FACTA UNIVERSITATIS
Series: **Law and Politics** Vol. 14, N° 1, 2016, pp. 1 - 14

Review Paper

THE LIABILITY OF SOCIAL NETWORKS FOR EXTREME FORMS OF SPEECH

UDC 342.727:004.738.4
343.41:004.738.4

Dejan Vučetić[1], Gala Bončić[2], Petar Pešić[3]

[1]Faculty of Law, University of Niš, Republic of Serbia
[2]University of Niš, Faculty of Law; Trainee-volunteer, Basic Court in Niš, Republic of Serbia
[3]University of Niš, Faculty of Law;
Legal Apprentice, at Bončić, Tešić and Petrović-Adamović Law Office, Republic of Serbia

Abstract. *This paper focuses on the research of the normative framework concerning the liability for extreme forms of speech on social media networks as a new form of the internet intermediaries. The main hypothesis elaborated in the paper is that current international and national legal systems do not recognize the specificities of social media networks as a new type of internet intermediaries. Thus, there is a need for new regulations that will preserve the role of social media as an important forum for debating numerous issues of public importance and prevent a possible chilling effect caused by inobservance of human rights in the social media terms of service. In order to address to the raised questions, the authors analyzed numerous international and national legal documents as well as the case law of the European Court of Human Rights, the US Supreme Court and decisions of national courts related to social media networks.*

Key words: *extreme speech, freedom of expression, social media, liability of internet intermediaries.*

1. INTRODUCTION

The world has been rapidly changing since the Internet revolution in 1990. The changes have brought many advantages that drastically transformed the way of living. The Internet has become an international phenomenon that enables users to do almost anything online: perform banking transactions, vote, use phone networks, buy and sell goods, etc. Despite all the benefits, the Internet revolution has inevitably brought new legal problems

Received March 23rd, 2016/ Accepted April 12th, 2016
Corresponding author: Dejan Vučetić, LL.D
Assistant Professor, University of Niš, Faculty of Law, Trg Kralja Aleksandra 11, 18000 Niš, Republic of Serbia
E-mail: dvucetic@prafak.ni.ac.rs

that require suitable solutions. In addition, the aggravating factor for finding those solutions is undoubtedly the highest possible dynamics of changes and innovations that can hardly be regulated once and for all.

One rather forgotten aspect of the Internet is its value as a public service, which implies certain duties and responsibilities of the state as specified in the Council of Europe Recommendation on measures to promote the public service value of the Internet of 2007. The public Internet values are: human rights-consistent Internet policies, e-democracy, e-participation and e-government policies, ensuring access, affirming freedom of expression and free circulation of information on the Internet, and ensuring that voices of all nations, cultures and languages are equally represented in the Net. The Internet opens up completely new spaces for public debate, allowing people to share ideas. It is "a progressive public sphere made up of private spheres where, nevertheless, issues of public interest are discussed" (Benedek, Kettemann, 2013: 102).

Currently, one of the burning issues on an international level is the responsibility for the harmful online content. The Internet appeared to create a seamless global network that allowed content to flow uncontrollably across borders (Keller, 2011: 66). Often, when it comes to responsibility for the harmful content, the original creator of the content can be out of the reach of the state, thus unable to be held liable for his actions. This unfairly makes victims unsatisfied, which further gives rise to the issue of responsibility of the internet intermediaries.

In finding the answer to the issue of internet intermediaries' legal liability one should refer to the old principle that publishers are to be held liable for the unlawful content they have not created. This is the logical consequence of their incapacity to completely control the content they publish. Traditionally, the responsibility for the dissemination of prohibited content was based on this incapacity and on the degree of knowledge about specific content. Before the Internet era, the different approach was applied, depending on whether it was a question of responsibility of broadcasters or responsibility of telecommunications operators. The distinction was again established on the fact that broadcasters had a full control over the content, while telecommunications operators were unable to control the enormous amount of data. Hence, based on the full control over the content, the broadcasters were traditionally held liable for the content they published. The telecommunications operators were exempt from liability due to the huge amount of data passing through the wires and their incapacity to control it. Some authors considered that responsibility of some intermediaries (internet service providers - ISP) should be regulated in the same way as that of telecommunication operators, while others strongly opposed. This issue will be further examined in the corresponding part of this article.

The Internet itself is not just a new media form or a counterpart to broadcasting, newspapers, radio and cinema. It is a whole new media platform that can be used for any of the previous forms (Keller, 2011: 12) As already mentioned, users were once a passive auditorium and the information flow was going in one direction. Now, there is the chance for users to perform an active role, and many of them got involved in different "publishing" activities online. Thus, the traditional borders between freedom of speech and freedom to publish have vanished. As Keller noted, in order to publish information in the newspaper, publishers had to check and double-check the accuracy of their sources and the validity of information that would be launched on the "marketplace of ideas", while the blogosphere relies on the community to do the quality control (Keller, 2011: 24). Earlier, it was highly unlikely that any person could be a publisher, especially recipients of the media information.

In contrast, each Internet user today is a potential publisher. Due to this huge transformation in the media sphere, the likelihood of encountering illegitimate content online has significantly increased. Bearing in mind the differences between the Internet and so-called traditional types of media, the historical dangers (incitement to violence and hatred, disclosure of information, etc.) have become more prominent than ever before (Solove, 2011: 15).

Due to a huge amount of corollaries that illegitimate online content can cause, the question of liability of both the speaker and the provider of the public forum must be meticulously resolved. We are of the opinion that there is no universal answer which can equally apply to all intermediaries. The liability regime has to be established regarding the technical particularities of each separate sort of intermediary. In particular, the distinction between news portals and intermediaries that function on the basis of Web 2.0, such as social media networks (e.g. Twitter) has to be taken into account (Wong, Dempsey: 2010). Currently, one of the rare European legal sources that regulate this issue is the E-commerce Directive (2001), adopted adopted almost 15 years ago[1]. Back in 2001, social networks such as Twitter did not exist and the platform that enables its operation appeared several years later. This Directive cannot be applied to every Internet intermediary, without taking into account the differences between them. There is a legal gap at the European level. The "notice and take down" system that is required by the E-Directive can be seen as very problematic (Goldman, 2010), as we will discuss further in this paper. In the context of freedom of expression, the question of legal liability of new types of internet intermediaries (such as, social media networks) has not been answered by the ECtHR either, which issued only a couple of judgments regarding the liability of the intermediaries for illegitimate online expression[2]. In order to find the answer to the question of legal position of this new kind of media intermediaries, we will explore the ECtHR case law as well as the findings of the common law tradition, especially those of the US courts.

2. Extreme Speech, Hate Speech and Freedom of Expression

Hate Speech as a phenomenon certainly predates the Internet era (Benedek, Kettemann, 2013: 82) but it is even more dangerous now, in the context of Internet usage, because of its wide reach. In his "Free Speech: A very Short Introduction", Nigel Warburton writes that Richard Posner has indentified four features of this new means of dissemination which may magnify the dangers of irresponsible speech: anonymity, lack of quality control, huge potential audience, and antisocial people who find their soul mates (Warburton, 2009: 81). The notion and general characteristics of the hate speech have been analyzed in numerous works of modern human rights' scholars (Wolfson, 1997; Weinstein, 1999; Weber, 2009; Waldron, 2012; Brown, 2015). Hate speech is prohibited by numerous international legal documents such as the International Covenant on Civil and Political Rights, the International Convention on the Elimination of All Forms of Racial Discrimination, the European Convention on Human Rights, and others.

When it comes to extreme forms of online speech, there are several relevant international documents. One of the most important is the General Policy Recommendation N°6:

[1] Art. 14, E-Commerce Directive, 2000/31/EC.

[2] For example: Case Ap.64569/09, *Delfi v Estonia*; Case Ap. 22947/13 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary.*

Combating the dissemination of racist, xenophobic and antisemitic material via the Internet, adopted by the European Commission against Racism and Intolerance (ECRI) on 15 December 2000. In this document, the ECRI recommends to member States:

- "to include the issue of combating racism, xenophobia and antisemitism in all current and future work at international level aimed at the suppression of illegal content on the Internet;
- to reflect in this context on the preparation of a specific protocol to the future Convention on cyber-crime to combat racist, xenophobic and antisemitic offences committed via the Internet;
- to take the necessary measures for strengthening international co-operation and mutual assistance between law enforcement authorities across the world, so as to take more efficient action against the dissemination of racist, xenophobic and antisemitic material via the Internet;
- to ensure that relevant national legislation also applies to racist, xenophobic and antisemitic offences committed via the Internet and prosecute those responsible for this kind of offences;
- to undertake sustained efforts for the training of law enforcement authorities in relation to the problem of dissemination of racist, xenophobic and antisemitic material via the Internet;
- to reflect, in this context, on the setting up of a national consultation body which might act as a permanent monitoring centre, mediating body and partner in the preparation of codes of conduct;
- to support existing anti-racist initiatives on the Internet as well as the development of new sites devoted to the fight against racism, xenophobia, antisemitism and intolerance;
- to clarify, on the basis of their respective technical functions, the responsibility of content host and content provider and site publishers as a result of the dissemination of racist, xenophobic and antisemitic messages;
- to support the self-regulatory measures taken by the Internet industry to combat racism, xenophobia and antisemitism on the net, such as anti-racist hotlines, codes of conduct and filtering software, and encourage further research in this area;
- to increase public awareness of the problem of the dissemination of racist, xenophobic and antisemitic material via the Internet while paying special attention to awareness-raising among young Internet-users – particularly children –as to the possibility of coming upon racist, xenophobic and antisemitic sites and the potential risk of such sites."

In 2003, the Council of Europe adopted Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. By the end of the 2014, a total number of 22 States have ratified this protocol and additional 13 States are in the ratification process, after signing the protocol. Under the provisions of the Additional Protocol, dissemination of the racist and xenophobic material through computer systems as well as racist and xenophobic motivated threats and insults are to be criminalized; in particular, it refers to "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of

individuals, based on race, colour, descent or national or ethnic origin, as well as, religion if used as a pretext for any of these factors" (Article 2 paragraph 1 of the Protocol).

The provisions in Article 3 of the Additional Protocol stipulate that:

"1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available."

Articles 4 and 5 of the Protocol prescribe that each State Party should adopt legislative and other measures under domestic law to treat racist and xenophobic motivated threats or insult through a computer system as a criminal offence. Article 6 envisages the same treatment in case of denial, gross minimisation, approval or justification of genocide or crimes against humanity.

When it comes to the practice of the European Court of Human Rights, the most important cases on this issue, that we would like to point out, are: *Erbakan v. Turkey* (6 July 2006), application No. 59405/00; *Feret v. Belgium* (16 July 2009), application No. 15615/07; *Leroy v. France* (2 October 2008), application No. 36109/03; *Vejdeland and Others v. Sweden* (9 February 2012), application No. 1813/07.; *Norwood v. the United Kingdom* (16 November 2004), application No. 23131/03; and *Karatas v. Turkey* (8 July 1999), application No. 23168/94 (European Court of Human Rights, 2013).

3. Normative Framework of Liability of Internet Intermediaries

Nowadays, the Internet is increasingly becoming a public forum or public sphere where private individuals can debate on numerous issues of public concern, irrespective of their rank, status or social position. However, a lot of those Internet places are not completely open to the whole public and they are regulated by terms of services of numerous private actors, such as: Internet service providers, blogging services and social media networks. Thus, we come to the paradoxical situation that debate of public importance is held at private Internet places. In the 2010 OpenNet Initiative report on public and private spheres, it is designated as a "quasi-public sphere", which is subject to both public and private content controls spanning multiple jurisdictions and differing social mores (Benedek, Kettemann, 2013: 103).

This rather controversial position is confirmed by the Committee of Ministers of the Council of Europe in the 2011 Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers. This Declaration underscores the importance of social networks, blogging sites and Internet-based companies as a means of mass communications for civil society activist, whistle-blowers and human rights' defenders through which they can exchange information, publish content, interact, associate and debate on the various matters of public concern.

Furthermore, there is a tendency among private Internet-based companies to regulate those private online spaces more strictly than it may be the case in national legal systems and their regulation of public forums. Another significant problem is that these companies, through their terms of services, apply the legal rules of their home countries to various users from all over the world. Although this may be an advantage in case where these rules are less restrictive than the national ones, these terms of services can sometimes directly or indirectly violate human rights. In some "human rights-sensitive states", those companies will further limit freedom of expression in order to comply with the rules of those states and protect their businesses, thus undermining the balance between the public and the private interest.

In the past decades, this legal domain was left to self-regulation of the intermediaries (especially when it comes to illegal content available on the Internet sites) and the underlying rules. The liability of Internet intermediaries for content generated by Internet users is established through the so-called “notice-and-take-down” procedures. Yet, these can be misused both by the state and private actors.

One of the most important obligations of Internet intermediaries is the limitation of the so-called *ex ante* content-moderation which is crucial for effective exercise of freedom of expression on the Internet and open online exchange of ideas. Even *ex post* content-moderation, which requires a right balance between public laws and self-created private rules can be extremely difficult especially when it comes to social media networking sites, which are faced with "conflicting demands and threats by states to disallow access altogether in case of non-removal of impugned information" (Benedek, Kettemann, 2013: 98).

This position is confirmed by the Committee of Ministers of the Council of Europe in its Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services, as well as in several ECtHR cases, such as: *Surek Renaud*, and *Delfi*.

Upon the aforesaid, we may conclude that freedom of expression in social networks environment is not endangered only by disproportional demand of the state but also by the self-regulation of the social networks themselves.

4. Extreme Speech on Social Networks and Open Legal Questions Concerning Web 2.0

With the development of Web 2.0 and rise of social media networks, they have gained the central role in securing the Internet's first place as a public forum for debate. In these virtual places, freedom of expression, assembly and much of the other human rights are being freely exercised and discussed, thus "amplifying" the principle of citizens’ participation in the matters of public concern as a cornerstone of democracy.

At the same time, social media have another "dark" rule-creating side, which was already analyzed in regard with internet intermediaries, and which may endanger human rights. According to the 2012 Council of Europe’s Council of Ministers’ *Recommendation on the protection of human rights with regard to social networking services*, the "danger" arises from:

> "lack of legal and procedural safeguards surrounding processes that can lead to the exclusion of users; inadequate protection of children and young people against harmful content or behaviours; lack of respect for others’ rights; lack of privacy-friendly default settings; lack of transparency about the purposes for which personal data are collected and processed".

Children are especially vulnerable in social networks environment where they may communicate unknowingly with sex predators, share personal information with serious negative effects, engage in harmful behaviour or come into contact with harmful content. Cyber-bullying and cyber-grooming are present dangers. Though children, especially teenagers and adolescents, should use social networks in their self-actualisation processes and in the development of their self-identity, social network service providers need to introduce adequate safeguards; and if they fail to do so, states need to enforce the protection framework envisaged in *K. U. v. Finland*.

In the case *K. U. v. Finland*[3] an unknown person had published the personal details of a 12-year-old on a dating website, which obviously put the child in danger of various predators. Since Finnish law at that time did not allow the police to ask Internet service providers to reveal the identity of the person who had published the profile, the publication of K.J.'s personal data was found to have violated the victim's right to privacy. As the anonymity that characterises much communication on the Internet makes it harder for the police to ensure the human rights of victims of privacy violations, states have to provide a legal framework sufficient to pierce the veil of anonymity in serious cases.

But, most harm can be caused by inadequate and human-rights-unfriendly terms of services, as Benedek and Kettemann explain in detail using the example of the Facebook Principles, the social network's Statement of Rights and Responsibilities, and the Facebook Community Standards (Benedek, Kettemann, 2013: 98). These authors point out that Facebook's Abuse Standards are becoming "*de facto* the law in force regarding freedom of expression in an important international forum". Thus, the regulation and standards governing the freedom of expressions end up in the hands of powerful private companies. In effect, they should be required to observe and comply with relevant international freedom of expression standards in devising such documents, which should be completely public, accessible, and foreseeable!

Thus, the Council of Europe Recommendation on social network providers (2012), issued by the Committee of Ministers to the Member States, suggested that social networking providers should respect human rights and the rule of law, and especially ensure that "procedural safeguards are respected by these mechanisms, including the right to be heard and to review or appeal against decisions, including in appropriate cases the right to a fair trial, within a reasonable time and starting with the presumption of innocence". The Council of Ministers also recommended that:

"... member States, in consultation with private sector actors and civil society, develop and promote coherent strategies to protect and promote respect for human rights with regard to social networking services, in line with the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5, hereinafter referred to as "the European Convention on Human Rights"), especially Article 8 (Right to respect for private and family life), Article 10 (Freedom of expression) and Article 11 (Freedom of assembly and association) and with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), in particular by engaging with social networking providers to carry out the following actions:

[3] K.U. v. Finland (2 December 2008), application No. 2872/02, paras. 41-50.

- to provide an environment for users of social networks that allows them further to exercise their rights and freedoms;
- to raise users' awareness, by means of clear and understandable language, of the possible challenges to their human rights and the ways to avoid having a negative impact on other people's rights when using these services;
- to protect users from harm without limiting freedom of expression and access to information;
- to enhance transparency about data processing, and refraining from illegitimate processing of personal data;
- to set up self- and co-regulatory mechanisms where appropriate, in order to contribute to the respect of the objectives set out in the appendix to this recommendation;
- to ensure accessibility to their services to people with disabilities, thereby enhancing their integration and full participation in society."

5. SOCIAL MEDIA NETWORKS IN THE JURISPRUDENCE OF NATIONAL COURTS

5.1. Twitter-related cases in the UK, France, Germany and Spain

In the *Paul Chambers* ("Twitter Joke") case, after finding out that the local airport was closed due to bad weather conditions, the defendant tweeted: "Crap! Robin Hood airport is closed, you've got a week and a bit to get your shit together otherwise I'm blowing the airport sky high!" In the first instance court, he was convicted of making statements of a menacing character; the decision was upheld by the second instance court. Upon appeal, the High Court overturned the judgment. Some of the British institutions (Director of the UK Crown Prosecution Service) stated that "a broader awareness-raising approach is necessary not only by prosecutors but also by others, including the police, the courts and service providers".

In January 2013, a French court ruled that Twitter had to identify authors of anti-Semitic messages "within the framework of its French site" and Twitter complied with the ruling (Benedek, Kettemann, 2013: 118). In a similar situation, Twitter responded to the state request and suspended the account of a German neo-Nazi group. In Spain, young Alba González Camacho (aged 21), a "very normal girl" was convicted for inciting to terrorism over Twitter after posting calls to a far-left terrorist organization to kill politicians (Minder, 2014).

5.2. US legal stance on liability of social media networks

The United States have developed strong jurisprudence with regards to liability of social media networks. The reason partly lies in the fact that the legal system developed in the US and other English-speaking countries embraces new legal issues and adapts its current system in order to resolve potential problems that may arise with those new legal issues. In addition to jurisprudence that is trying to create solutions for new problems, some solutions are also provided in legislative acts.

The most important legislative act is certainly the 1996 Communications Decency Act (CDA), which includes Article 230 titled "Protection for private blocking and screening of offensive material", which clearly reflects the legislator's intention in enacting this provision. Namely, this Article has been known as "*safe harbour*" (Peter, 1993: 349) for intermediaries in general, including social media networks. Notably, the first two parts of Article 230 state

the current situation related to the Internet services and the US policy with regards to development of new technologies. The third part of Article 230 stipulates: C (1) "N*o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."* What does this actually mean?

The provision in Article 230, section C (1), basically creates a freedom to use content that is provided by somebody else without exposing yourself to the potential legal problems. The legislators' creative thinking is mind-boggling. This provision was introduced in the US Code in 1998. Back then, there were no social media and there was maybe a handful of websites. "*Share*" option did not exist either. Yet, this Article envisaged the possibility of "*sharing*" content provided by other people or providers, without being sued. This kind of provision undoubtedly helped the Internet flourish and become what it is today, a place full of different interactive websites and networks where users may freely exchange ideas and information.

The provision in Article 230, section C (2), stipulates that providers and users of interactive computer services shall not be held liable in cases where they take voluntary action in good faith to restrict access to or availability of material that the provider or a user find to be obscene, lewd, lascivious, violent, harassing, or otherwise objectionable. Having in mind the EU system of liability of internet intermediaries, this provision is more foreseeable and imposes fewer obligations on intermediaries. First of all, there are no classes of intermediaries. There is no definition of hosts, providing streaming services or cache content; instead, there are only users and providers. Second, unlike the EU E-Commerce Directive, there are no requirements to be met in order to invoke exemptions from liability. The knowledge and the degree of provider's awareness is not prescribed, which may be a good thing for intermediaries for two reasons: it gives them more power to remove content which is not in accordance with their policy, and it provides more security from invoking liability by those harmed by content on their platform.

Yet, the glass is only half full, given the fact that this provision does not apply to some of the most troublesome issues that arise daily on the Internet. Those are the problems of criminal liability for the most serious criminal offences and copyright infringement, which Internet users face on the daily basis. The intermediaries may he charged and found criminally liable on the grounds of federal criminal offences stipulated in the US Code, such as: hate crimes, offences related to terrorism, etc. Nowadays, everyone may easily be subject to some form of hate speech online; due to the rise of ISIS, incitement to terrorism or encouragement to commit terrorist acts or to spread the ideology of terrorist organizations is also a topical issue. Thus, we can conclude that social media networks can be held accountable for committing some forms of offences. However, so far there has been no record of any social media network being criminally prosecuted in the US although most popular social networks are based there. Should a social media network be prosecuted and convicted for committing a criminal offence, it would most likely be the end of social networks as we know them today. In that case, social networks would have to adapt; they would either have to engage more resources in controlling the posted contents or give up and stop working. Any of these routes would be restricting the freedom of speech or expression online.

Now, let us examine the reasoning of the US court judges in applying Article 230 of the Communications Decency Act. This provision has been applied in a lot of cases but we will focus on just a few that we believe sufficiently illustrate the practical application of this Article in the US jurisprudence.

5.3. DOE v My Space, Inc

This case was brought up before the Fifth Circuit Court of Appeals in May 2008. Plaintiffs (representing a minor) claimed that *My Space* acted negligently by not using a software to verify the users' age, which ultimately led to the minor's sexual abuse. The plaintiffs also alleged fraud but as the allegations were not substantiated, so that they have not been reviewed separately. The Court first noted that Article 230 of the CDA has been enacted in order to further develop the Internet as a powerful medium for communication and information, and explained the standards developed in the Court jurisprudence on the grounds of applying this Article. It shows that this provision has been broadly interpreted by the courts, which were more lenient towards providers than the text of Article 230. The Court also referred to a case of *Carafano*[4], where the 9th Circuit Court held that full immunity from liability is given to providers in cases when "third parties willingly provides the essential published content". This case also casts more light on the "notice-and-takedown" system that providers may call upon the opinion in the case of *Zeran*[5]. In that case, the Court said: "*If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement—from any party, concerning any message... Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not. Thus, like strict liability, liability upon notice has a chilling effect on the freedom of Internet speech...*"

However, although plaintiffs acknowledged the opinions in *Zeran* and *Carafano*, they claimed that this case was different because *My Space* "failed to implement safety measures to protect minors". The Court stated that there was no case law to support their arguments. In the common law system, judges have had the opportunity to be the first ones to address the issue of liability of social networks in a different manner, by establishing situations and conditions which are to be met in order to conclude that social networks in some cases may be held accountable for third-party content. Standing by the decision of the District Court, the Supreme Court held that social networks are barred from liability under the CDA. Yet, the Court failed to demonstrate forward thinking, which would have a much bigger effect on the way social networks are perceived today. By holding onto procedural aspects like the plaintiffs' failure to invoke certain claims before the District Court, which led to dismissal in the Court of Appeals, the Supreme Court has failed to respond to the question: Can social networks be held liable for negligence, and in what situations? The fact is that there are not many cases that specifically concern social networks and their policies on the content posted by users; more cases on these issues would have certainly contributed to recognizing the importance of social media networks' liability. Instead, the Court stood by Article 230 exemptions from liability without showing the boundaries of that liability. We can conclude that in cases involving potential civil liability, social networks in the US are always most likely to be exempted from it.

[4] *Carafano v. Metrosplash*.com, Inc., 339 F.3d 1119, 1123–24.
[5] *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330–31.

5.4. DOE v SexSearch.com, et al

The case was initially decided by the US Court for the Northern District of Ohio in 2007. After being prosecuted for engaging in consensual sexual activities with a minor, one of the users of the said social network sued the network which warranted that all users were adults, which was obviously not the case. Moreover, only adults could be paying members (subscribers) of the network but somehow a minor turned out to be one of the paying members. The plaintiff claimed that Article 230 (exemption from liability) could not apply to the defendants who did not satisfy the conditions set out in this provision. More specifically, the plaintiff claimed that the social network modified content and should be held liable for creation of content. The District Court reasoned that social network did not create content in this particular case although they may have done it in some other cases. What can potentially be important is that the District Court found that there were no claims for liability of social networks other than those of civil liability. The Court reaffirmed that, should civil liability be imposed on social networks, it would have a seriously chilling effect on the freedom of speech. Notably, this reasoning reflects a higher degree of forward thinking than the legal reasoning provided in the previously examined case, and it shows the major concern underlying many US judicial decisions dealing with the issue of liability of social media networks. Even though the Court concluded that Article 230 of CDA was applicable in this case, it still assessed the plaintiff's claims on the merits which may be beneficial only in future cases. One of the opinions of the Court which may have a long lasting effect is the stance that the limited liability warning that social networks usually have in their Terms of Service or Terms of Use are binding to users; hence, if something unexpected happens on a social network, even if it is inconsistent with the guarantees made by the network itself, the intermediaries may still invoke exemption from liability. Thus, the Court concluded that the plaintiff's civil liability claims were barred by the application of Article 230.

From these cases we can conclude that Article 230 of the CDA grants social media networks broad immunity from civil liability. However, as there were no criminal proceedings brought against social media networks, we can only speculate what the legal reasoning would be in such circumstances.

6. CONCLUSION

Facebook, Twitter and other social media earn billions of dollars quarterly. In that context, we cannot help posing the first question: do these companies even need any protection from liability? They can certainly invest in creating effective solutions in order to make their services free of unlawful content. Some of them are already doing something like that (Zeller, 2015). The second question is why social media networks in the US are not subjected to prosecution for certain criminal offences. It would be ideal to think that the protection of freedom of expression is the driving force behind the impenetrable "defence" of social networks. Yet, there are other strong reasons, one of which is the fact that this business sector is attracting huge profits and helping other companies to position themselves and attract new customers. There is also a concern about the subsistence of smaller social networks which cannot afford to fund monitoring and screening of user-generated content. There is a growing pressure on social networks to work more closely with national authorities, to reveal data of those who commit criminal offences online or to remove content that is deemed unlawful by

national authorities. That pressure is likely to impact the business operations of social media networks, which are increasingly exercising self-censorship. Social media networks are increasingly prone to performing their public role and even suppressing expression in certain situations. Yet, that form of self-censorship is still a better choice than prosecution for hosting unlawful content and committing criminal offences.

The Internet does not recognize any borders. Therefore, it would be logical to create universal rules which would be applied in resolving the problem of liability of social media networks. Such rules should be created by an international body of authority, such as the UN. However, the diversity of legal solutions in different legal systems generates a huge gap which is currently highly unlikely to be closed for the benefit of social network users. We can only look forward to a prospective change in this area which would bring a new tidal-wave of development in the field of freedom of expression.

At the end, we must conclude that Internet gatekeepers have an important role not only as "watchdogs" but more frequently as providers of virtual space for public debate, whose participants are the real-life human rights' "watchdogs" (such as: NGOs, citizen activists, etc.). On the other hand, states have an obligation not to exert politically motivated pressure on social media networks and to respect all human rights, especially the freedom of expression.

Acknowledgement: *The research is realized under the project no. 179046 financed by the Ministry of Education, Science and Technological Development of the Republic of Serbia.*

REFERENCES

1. Brown, A. (2015). *Hate speech law: a philosophical examination*. Abingdon, New York: Routledge.
2. Council of Europe (2003). *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. Strasbourg: Council of Europe.
3. Council of Europe, European Commission against Racism and Intolerance. (2001). *General Policy Recommendation N°6: Combating the dissemination of racist, xenophobic and antisemitic material via the internet*, adopted by ECRI on 15 December 2000. Strasbourg: Council of Europe.
4. Council of Europe, Committee of Ministers. (2011). *Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers*, (7 December 2011), Strasbourg: Council of Europe.
5. Kettemann, M., Benedek, W. (2014). *Freedom of expression and the Internet*, Strasbourg, Council of Europe Publishing.
6. Keller P. (2011). *European and international media law: liberal democracy, trade, and the new media*. Oxford; New York: Oxford University Press.
7. Solove D. (2011). Speech, Privacy and Reputation on the Internet" in Nussbaum, M. and Levmore, S.,(eds), *The Offensive Internet: Speech, Privacy and Reputation* (Harvard University Press.
8. Swire, P. (1993). "Safe Harbors and a Proposal to Improve the Community Reinvestment Act", *Virginia Law Review* 79 (349).
9. Waldron, J. (2012). *The Harm in Hate Speech*. Cambridge, Mass. : Harvard University Press.
10. Warburton, N. (2009). *Free Speech: A Very Short Introduction*. Oxford; New York: Oxford University Press.
11. Weber, A. (2009). *Manual on hate speech*. Strasbourg: Council of Europe Pub.
12. Weinstein, J. (1999). *Hate Speech, Pornography, and Radical Attacks on Free Speech Doctrine*. Boulder, Colo: Westview Press.
13. Wolfson N. (1997). *Hate Speech, Sex Speech, Free Speech*. Westport, Conn.: Praeger.

List of cases

Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123–24.
Case Ap. 23168/94, Karatas v. Turkey.
Case Ap. 24762/94, Surek v. Turkey (No. 4).
Case Ap. 59405/00, Erbakan v. Turkey.
Case Ap. 2872/02, K.U. v. Finland.
Case Ap. 36109/03, Leroy v. France.
Case Ap. 15615/07, Feret v. Belgium.
Case Ap. 1813/07, Vejdeland and Others v. Sweden.
Case Ap.64569/09, Delfi v Estonia.
Case Ap. 23131/03, Norwood v. the United Kingdom.
Case Ap. 22947/13 Magyar TartalomszolgáltatókEgyesülete and Index.hu Zrt v. Hungary.
Zeran v. Am. Online, Inc., 129 F.3d 327.

Treaties and legislation

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 *on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* ('Directive on electronic commerce') OJ L 178, 17. 7. 2000.
Recommendation CM/Rec(2012)4 on *the protection of human rights with regard to social networking services,* (adopted by the Committee of Ministers on 4 April 2012, at the1139th meeting of the Ministers' Deputies).
Telecommunications Act of 1996. Public Law 104-104, 104th Congress. (Communication Decency Act).

Internet sources

1. European Court of Human Rights (2016). *Factsheet - Hate speech* Retrieved 13. 3. 2016. (http://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf)
2. Goldman, E, (2010) "Rare Ruling on Damages for Sending Bogus Copyright Takedown Notice – Lenz v. Universal," Technology & Marketing Law Blog, Retrieved 13. 3. 2016. available at http://blog.ericgoldman.org/.../2010/02/standards_for_5.htm (accessed 15 November 2015).
3. Minder, R. (2014), In a First for Spain, a Woman Is Convicted of Inciting Terror Over Twitter, NY Times Retrieved 13. 3. 2016. http://www.nytimes.com/2014/02/23/world/europe/in-a-first-for-spain-a-woman-is-convicted-of-inciting-terror-over-twitter.html?hp&_r=1
4. Wong C., Dempsey, J. X. (2010). T*he Media and Liability for Content on the Internet, Mapping Digital Media*: Reference Series No. 12. London: Open Society Institute Retrieved 13. 3. 2016. https://www.opensocietyfoundations.org/sites/default/files/mapping-digital-media-liability-content-internet-20110926.pdf.
5. Zeller, F. (2015), *Facebook pledges to combat racism on German platform*, Yahoo News Retrieved 13. 3. 2016. http://news.yahoo.com/facebook-pledges-combat-racism-german-platform-151330415.html

PRAVNA ODGOVORNOST DRUŠTVENIH MREŽA ZA EKTREMNI GOVOR

Društvene mreže predstavljaju svakodnevnicu 21. veka. Na njima objavljujemo svoja razmišljanja, komentarišemo tuđa, a mnoge od misli koje ne bismo pomislili da kažemo naglas, na mrežama bivaju objavljene bez obzira na posledice. Ovaj rad je fokusiran na sagledavanje granica odgovornosti društvenih mreža za ekstreman govor koji se na njima često pojavljuje. Sve je više država koje procesuiraju građane zbog različitih oblika izražavanja na mrežama. Međutim, ne postoji jedinstven stav po pitanju toga šta predstavlja ekstreman govor na mrežama i internetu i kada za te vrste govora treba da odgovaraju i same društvene mreže. Ipak, postoje određeni zajednički činioci koji se provlače kroz gotovo sve jurisdikcije a u radu su prikazane one najznačajnije - Evropa i SAD.

Društvene mreže, kao svojevrsni prenosioci tuđih reči, uglavnom su bile izuzete od pravne odgovornosti. Ali se plima polako menja i sve češće možemo čuti na vestima da je neka društvena mreža optužena za određeno krivično delo, a nisu retki ni slučajevi u kojima te iste mreže bivaju tužene, kojom prilikom se od njih često traži i višemilionska odšteta. Na međunarodnom planu postoje brojna rešenja ovog problema. Neka pretežu u korist društvenih mreža dok im druga nameću povećanu odgovornost za sadržaj koji se na njima pojavljuje. Pravni akti koji su propisivali izuzmanje od odgovnornosti su uglavnom bili doneti daleko pre pojave društvenih mreža, u momentu kada se htelo podstaknuti njihovo stvaranje. Danas kada su one postale multinacionalne kompanije sa ogromnim profitima postavlja se pitanje njihovog daljeg važenja. I same društvene mreže prepoznaju probleme koji mogu nastati nepažnjom te često i same sklanjaju određeni sadržaj bez naloga ili zahteva javnih vlasti, što se sve više prepoznaje kao štetno po slobodu izražavanja i govora. Zbog sveta navedenog, jasno je da je ovo tema koja će tek proizvesti brojne debate u svetu.

Pitanja na koja smo pokušali da odgovorimo u radu obuhvataju sledeće dileme: Šta obuhvata ekstreman govor? Kakva je praksa u svetu po pitanju odgovornosti društvenih mreža? Koja se pravna pitanja postavljaju u vezi sa ekstremnim govorom na društvenim mrežama? U davanju odgovora na ova pitanja autori su koristili međunarodne pravne dokumente, praksu najviših nacionalnih sudova, kao i Evropskog suda za ljudska prava.

Ključne reči: *ekstreman govor, sloboda izražavanja, društvene mreže, pravna odgovornost internet posrednika.*