefore urge participants in an unsanctioned assembly to stop it immediately on the first request of the police;

b) They a priori aim to escalate the confrontation and by their provocative actions (appeals, orders, etc.) promote an early and violent confrontation with the forces of law and order;

c) They choose not to comply with the legitimate demands of the authorities and proceed "on the spot" to coordinate the actions of the crowd against the forces of law and order.

ICTs can be used to transmit alerts in all of the above cases: of impending National Guard units, police (riot control units); of coordination within 'small groups'; and of command for further mass violent action.

In a mobilized crowd, participants need to be aware of specific plans for unlawful activity, as a lack of coordination among participants can reduce the effectiveness of the action as a whole. The dissemination of such plans can also be accomplished through the use of ICTs.

When assessing the possible impact of ICT use on the course of a mass riot, it is necessary to identify the perpetrators to be held criminally liable. ICTs and associated devices appear to function effectively as tools and instruments of crime. At the very least, incitement, organization and instigation to mass disorder do not seem possible in the current circumstances without the use of ICTs.

A topical issue today is the criminal liability of Internet service providers. The fact is that in the process of dissemination of information on the network, along with the author himself, other entities are involved, in particular, the owner of the network information resource, the owner of the server, etc. [23]. In other words, this process involves, in parallel, entities providing communication services, in particular, operations of receiving, processing, storage, transmission, delivery of telecommunications, etc. These are usually legal entities or self-employed individuals (entrepreneurship & self-employment) providing the above services on the basis of a proper license obtained.

Among ISPs, access providers, hosting providers, caching providers, backbone providers and last-mile providers can be distinguished. In defining legal responsibilities, ISPs should be differentiated according to the functions they perform [24], which are described below.

The functions of access providers include providing access to third-party content by moving, routing data without permanently storing it [25]. For example, through such a provider a user connects to the Internet or an information system from his location to the underlying network of the Internet [25]. Hosting providers store, make available, third-party content both on their own and on a rented technical base (server) [25, 26]. As a consequence, content is permanently online. Most often, users are given direct access to upload content to the network, bypassing the mechanism of manual control by the hosting provider [25].

The mechanism of automatic temporary storage and transfer of data, in order to optimise the technological process of information transfer, is carried out by the caching service provider [27, 28]. Being a technological process, caching in order to reduce the intensity of the flow, accelerate the loading of Web sites and improve the transfer of information provides intermediate storage in the server cache memory [27].

The provision of data and communication services is usually provided by the transport telecommunications infrastructure. Backbone providers lay data links, namely connecting strategic parts of the Internet to backbone lines [29, 30].

The communication line directly from the backbone networks to the user/consumer is laid by last mile providers [31, 32, 33].

The right to freedom of expression is clearly applicable to all citizens, provided that they follow the established rules for the organization and conduct of events, meetings, protests, marches or pickets [34]. However, when there is a conflict between the right to freedom of expression and association and the need to maintain public order and safety, it is crucial to strike a balance. In a democratic state governed by the rule of law, a citizen has the right to freedom of expression and association [34]. Equally important is the security of civilians, who face imminent risks due to potential escalation in the exercise of these rights.

In this context, bans on the dissemination of information aimed at propaganda for war, inciting national, racial, or religious hatred and enmity, as well as other information for the dissemination of which criminal liability is prescribed, are justified [35, 36].

The owner (moderators) of websites, pages on the Internet and/or information system and/or software for electronic data processing shall be guided by the established regulations when disseminating information on social networks in order to attract persons to participate in the mass disorder. That is, they must not allow their resources to be used to commit crimes or to disseminate information that promotes a cult of violence and cruelty.

Channel-specific policies for information systems and programs that enable end-to-end encryption for the transmission and reception of messages are also important. Cryptographic algorithms in such ICT tools are designed to be encrypted in such a way that messages sent and received are intended for two parties only, excluding third parties, including state agencies, from receiving the information [37, 38]. Such systems and programs include Telegram, SafeSMS, None of your business (NOYB), FlyByNight, Pretty Good Privacy (PGP), Off-the-record (OTR), Signal, etc. Obviously, riot masterminds can take advantage of such technologies.

This raises two questions: the possibility of blocking specific individuals using ICT for illegal purposes by these networks, and the permissibility of the state authorities monitoring the communications of citizens with the help of such technologies. On the first issue, there are already known examples of the blocking of the accounts of the 45th President of the United States, Donald Trump, as well as other accounts relaying his messages. However, there are many accounts that incite, urge, recruit and engage people in violent acts without being detected or blocked. Regarding the second question, it seems that monitoring and surveillance of correspondence is permissible in cases of threats to the security of individuals, society and the state.

V. Liability Of ICTS

When qualifying acts of incitement, inducement, recruitment, or other involvement of a person in the commission of acts of mass disorder on the Internet, it is necessary to unambiguously clarify the function performed by each particular person (Internet service providers) in committing the crime. The existence of guilt and, accordingly, the incidence of criminal responsibility for these acts depends on the cognitive elements in a person's psyche, i.e. the intellectual (the ability to understand the wrongfulness of his behavior, foresee consequences) and the orientation of mental and physical efforts to make a decision, i.e. the volitional (the desire for these consequences to occur) elements of guilt [31].

On this issue, we must agree with the position of researchers who argue that ISPs providing technological support in the communications of subjects, i.e. providing only technical support/connecting network access, should not be criminally liable [24]. The criminal liability of ISPs arises if they have the organizational and technical capacity to influence the informational social relations of their users at any time.

Access providers, caching service providers, backbone providers and last-mile providers are therefore not liable because their activities consist only of technological support for the connection of users to the network [24]. In the case of a hosting provider there is a special approach to liability depending on the specific functions performed. If the hosting provider only provides disk space for the physical hosting of information permanently on the network, no liability should be imposed on it. However, if the competent authorities are notified of the illegal content of the uploaded information, and if it is technically possible to restrict access to such information, the hosting provider should be liable for not fulfilling his obligation to restrict access to such information [24].

In view of the above, it may be argued that the liability of Internet service providers for failure to take measures to restrict Internet users' access to information containing appeals, incitement, recruitment or other involvement of persons in the commission of acts of mass unrest arises only if they are aware of the social danger of not restricting access to such information, anticipate dangerous consequences in the form of mass unrest which are a direct consequence of such failure, and in doing so consciously fail to take action.

The guilt of the provider is based on an assessment of the factual circumstances of a particular case, the presence or absence of a mental attitude in the person's actions towards the omission (not restricting access to the information in question) which subsequently contributed to the mass disorder.

Conclusion

To summarize the above, the following conclusions are relevant in relation to the exploitation of information and communication technologies as a high-tech means of committing riots:

(1) Attributes of the information society, being ancillary and peripheral factors, are not a direct determinant of riots. Stepping aside from the techno-determinist model, the views of Professor C. Fuchs are convincing, because the triggers of conflict atmosphere in society are exclusively social relations (problems).

2. The use of information and communications technologies by organizers and instigators enables them to be included among the sources of threats in the event of social unrest. Potentially dangerous areas of illicit use of ICTs can be distinguished as follows:

a) Information interaction, communication, appeals;

b) Mobilising people (rioters);

c) Organising mass unrest;

d) Role allocation;

e) Coordination in confrontation with law enforcement agencies;

f) Coordination in achieving the final objective.

3. The criminal liability of ISPs for failing to take measures to restrict Internet users' access to information containing appeals, incitement, recruitment, or other involvement of persons in the commission of acts of riots shall only occur where they are aware of the social danger of not restricting access to such information, foresee dangerous consequences in the form of mass disorder that are a direct result of such restrictions and yet consciously fail to act.

References

[1] Collins, A. (Ed.). (2016). Contemporary security studies. Fourth edition. Oxford university press. P. 401

[2] Ignatov, A. N. O kategoriyax «mexanizm prestupnogo povedeniya», «mexanizm prestupleniya» i «mexanizm sovershеniya prestupleniya» // Gumanitarny`e, social`no-e`konomicheskie i obshhestvenny`e nauki. № 6–7. 2017. S. 126–132. (Игнатов, А. Н. О категориях «механизм преступного поведения», «механизм преступления» и «механизм совершения преступления» // Гуманитарные, социально-экономические и общественные науки. № 6–7. 2017. С. 126–132.)

[3] Masuda Y., The Information Society as Post-industrial Society, World Future Society, 1981, p. 147

[4] Bell D. The Coming of the Post-Industrial Society // The Educational Forum, (1976) No 40:4, p. 576

[5] Webster F., Theories of the information society, Third edition, Routledge, London, 2006, p. 9-19

[6] Translated by Thomas Burger, Habermas, J., The structural transformation of the public sphere, MA: MIT Press, Cambridge, 1989, pp. 328

[7] Iosifidis P., Wheeler M. The public sphere and network democracy: Social movements and political change? // Global Media Journal, 13 (25), 2015. pp. 1–17

[8] Schäfer M.S., Digital Public Sphere // In The International Encyclopedia of Political Communication, G. Mazzoleni (Ed.). (2015). London: Wiley Blackwell. p. 322

[9] Sousa H., Pinto M., Silva E. C. e. Digital public sphere: weaknesses and challenges // Comunicação E Sociedade, 2013, vol. 23, p. 9

[10] Anderson L, Holt C.A., Information cascade experiments. In: Durlauf S.N., Blume L.E. (eds) Behavioural and Experimental Economics. The New Palgrave Economics Collection. Palgrave Macmillan, London. 2010. pp. 166-167

[11] Anderson L, Holt C.A., Information Cascades in the Laboratory // The American Economic Review, American Economic Association, Dec., 1997, Vol. 87, No. 5, pp. 847- 862

[12] De Vany A., Lee C., Information Cascades in Multi-Agent Models. Papers 99-00-05, California Irvine - School of Social Sciences. 1999, p. 2

[13] Bikhchandani S., Hirshleifer D., Welch I. Information Cascades. In: Palgrave Macmillan (eds) The New Palgrave Dictionary of Economics. Palgrave Macmillan, London. 2008, p. 1.

[14] Blazheev V. V. Cifrovoe pravo: uchebnik / pod obshh. red. V. V. Blazheeva, M. A. Egorovoj. Moskva: Prospekt, 2020. S. 71 (Блажеев В. В. Цифровое право: учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. Москва: Проспект, 2020. С. 71.)

[15] Measuring digital development Facts and Figures 2022. United Nations International Telecommunication Union (ITU), Development Sector. 2022. Official text [Electronic resource]. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (Access date: 14.02.2023).

[16] United States. National Advisory Commission on Civil Disorders, & United States. Kerner Commission. Report of the national advisory commission on civil disorders. pp. 8–20.

[17] Mancini F., O'Reilly M. New Technology and the Prevention of Violence and Conflict. Stability: International Journal of Security & Development. Volume 2. Issue 3. Art. 55. 2013. P. 3. URL: https://ssrn.com/abstract=2902494 (22.02.2022)

[18] Smith, L. G., Blackwood, L., & Thomas, E. F. The need to refocus on the group as the site of radicalization. Perspectives on psychological science, 2020. 15(2), P. 335 DOI: https://doi.org/10.1177/1745691619885870

[19] Mancini F., O'Reilly M. New Technology and the Prevention of Violence and Conflict. Stability: International Journal of Security & Development. Volume 2. Issue 3. Art. 55. 2013. P. 3.

[20] Della Porta, D., Diani, M. Social movements: An introduction. Third edition. John Wiley & Sons. 2020. pp. 21–22.

[21] Shultziner D., Goldberg S. The stages of mass mobilization: separate phenomena and distinct causal mechanisms. Journal for the theory of social behaviour. Volume 49, Issue 1. 2019. P. 12. DOI: https://doi.org/10.1111/jtsb.12187.

[22] Leizerov S. Privacy Advocacy Groups Versus Intel: A Case Study of How Social Movements Are Tactically Using the Internet to Fight Corporations. Social Science Computer Review. Volume 18, Issue 4. 2000. pp. 464–465.

[23] Duncan F. Collective Action and Digital information Communication Technologies: The Search for Explanatory Models of Social Movement Organizations' Propensity to Use Dicts in Developed Democracies. Publicly Accessible Penn Dissertations. 2015. 1048. P. 90. (Order No. 3709451). Available from ProQuest Dissertations & Theses Global. (1699101824). URL: https://www.proquest.com/dissertations-theses/collective-action-digital-information/docview/1699101824/se-2?accountid=30408 (23.02.2022).

[24] Rassolov I.M. Pravovy`e problemy` obespecheniya informacionnoj bezopasnosti: yuridicheskaya otvetstvennost` operatorov svyazi. Vestnik Moskovskogo universiteta MVD Rossii. 2013. №12. S. 103. (Рассолов И.М. Правовые проблемы обеспечения информационной безопасности: юридическая ответственность операторов связи. Вестник Московского университета МВД России. 2013. №12. С. 103.)

[25] Perchatkina S. A., Cheremisinova M. E., Cirin A. M., Cirina M. A., Czomartova F. V.. Social`ny`e internet-seti: pravovy`e aspekty`. Zhurnal rossijskogo prava. 2012. №5 (185). S. 20. (Перчаткина С. А., Черемисинова М. Е., Цирин А. М., Цирина М. А., Цомартова Ф. В.. Социальные интернет-сети: правовые аспекты. Журнал российского права. 2012. №5 (185). С. 20.)

[26] Zharova A. K. O neobxodimosti pravovoj klassifikacii operatorov seti Internet // Biznes-informatika. 2011. №3 (17). S. 63. (Жарова А. К. О необходимости правовой классификации операторов сети Интернет // Бизнес-информатика. 2011. №3 (17). С. 63.)

[27] Weber, R. H. Internet Service Provider Liability: The Swiss Perspective. Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 1, 2010. P. 148.

[28] Chubukova S.G. Problemy` pravovogo statusa informacionnogo posrednika. Vestnik akademii prava i upravleniya. 2017. № 2 (47). S. 41 (Чубукова С.Г. Проблемы правового статуса информационного посредника. Вестник академии права и управления. 2017. № 2 (47). С. 41)

[29] Pfender, J., Valera, A., & Seah, W. K. Reassessing caching performance in information-centric IoT. Internet of Things, 100479. 2022. P.1 DOI: https://doi.org/10.1016/j.iot.2021.100479.

[30] Ozhiganova E. M. Primenenie sistemy` motivacii vremenny`x sotrudnikov na primere AO «E`R-Telekom xolding» // Biznes-obrazovanie v e`konomike znanij. 2016. №1 (3). S. 44. (Ожиганова Е. М. Применение системы мотивации временных сотрудников на примере АО «ЭР-Телеком холдинг» // Бизнес-образование в экономике знаний. 2016. №1 (3). С. 44.)

[31] Mayr, C., Risso, C., & Grampín, E. Crafting optimal and resilient iBGP-IP/MPLS overlays for transit backbone networks. Optical Switching and Networking, 42, 100635. 2021. P. 2 DOI: https://doi.org/10.1016/j.osn.2021.100635.

[32] Cirina M. A. Rasprostranenie pronarkoticheskoj informacii v Internete: mery` protivodejstviya // Zhurnal rossijskogo prava. 2012. №4 (184). S. 48. (Цирина М. А. Распространение пронаркотической информации в Интернете: меры противодействия // Журнал российского права. 2012. №4 (184). С. 48)

[33] Gevaers, R., Van de Voorde, E., & Vanelslander, T. Cost modelling and simulation of last-mile characteristics in an innovative B2C supply chain environment with implications on urban areas and cities. Procedia-Social and Behavioral Sciences. 2014. 125, P. 400. DOI: https://doi.org/10.1016/j.sbspro.2014.01.1483

[34] Boysen, N., Fedtke, S., & Schwerdfeger, S. Last-mile delivery concepts: a survey from an operational research perspective. Or Spectrum. 2021. 43(1), P. 4. DOI: https://doi.org/10.1007/s00291-020-00607-8.

[35] Pukovodyashhie principy` po svobode mirny`x sobranij, Izdanie 2-e. BDIPCh OBSE. 2011. 192 C. URL: https://www.osce.org/odihr/73405 (data obrashheniya: 25.11.2021). (Руководящие принципы по свободе мирных собраний, Издание 2-е. БДИПЧ ОБСЕ. 2011. 192 С. URL: https://www.osce.org/odihr/73405 (дата обращения: 25.11.2021).)

[36] United Nations. (2020). United Nations Strategy and Plan of Action on Hate Speech–Detailed Guidance on Implementation for United Nations Field Presences. URL: https://www.un.org/en/genocideprevention/hate-speech-strategy.shtml (дата обращения: 14.12.2021).

[37] Grambo, K. Fake news and racial, ethnic, and religious minorities: A precarious quest for truth. U. Pa. J. Const. L., 21. 2018. P. 1304.

[38] Schillinger F., Schindelhauer C. End-to-End Encryption Schemes for Online Social Networks // Security, Privacy, and Anonymity in Computation, Communication, and Storage 12th International Conference, SpaCCS 2019 Atlanta, GA, USA, July 14–17, 2019 Proceedings. Springer Nature Switzerland AG 2019. P. 138.

[39] Ullah, S., & Zahilah, R. Curve25519 based lightweight end-to-end encryption in resource constrained autonomous 8-bit IoT devices. Cybersecurity. 2021. 4(1), 1-13. P. 1