INTRODUCTION
Criminal justice measures aimed at maintaining public security and order are essential to the functioning and progress of society and the state. The civil unrest represents a serious national security threat. The probable consequences are not confined to the main field of exposure. There are so-called wave effects such as: threats to the lives and/or health of citizens; threats of property damages; threats of mass disruption of public order and/or safety; threats of tampering or dysfunction of infrastructure, transportation or social services, businesses, energy facilities, industry and/or telecommunications networks.

Democracy coexists alongside public activism. International and regional human rights treaties provide protection for the freedoms of peaceful assembly and association. For instance, the Universal Declaration of Human Rights (art. 20(1)), International Covenant on Civil and Political Rights (art. 21 and 22), African Charter on Human and Peoples’ Rights (art. 10 and 11), the American Convention on Human Rights (art. 15 and 16) and the European Union Charter of Fundamental Rights (art. 12).

These rights can be carried out in a various way, whether it be individual pickets, rallies, demonstrations, marches, sit-ins, flashmobs, or protests. (ODIHR, 2011, pp. 11-12). Exercising these rights creates a possibility of escalation. Such gatherings are not always deemed to be civil unrest. Indeed, as long as they occur within the framework of the relevant rules, they can be regarded as mass civil obedience. It is then vital to make a clear distinction between the exercise of civil rights and their excesses. Civil unrest is a powerful form of collective dynamics which has led (and is still able to lead) to major societal changes in modern history. (BRAHA, 2012, p. 1).

RESEARCH QUESTION
It is clear through the study of actus reus of riots that, in contemporary conditions, it is almost inconceivable to incite such violent offense without means of information and communication technologies (ICTs). This, in turn, leads to the question of whether Internet service providers (ISP) are liable under criminal law. Since the dissemination of information on the network involves other parties alongside the author himself. In particular, the owner of the network information resource, the server holder, etc....

ESTABLISHMENT OF CRIMINAL LIABILITY FOR RIOTS IN THE US
In the 1960s, many major cities in the United States, including Los Angeles, Chicago and Newark, experienced racial riots. The 1967 riots resulted in at least 84 fatalities and $75 million to $100 million in damages. (FLANAGAN, 2021). In Detroit alone, 43 deaths, more than 7,000 arrests and almost 1,400 burning buildings have been reported. (FLANAGAN, 2021).

Pursuant to US President Lyndon B. Johnson’s Executive Order 11365, was established the National Advisory Commission on Civil Disorders on 29 July 1967. (GRAHAM, 1980, p. 17). Its chairperson was appointed Otto Kerner, Jr., former governor of Illinois, henceforth the commission would also be referred as the Kerner Commission. While investigating the determinants of riots, the commission was tasked with answering three main questions: “What happened? Why did it happen? What could be done to prevent it from happening again?” (HUGHEY, 2018, p. 619). Notwithstanding President Johnson’s suspicions, the Commission did not detect any evidence of political conspiracy among the city’s colored, militant illegal armed groups against him, which is reflected in the final report, published on 1 March 1968.

The main outcome was as follows: “Our nation is moving toward two societies, one black, one white – separate and unequal”. (US KERNER COMMISSION et al. Report, 1968, p. 1) Both economic deprivation and racial discrimination triggered intense anger in the ghetto areas and caused a climate liable to rioting. The riots were considered as political protests by
outraged people of color from the ghettos. Consequently, President Johnson overturned the Commission’s specific recommendations and some of its findings.

Riots became a serious political issue which prompted a debate in the 1968 session of the US Congress. Conservative senators Lausche - Thurmond proposed anti-riot measures in the form of amendments to the 1968 Civil Rights Act. During the Senate’s consideration of the bill on 5 March 1968, the US Department of Justice had sent to Congress a bill proposed by the president's administration. However, the reticent suggestions of the administration were ignored to a great extent by the Congress, and the Lausche - Thurmond amendment was passed on April 11, 1968, just seven days after the assassination of Martin Luther King, Jr (murdered on April 4, 1968), who had advocated the protection of civil rights through non-violence and civil disobedience. (STALMACK, 1973, p. 593). Afterwards, a chain of the most devastating riots of that decade followed in April and May. Expectedly, amidst those social unrest and legislative compromise between two diametrically opposed approaches, the bill was ultimately far from perfect. It was not only misdrafted, but many would also argue that it was simply redundant: the existing federal and state laws at the time allowed for effective management of civil unrest.

At the federal level, there are a number of provisions to establish criminal liability in the event of riots: United States Code § 231-233 (civil disorders) and § 2101-2102 (riots).

Riots (§ 2101-2102) covers practically the acts making the disturbances possible. For instance, § 2101 criminalizes travels in interstate or foreign commerce or use any facility of interstate or foreign commerce, including, but not limited to, the mail, telegraph, telephone, radio, or television, with intent:

- to incite a riot; or
- to organize, promote, encourage, participate in, or carry on a riot; or
- to commit any act of violence in furtherance of a riot; or
- to aid or abet any person in inciting or participating in or carrying on a riot or committing any act of violence in furtherance of a riot; and
- who either during the course of any such travel or use or thereafter performs or attempts to perform any other overt act for any purpose specified in subparagraph (A), (B), (C), or (D) of this paragraph.

18 U.S. Code § 2102. (a) defines concept of riot as a public disturbance involving:

1. an act (acts) of violence
   - by one (more) persons part of an assemblage of three or more persons,
   - which act or acts shall constitute a clear and present danger of, or
   - shall result in, damage or injury to the property of any other person or to the person of any other individual or

2. a threat (threats) of the commission of an act (acts) of violence
   - by one (more) persons part of an assemblage of three or more persons
   - having, individually or collectively, the ability of immediate execution of such threat or threats,
   - where the performance of the threatened act or acts of violence would constitute a clear and present danger of, or
   - would result in, damage or injury to the property of any other person or to the person of any other individual.

18 U.S. Code § 2102. (a) defines concept of incitement to riot or terms “to organize, promote, encourage, participate in, or carry on a riot” as a public disturbance involving:


- includes, but is not limited to, urging or instigating other persons to riot,
- but shall not be deemed to mean the mere oral or written (1) advocacy of ideas or (2) expression of belief, not involving advocacy of any act or acts of violence or assertion of the right of, or the right to commit, any such act or acts.

Federal anti-riot legislation differs from state statutes in the way that it does not criminalize mere participation in a riot. (SHEB, 2015, p. 362). It punishes acts that contribute to riots, aggravating public danger and assisting future rioters to become proficient in the use of weapons, explosive and incendiary devices, etc.

US Code § 231 (a) (1) makes it a punishable offense to teach or exhibit the use, application or manufacture of any firearm, explosive or incendiary or technical device capable of causing bodily injury or harm to a person. Mens rea includes knowing, having reason to believe, intending that it will be used unlawfully in a riot or to support a riot, whereby the riot could in any way or to any extent obstruct, delay or adversely affect commerce, or the flow of goods or services, or the performance of any federally protected function.

Section 231 (a) (2) of the US Code penalizes the manufacture for the purpose of transporting or conveying in the course of commerce firearms, explosives, or incendiary devices for their unlawful use in furtherance of a riot. In this context, a person knows, has reason to believe or intends that all of these items will be unlawfully used in the course of riot. Since no explicit degree of mens rea has been established, it is assumed that even "reckless" behavior is sufficient to form the subjective element of the crime. (DAVIS, 2014).

Section 231 (a) (3) of the US Code sets out the liability of any person who does or attempts to do any act to obstruct, hinder, interfere with, or influence a firefighter or law enforcement officer who is lawfully carrying out his duties during a public disturbance.

In accordance with Article 232 (“Definitions”) of the US Code, civil disorders are defined as any social unrest involving acts of violence committed by groups of three or more persons which cause damage or injury to another person’s property or person or which involve a risk of immediate harm or injury.

**INCITEMENT TO RIOT (E-INCITEMENT)**

The methods and techniques available to incite someone to commit an offense are wide-ranging. Words, gestures and textual means of communication might be used for this purpose.

Regarding incitement to crime, the precedent of Brandenburg v. State of Ohio also needs to be considered. Clarence Brandenburg, a leader of the far-right racist organization Ku Klux Klan, was convicted of violating Ohio’s Criminal Syndicalism Statute. (EMERSON, 2019, p. 21). Under the act, it was unlawful to "promote, advocate, persuade to commit a crime, sabotage, use violence or terrorist methods as a means of industrial or political reform".

Addressing a KKK rally he stated the following: "We are not a revengent organization, but if our President, our Congress, our Supreme Court continue to suppress the white, Caucasian race, it is possible that there might have to be some revenge taken. We are marching on Congress July the Fourth, four hundred thousand strong". (BRANDENBURG V. OHIO, 1969). Many of those attending were armed with firearms.

The US Supreme Court ruled: “the constitutional guarantees of freedom of speech and of the press do not permit the state to prohibit or limit activities advocating use of force or violation of the law unless such activities (1) are designed to incite or carry out (2) an imminent unlawful act and have (3) a likelihood of inciting or carrying out such an act. (BRANDENBURG V. OHIO, 1969).

The purpose of the instigator is to persuade or induce those who are not under the control of the instigator to commit unlawful acts. In order to avoid vagueness or redundancy, and to meet the requirements of the Brandenburg Standard, the regulation of the content of the speech (wording) of the instigator implies the existence of the elements of criminal intent. (STEINBLATT, 2012, p. 782). For the determination of the instigator’s intent, Professor Clay
Incitement to riot: intermediary liability of ISPs

Calvert (2019, p. 139-143) suggests that the following elements should be established: 1) the meaning of the words used; 2) the instigator’s awareness of the mental state (mood) of the perpetrator(s) and 3) the instigator’s awareness of prior reactions, responses to the words used.

Incitement to crime through the dissemination of information online can be seen in two ways, via “open” social media platforms and channels of information systems and programmes that enable the transmission and reception of messages through end-to-end encryption. Cryptographic algorithms in such ICT tools are based on the principle of encryption so that messages sent and received are intended only for two parties and the receipt of information by third parties, including government agencies, is excluded. (SCHILLINGER; SCHINDELHAUER, 2019, p. 138). Systems and programmes such as Telegram, SafeSMS, None of your business (NOYB), FlyByNight, Pretty Good Privacy (PGP), Off-the-record (OTR) and Signal are some examples. Naturally, the organisers of the disturbances will exploit such technologies.

EXPLOITATION OF INTERNET SERVICE PROVIDERS IN CIVIL DISTURBANCES

Apparently, the events of the last decade in various countries have shown that such technologies can be used to influence the minds of large masses of people and subsequently provoke escalation of unrest. 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 sense. In addition, the tactics used by the non-systemic opposition in a number of countries, when calls for “peaceful” assemblies are posted online, knowingly planned to aggravate the situation, can be highlighted as well. During riots, ICTs can be exploited in a variety of ways:

1. Most importantly, it is informational interaction, communication, urging for action. Individuals express their frustration through ICTs.
2. Subsequently, upon the availability of catalysts for civil disturbances, individuals will mobilize cohesively. Such a process may take hours, days, weeks or even months, and may involve a significant number of citizens.
3. ICT can be exploited by the organizers of disturbances due to their low cost.
4. Given technologies also allows to allocate roles between the participants of public disturbances and to determine plans. Moreover, it helps to be coordinated in confrontations with anti-riot units.

As mentioned above, every dissemination of information online is a particular process. Besides the disseminator him/herself, there are a number of other actors that make dissemination possible. Internet service providers probably appear to be the first respondents in this regard. This raises the question of whether ISPs are criminally liable. As such, it is necessary to establish their types and the functions they perform. ISPs include access providers, hosting providers, caching providers, backbone providers, and last mile providers.

Given that information is usually transmitted through an automated technical process without the involvement of an access provider, it only performs a “transport” function. (WEBER, 2010, p. 147). Hence, it only makes connection of the user to the Internet technically possible.

The host provider offers a storage space on its server to the content provider. (WEBER, 2010, p. 148). Besides, such storage can be either own or rented technical base. Therefore, the content remains available online on a permanent basis. The information is automatically uploaded to the network (manual control is bypassed). (ZHAROVA, 2011, p. 63).

Caching refers to the process of storing websites on local drives to improve the speed and efficiency of accessing information. (GERKE, 2014, p. 284, from NAUMENKO, 1999). Usually, it is done by installing proxy servers. (GERKE, 2014, p. 284, from NAUMENKO, 1999). They enable access to the information stored on the local storage. (GERKE, 2014, p. 284, from NAUMENKO, 1999).
A data and communication services are usually provided by a transport telecommunications infrastructure. Backbones networks are high-capacity, long-distance routes among interconnected networks and primary routers to transmit data packets online. (GREENSTEIN, 2020, pp. 193 - 194).

Last-mile providers deliver Internet to the end user. (INTERNATIONAL TELECOMMUNICATION UNION, 2020). A local loop, central office, and wireless masts can all be involved in this. (INTERNATIONAL TELECOMMUNICATION UNION, 2020). The access network reaches users' devices, usually smart phones, laptops, and other Internet-enabled devices. (INTERNATIONAL TELECOMMUNICATION UNION, 2020).

**FINDINGS**

Understanding each individual's function, as well as the role of the ISPs, are essential for the qualification of incitement to civil disturbances. Criminal culpability will depend on the intellectual and volitional elements of guilt. The first element refers to the cognitive aspects of a person's state of mind. It refers to the person's ability to understand the illegality of his/her behaviour and to foresee the occurrence of certain consequences. The second element indicates the direction of mental and physical efforts to make a decision on committing an act. Here, a person's intention regarding the occurrence of these consequences must be considered.

In light of the facilitative nature of ISPs, it is worth taking a brief look at the models of intermediary liability. There are three models to consider: “blanket” or strict liability; “safe harbour” or conditional liability; and broad immunity. (MACKINNON et al., 2015, p. 40).

“Blanket” or strict liability imposes criminal liability for the non-guilty causation of damage. In this model, the ISP is held liable even if it did not anticipate or know that the information disseminated by a third party (the user) was illegal. (MACKINNON et al., 2015, p. 40). It is believed that the only way to avoid liability is to monitor, filter and remove content that is “possibly” illegal. (MACKINNON et al., 2015, p. 40).

The "safe harbour" or conditional liability approach ensures that the provider is exempt from liability for third-party content as long as certain prerequisites are met. (MACKINNON et al., 2015, p. 40). Such conditions may include the removal or restriction of access to potentially unlawful information. It does not presume monitoring by the provider, instead it requires notification by the competent structures in order to remove such information.

Broad immunity represents the provider's exemption from liability for third-party content, regardless of the function they perform or the type of content. (MACKINNON et al., 2015, p. 42).

The Safe Harbor or conditional liability and broad immunity models are applicable in the US. (MACKINNON et al., 2015, p. 50). The first model is stipulated in the Digital Millennium Copyright Act, which is essentially irrelevant to our study. The second model is envisaged in section 230 of the Communications Decency Act (CDA). Stepping aside slightly, it may be noted that there are cases where courts have dismissed claims against social media service providers in cases where they have not restricted material that incites terrorism precisely on the grounds of the mentioned provision. (BERRYMAN, 2020, p. 1338). Furthermore, courts have dismissed such cases due to the lack of a proximate cause between the ISPs' behaviour and the ensuing dangerous consequences. (BERRYMAN, 2020, p. 1338).

**CONCLUSION**

Author of this paper agrees with the views of scholars such as S.A. Perchatkina, M.E. et al., (2012, p. 20) and M.A. Tsirina (2012, p. 49). They suggest considering as criminally liable ISPs, which have organizational and technical capacity to influence information social relations of their users at any time. (TSIRINA, 2012, p. 49). Accordingly, in the absence of such an opportunity, i.e. in cases where providers provide only technical support/connection of access to the network, they are not subject to criminal liability.
In the light of the foregoing, access providers, caching service providers, backbone providers and last mile providers are not liable for prosecution. Because their activity is merely a technological support of the connection of users to the network. (PERCHATKINA et al., 2012, p. 20), (TSIRINA, 2012, p. 49). The same can be applied to a hosting provider which only provides disk space for the physical location of information which is permanently online. The latter are liable only if they refuse or simply do not restrict access to the data when it is technically possible. Obviously, in the second case, it is necessary a notification from the competent authorities. As a result, they are aware of the danger of not restricting access to such information, foresee harmful consequences such as riots as a direct consequence of not restricting access, and consciously direct their mental and physical efforts to do so.

Lately, there has been raised concerns among scholars regarding amendments to the Communications Decency Act (CDA) by the US Congress, either repealing the shield of protection for certain cases or at least clarifying that intermediary liability of ISPs in dangerous acts. (TSESIS, 2017, p. 624), (BERRYMAN, 2020, p. 1346-1348).

REFERENCES

BERRYMAN, C. Holding Social Media Providers Liable for Acts of Domestic Terrorism. Florida Law Review, 2020, Volume 72, p. 1338.

BRAHA, D. Global Civil Unrest: Contagion, Self-Organization, and Prediction. PLoS ONE, 2012, Volume 7, Issue 10, e48596, p. 1.

BRANDENBURG v. OHIO, 395 U.S. 444 (1969) (per curiam). Available at: https://www.law.cornell.edu/supremecourt/text/395/444. Access: April 08, 2021.

CALVERT, C. First Amendment Envelope Pushers: Revisiting the Incitement-to-Violence Test with Messrs. Brandenburg, Trump, & Spencer. Connecticut Law Review, 2019, Volume 51, Number 1, p. 139-143.

DAVIS, J. H. Civil Disobedience and Civil Disorder. In DAVIS J. H. Perpetuation of the United States of America: 360-Degree Synchronization Zero Defects, 2014 XLIBRIS, Illustrated edition, USA, 172p.

EMERSON, J. S. In Defense of Brandenburg: The ACLU and Incitement Doctrine in 1919, 1969, and 2019. Brooklyn Law Review, 2019, Volume 85, Issue 1, Symposium: Incitement at 100-and 50-and Today, p. 21.

FLANAGAN, R. Kerner commission. Dictionary of American History. 2021. Available at: https://www.encyclopedia.com/history/dictionaries-thesauruses-pictures-and-press-releases/kerner-commission. Access: April 08, 2021.

GERKE, M. Understanding cybercrime: Phenomena, Challenges and legal response. ITU Telecommunication Development Sector, Geneva: Switzerland, 2014.

GRAHAM, H. D. On Riots and Riot Commissions: Civil Disorders in the 1960s. The Public Historian, 1980, Volume 2, Issue 4, p. 17.

GREENSTEIN, S. The basic economics of internet infrastructure. Journal of Economic Perspectives, 2020, Volume 34, Number 2, p. 193-194.

HANDBOOK ON MONITORING FREEDOM OF PEACEFUL ASSEMBLY. Warsaw, Poland, OSCE Office for Democratic Institutions and Human Rights (ODIHR), 2011.

HUGHEY, M. W. Of Riots and Racism: Fifty Years Since the Best Laid Schemes of the Kerner Commission (1968-2018). In Sociological Forum, 2018, Volume 33, Number 3, p. 619.

MACKINNON, R. et al. Fostering freedom online: The role of internet intermediaries. UNESCO Publishing. Paris, France, 2015.
NAUMENKO, A. Real Benefits of Active Caching in the WWW. In the 17th IASTED International Conference-Applied Informatics, 1999, No. CONF, p. 172-174.

PERCHATKINA, S. A., et al. Social internet networks: legal aspects. Journal of Russian Law, 2012, Volume 5, Issue 185, p. 20.

SCHEB, II J. M. Criminal Law. Seventh Edition. Stanford: USA, Cengage Learning. 2015.

SCHIPPELLE, 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, p. 138, 2019.

STALMACK, J. M. Constitutional Law - 1968 Anti-Riot Statute Up-held in United States v. Dellinger. Loyola University Chicago Law Journal, 1973, Volume 4, Issue 2. p. 593.

STEINBLATT, H. E-Incitement: A Framework for Regulating the Incitement of Criminal Flash Mobs. Fordham Intellectual Property, Media and Entertainment Law Journal, 2012, Volume 22, Number 3, Book 3, p. 782.

THE LAST-MILE INTERNET CONNECTIVITY SOLUTIONS GUIDE: Sustainable Connectivity Options for Unconnected Sites. Geneva: International Telecommunication Union, 2020. Licence: CC BY-NC-SA 3.0 IGO. p. 5.

TSESIS, A. Social media accountability for terrorist propaganda. Fordham Law Review, 2017, Volume 86, Issue 2, p. 624.

TSIRINA, M. A. Dissemination of pro-drug information on the Internet: measures to counteract. Journal of Russian Law, 2012, Volume 4, Issue 184, p. 49.

US KERNER COMMISSION et al. Report of the national advisory commission on civil disorders. US. US Government Printing Office, 1968.

WEBER, R. H. Internet Service Provider Liability: The Swiss Perspective. Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 2010, Volume 1, Number 3, p. 147.

ZHAROVA, A. K. On the necessity of legal classification of Internet operators. Business informatics, 2011, Volume 3, Issue 17, p. 63.
Resumo
Ações coletivas, particularmente organização, promoção, incentivo e incitação a distúrbios civis, são difíceis de imaginar sem o uso de tecnologias de informação e comunicação (TIC). Eventos recentes como a Primavera Árabe, as revoluções coloridas (por exemplo, no antigo Bloco Oriental e nos Países Balcãs), a agitação em Minneapolis em 2020 que posteriormente se espalhou para outras cidades dos EUA, e os distúrbios do Capitólio dos EUA 2021 apresentam evidências significativas a esse respeito. A disseminação de informações on-line incitando tumultos envolve provedores de serviços de internet (ISPs) ao lado do autor. O objetivo do artigo é especificar os atores de acordo com suas funções e determinar sua elegibilidade para ser processado em casos de incitação a tumultos usando TIC. Formulou uma conclusão sobre o início da responsabilidade intermediária dos ISPs, mantendo a capacidade organizacional e técnica de influenciar as relações sociais de informação de seus usuários a qualquer momento.

Keywords: Distúrbios civis. Motins. TIC. ISPs. Responsabilidade intermediária.

Abstract
Collective actions, particularly organization, promotion, encouragement, and incitement to civil disturbances, are hard to imagine without use of information and communication technologies (ICTs). Recent events such as the Arab Spring, the colour revolutions (e.g. in former Eastern Bloc and the Balkan countries), the unrest in Minneapolis in 2020 which subsequently spread to other US cities, and the US Capitol riots 2021 present significant evidence in this regard. The dissemination of information online inciting to riots involves internet service providers (ISPs) alongside the author. The aim of the paper is to specify the actors in accordance with their functions and determine their eligibility to be prosecuted in cases of incitement to riots using ICTs. Formulated a conclusion about the onset of intermediary liability of ISPs, holding the organizational and technical capacity to influence the information social relations of their users at any time.

Keywords: Civil disturbances. Riots. ICTs. ISPs. Intermediary liability.

Palavras-chave: Distúrbios civis. Motins. TIC. ISPs. Responsabilidade intermediária.

Resumen
Las acciones colectivas, en particular la organización, la promoción, el estímulo y la incitación a disturbios civiles, son difíciles de imaginar sin el uso de las tecnologías de la información y la comunicación (TIC). Eventos recientes como la Primavera Árabe, las revoluciones de color (por ejemplo, en el antiguo Bloque del Este y los países balcánicos), los disturbios en Minneapolis en 2020, que posteriormente se extendieron a otras ciudades estadounidenses, y los disturbios del Capitolio de Estados Unidos de 2021 presentan evidencia significativa en este sentido. La difusión de información en línea que incita a los disturbios involucra a los proveedores de servicios de Internet (ISP) junto con el autor. El objetivo del documento es especificar los actores de acuerdo con sus funciones y determinar su elegibilidad para ser procesados en casos de incitación a disturbios utilizando las TIC. Formuló una conclusión sobre el inicio de la responsabilidad intermediaria de los ISP, manteniendo la capacidad organizativa y técnica para influir en las relaciones sociales de información de sus usuarios en cualquier momento.

Palabras-clave: Disturbios civiles. Disturbios. TIC. ISPs. Responsabilidad del intermediario.