DIGITALNI VIGILANTIZAM: ANALIZA INTERNETSKE PRAVDE, ETIČKIH IZAZOVA I ULOGE DRUŠTVENIH MEDIJA

DIGITAL VIGILANTISM: EXAMINING ONLINE JUSTICE, ETHICAL CHALLENGES, AND THE ROLE OF SOCIAL MEDIA

DALIBOR DOLEŽAL

University of Zagreb, Faculty of Education and Rehabilitation Sciences, Borongajska 83 f, Zagreb, Croatia,
contact: dalibor.dolezal@erf.unizg.hr

Received: 02.05.2024.
Accepted: 13.11.2024.

Review article
UDK: 343.254:004
doi: 10.31299/hrri.60.2.10

Sažetak: *Kriminalitet se u povijesti javljao u različitim oblicima i opsezima, a jedan od posebnijih oblika je tzv., vigilantizam. U tradicionalnom smislu vigilantizam označava prisvajanje odluke pojedinaca i/ili grupa o izvršavanju pravde u situacijama kada se percipira kako formalne institucije zadužene za te aktivnosti nisu reagirale kako treba ili nisu reagirale uopće (Brown, 1975). S pojavom novih tehnologija, posebice interneta, vigilantizam je poprimio i svoj digitalni oblik – digitalni vigilantizam. Iako se osnovna osobina ovih pojava, izvršavanje pravde kada ona nije percipirano zadovoljena, uzroci, motivi, metodologije i pojavni oblici digitalnog vigilantizma se zbog mogućnosti digitalnih tehnologija sve više razlikuju od vigilantizma. Stoga je svrha ovog rada dati pregled dosadašnjih saznanja o osobitostima digitalnog vigilantizma te problematici koja se veže uz ovu pojavu.*

Ključne riječi: *kriminologija, vigilantizam, digitalni vigilantizam, cyber kriminalitet*

Abstract: *Crime has emerged in various forms and contexts throughout history, and one of the more specialised forms is so-called vigilantism. In the traditional sense, vigilantism is the appropriation of the decision by individuals and/or groups to pursue justice in situations where it is felt that the formal institutions responsible for these activities have not responded properly or at all (Brown, 1975). With the advent of new technologies, especially the Internet, vigilantism has taken on a digital form - digital vigilantism. Although the basic characteristic of these phenomena is the execution of justice when it is not perceived to be fulfilled, the causes, motives, methods, and manifestations of digital vigilantism increasingly differ from traditional vigilantism due to the possibilities offered by digital technologies. The aim of this study is therefore to provide an overview of the current state of knowledge about the particularities of digital vigilantism and the issues associated with this phenomenon.*

Keywords: *criminology, vigilantism, digital vigilante justice, cybercrime*

UVOD

S pojavom sve većeg broja kaznenih djela koja uključuju uporabu računala te internet kao sredstvo komunikacije, kriminološka istraživanja sve su više usmjerena na analize kako se tradicionalne teorije mogu upotrebljavati za razumijevanje kriminalnih interakcija koje se odvijaju u okvirima interneta, odnosno, u tzv., *online* svijetu. Kao

INTRODUCTION

With the occurrence of an increasing number of crimes using computers and the Internet as a means of communication, criminological research is increasingly focusing on analyses of how traditional theories can be used to understand criminal interactions that take place in the digital context,

mrežno okruženje, internet nudi nove mogućnosti za istraživanje kriminalnih interakcija, ali i mogućnosti za digitalno ulaženje u kriminalne aktivnosti (Clarke, 2004; Goldsmith i Brewere, 2014). Internet i digitalne tehnologije također pružaju mogućnosti široj javnosti da se uključe u aktivnosti koje uglavnom spadaju u djelokrug policije, uzimajući time nerijetko pravdu u svoje ruke (Huey, Nhan i Broll, 2013; Powell, Stratton i Cameron, 2018; Trottier, 2014; Yardley, Lynes, Wilson i Kelly, 2018).

Pojava gdje pojedinci ili grupe koji ne pripadaju formalnim institucijama s pripadajućim ovlastima za provedbu aktivnosti protiv kriminaliteta prisvajaju te ovlasti s ciljem poduzimanja aktivnosti koji su djelokrugu rada formalnih institucija otprije je poznata kao vigilantizam. Vigilantizam u tradicionalnom smislu znači provođenje zakona ili pravde izvan pravnog sustava, odnosno uzimanje pravde „u svoje ruke“. Izveden iz riječi “vigilante”, pojam se odnosi na čin uzimanja zakona u vlastite ruke, često s namjerom provođenja uočene pravde ili ispravljanja uočenih nepravdi (Brown, 1975). Osobe ili grupe koje to čine, tzv., vigilanti, obično djeluju izvan utvrđenog zakonskog okvira, bez službenih ovlasti ili mandata. Njihove radnje mogu varirati od patroliranja susjedstvima do uhićenja osumnjičenih, a u nekim slučajevima čak i izricanja kazni. Vigilantizam se shvaća kao odgovor na percipirano nedolično ponašanje koje se smatra dovoljno ozbiljnim da zaslužuje pozornost formalnog pravosudnog sustava, ali koje ovlaštena tijela ne rješavaju na odgovarajući način ili na način na koji vigilanti smatraju da bi trebalo. Slabosti i nepravde u formalnom pravosudnom sustavu postoje u svakom društvu, a vigilanti djeluju kao neformalni psi čuvari zajednice kako bi kompenzirali nedostatke ovog sustava (Burrows, 1976).

Digitalni vigilantizam, također poznat i kao digilantizam, internetski ili *online* vigilantizam te *cyber* vigilantizam, pojam je koji je nastao spajanjem “digitalnog” i “vigilantizma” i odnosi se na upotrebu digitalnih sredstava i online platformi od strane pojedinaca ili grupa za aktivnosti tradicionalno povezane s vigilantizmom. U digitalnom kontekstu to znači da pojedinci ili grupe upotrebljavaju *online* alate i tehnike kako bi ostvarili

i.e., in the so-called online world. As a network environment, the Internet offers new opportunities for the study of criminal interactions, but also opportunities to engage in criminal activity digitally (Clarke, 2004; Goldsmith and Brewere, 2014). The internet and digital technologies also provide opportunities for the general public to engage in activities that typically fall under the purview of the police and take justice into their own hands (Huey, Nhan, & Broll, 2013; Powell, Stratton, & Cameron, 2018; Trottier, 2014; Yardley, Lynes, Wilson, & Kelly, 2018).

Vigilantism is the phenomenon whereby individuals or groups, who do not belong to formal institutions with appropriate jurisdiction to carry out anti-crime measures, carry out activities that fall within the purview of formal institutions. Vigilantism in the traditional sense means enforcing the law or justice outside the legal system, i.e., taking the law “into one’s own hands”. Derived from the word “vigilante,” the term refers to the act of taking the law into one’s own hands, often with the intention of enforcing perceived justice or correcting perceived injustices (Brown, 1975). The individuals or groups who do this, known as vigilantes, usually act outside the established legal framework, without official authority or mandate. Their actions can range from patrolling neighbourhoods to arresting suspects, and in some cases, even imposing sentences. Vigilantism is understood as a response to perceived misbehaviour that is considered serious enough to merit the attention of the formal justice system, but is not dealt with appropriately, or as the vigilantes believe it should be dealt with by the authorities. Weaknesses and injustices in the formal justice system exist in every society, and vigilantes believe that they need to act as an informal watchdog of the community to compensate for the shortcomings of that system (Burrows, 1976).

Digital vigilantism, also known as *digilantism*, internet or online vigilantism, and cyber vigilantism, is a term created by combining “digital” and “vigilantism” and it refers to the use of digital means and online platforms by individuals or groups for activities traditionally associated with vigilantism. In a digital context, this means that

ono što smatraju pravdom, često bez službenog odobrenja (Powell i sur., 2016; Johnston, 1996; Trottier, 2017).

Svrha je ovog rada dati uvid u fenomen digitalnog vigilantizma, a cilj je rada analizirati karakteristike digitalnog vigilantizma te aktualnu problematiku s obzirom na dosadašnje spoznaje. U daljnjem tekstu će se upotrebljavati termin „digilantizam“ za naziv fenomena digitalnog vigilantizma radi lakšeg praćenja teksta.

DIGILANTIZAM - KONCEPTI I DEFINICIJE

Konceptualna usporedba digilantizma i vigilantizma uključuje i njihova objašnjenja i rizike. U smislu objašnjenja, digitalni vigilantizam i vigilantizam shvaćeni su kao reakcija na policijsku, odnosno formalno-pravnu neučinkovitost (Trottier, 2017) i nedostatak sigurnosti koju pruža država (Byrne, 2013). Ovi razlozi jasno pokazuju da se istraživanje digilantizma i vigilantizma mora usredotočiti na specifični društveni kontekst.

Digilantizam i vigilantizam također dijele rizike. Ti rizici uključuju da vigilanti i digilanti mogu „kazniti“ ili „označiti“ pogrešnu metu na temelju pogrešne identifikacije, uzrokovati nerazmjernu štetu označenoj meti ili odbiti dati meti priliku da objasni mogući razlog za svoje postupke (Jane, 2017). U tom smislu i vigilantizam i digitalni vigilantizam mogu uključivati legalne i ilegalne aktivnosti.

Različiti pristupi digilantizmu, uključujući one iz područja kibernetičke sigurnosti, kriminologije i društvenih medija, predlažu okvire vigilantizma za definiranje digitalnog vigilantizma (e Silva, 2018; Trottier, 2017; Loveluck, 2019; Tanner i Campana, 2019; Smallridge, Wagner i Crowl, 2016). Ove studije nastoje uspoređivati aktivnosti vigilantizma i digitalnog vigilantizma te identificirati sličnosti i razlike među njima. Studije o društvenim medijima definiraju digilantizam kao građane koji koordiniraju digitalnu odmazdu putem tehnoloških uređaja i stranica društvenih medija (Trottier, 2017; Gabdulhakov, 2018). Jane (2017:5) povezuje digilantizam sa zagovaranjem i aktivizmom, definirajući digilantne aktivnosti

individuals or groups use online tools and techniques to achieve what they see as justice, often without official authorisation (Powell et al., 2016; Johnston, 1996; Trottier, 2017).

The aim of this study was to provide further insight into the phenomenon of digital vigilantism. The characteristics of digital vigilantism and the current problem were analysed with respect to the current state of knowledge. In the following text, in order to make the text easier to understand, the term “digilantism” has been used to describe the phenomenon of digital vigilantism.

DIGILANTISM - CONCEPTS AND DEFINITIONS

A conceptual comparison of vigilantism and digital vigilantism encompasses both their interpretations and their risks. In terms of explanation, digital vigilante justice and vigilantism are understood as a reaction to police inefficiency, i.e., formal/legal inefficiency (Trottier, 2017), as well as the lack of state security (Byrne, 2013). These reasons clearly show that research on vigilantism and vigilante justice needs to focus on a specific social context.

Digilantism and vigilantism also share common risks. These risks include vigilantes ‘punishing’ or ‘labelling’ the wrong target based on misidentification, causing disproportionate harm to the labelled target, or refusing to give the target the opportunity to explain or provide reasoning for their actions (Jane, 2017). In this sense, both vigilantism and digital vigilantism can include legal and illegal activities.

Various approaches to vigilantism, including from the fields of cybersecurity, criminology, and social media, propose vigilantism frameworks to define digital vigilantism (e Silva, 2018; Trottier, 2017; Loveluck, 2019; Tanner & Campana, 2019; Smallridge, Wagner, & Crowl, 2016). These studies attempt to compare vigilantism and digital vigilantism activities, as well as identify the similarities and differences between them. Studies on social media define digilantism as citizens coordinating digital retaliation via technological devices and social media sites (Trottier, 2017; Gab-

kao "politički motivirane (ili percipirane politički motivirane) prakse izvan države koje imaju za cilj kazniti ili držati druge odgovornima kao odgovor na percipirani ili stvarni nedostatak institucionalnog odgovora" .

Iz kriminološke perspektive, Smallridge i sur. (2016) gledaju na digitalni vigilantizam kao na varijantu vigilantizma i upotrebljavaju Johnstonovih (1996) šest elemenata vigilantizma kao osnovu za razvoj svoje definicije. Prema Johnstonu (1996:232), vigilantizam je "društveni pokret koji dovodi do namjernih činova nasilja — ili prijetnje nasiljem — od strane autonomnih građana. Nastaje kao odgovor na kršenje institucionaliziranih normi pojedinaca ili skupina — ili na njihovu potencijalnu ili impliciranu transgresiju. Takva djela usmjerena su na prevenciju zločina i/ili društvenu kontrolu i imaju za cilj pružiti sigurnost (ili „jamstva") i sudionicima i drugim članovima određenog uspostavljenog poretka". Prema kriminološkoj perspektivi digilantizam obuhvaća niz aktivnosti sličnih vigilantizmu, a koje se provode u digitalnoj sferi s ciljem poduzimanja radnji protiv percipirane nepravde ili nepoštenosti što može uključivati *online* aktivizam, *doxxing* (otkrivanje privatnih podataka o pojedincu), hakiranje radi cilja (haktivizam) i druge oblike *cyber*-vigilantizma. Često uključuje pojedince ili skupine koji se osjećaju prisiljenima djelovati izvan utvrđenih pravnih kanala kako bi razotkrili ili kaznili počinitelje s obzirom na činjenicu kako, prema njihovoj percepciji, formalne institucije to nisu ili ne žele učiniti. Važno je napomenuti da, iako digilantizam može nastati iz istinske želje za pravdom ili društvenom promjenom, on također izaziva određene etičke probleme. Nedostatak kontrole i mogućnost zlouporabe digitalnih alata mogu dovesti do neželjenih, čak i fatalnih, posljedica i sukoba s formalnim pravnim sustavima.

Digilantizam se također može razumjeti kroz objektiv *crowdsourcinga*, gdje pojedinci udružuju svoje znanje i resurse kako bi prikupili informacije o meti. Ova kolektivna inteligencija može dovesti do brzog širenja informacija i omogućiti istrage koje pokreće zajednica, iako također može dovesti do širenja dezinformacija i naštetiti nevinim stranama (Huey i sur., 2012; Nhan i sur., 2017)

dulhakov, 2018). Jane (2017:5) links vigilantism to advocacy and activism and defines vigilante activities as "politically motivated (or perceived to be politically motivated) practises outside the state that aim to punish or hold others accountable in response to a perceived or actual lack of institutional response".

From a criminological perspective, Smallridge et al. (2016) regarded digital vigilantism as a variant of vigilantism and used Johnston's (1996) six elements of vigilantism as the basis for developing their definition. According to Johnston (1996:232), vigilantism is "a social movement that leads to deliberate acts of violence — or the threat of violence — by autonomous citizens. It arises as a reaction to the violation of institutionalised norms by individuals or groups — or to their potential or implied violation. Such acts serve crime prevention and/or social control and aim to provide security (or "guarantees") to both participants and other members of a particular established order". From a criminological perspective, digilantism encompasses a range of activities similar to vigilantism that are carried out in the digital sphere with the aim of addressing perceived injustice or dishonesty. This can include online activism, doxing (disclosing private information about an individual), hacking for a cause (hacktivism), and other forms of cyber vigilantism. It often involves individuals or groups who feel compelled to act outside established legal channels to expose or punish perpetrators because they believe that official institutions are unwilling or unable to do so. It is important to point out that while digilantism can arise from a genuine desire for justice or social change, it also raises certain ethical issues. The lack of control and the possibility of misuse of digital tools can lead to undesirable, even fatal, consequences and conflicts with formal legal systems.

Digilantism can be also understood through the lens of crowdsourcing, where individuals pool their knowledge and resources to gather information about a target. This collective intelligence can lead to the rapid dissemination of information and enable community-driven investigations, although it may also lead to the spread of misinfor-

Za snalaženje u složenom konceptu digitalnog aktivizma važno je razumjeti motive i implikacije digilantizma. Motivacija počinitelja koristan je kriterij za razlikovanje digitalnog vigilantizma od nekih drugih oblika cyberkriminaliteta kao što je primjerice *cyberbullying* (Smallridge i sur., 2016). Loveluckova definicija (2019) digitalnog vigilantizma ističe da je motivacija digilanta povezana s pravdom, redom ili sigurnošću. U tom smislu Loveluck je (2019:4) ponudio definiciju digilantizma koja odražava ciljeve i mehanizme kojima se koriste digilanti, a glasi kako su to „izravne mrežne akcije ciljanog nadzora, odvraćanja ili kažnjavanja, koje se obično oslanjaju na javno osuđivanje ili višak neželjene pažnje, a koja se provodi u ime pravde, reda ili sigurnosti".

Loveluckov koncept naglašava tri kritična elementa digitalnog vigilantizma: (1) njegovu osuđujuću prirodu (Trottier, 2019), (2) ideju građanske policije (Chang i Poon, 2017; Huey i sur., 2013), i (3) kažnjavanje (Byrne 2013; Jane, 2017; Gabdulhakov, 2018; Chang i Poon, 2017). Drugim riječima, digitalni vigilantizam ima i informativnu i kaznenu svrhu (Trottier, 2017).

Slučajeve digilantizma obično karakteriziraju spontane i nereflektirane aktivnosti, kao i koordinirane akcije. Međutim, sposobnosti društvenih platformi, poput njihove povezanosti (van Dijck i Poell, 2013.), sugeriraju da planirana koordinacija može slijediti spontanu akciju i obrnuto. Drugim riječima, neke aktivnosti mogu biti spontane, poput trenutnog snimanja i postavljanja sadržaja te dijeljenja i komentiranja tog sadržaja. Drugi aspekti, međutim, zahtijevaju promišljeno planiranje, kao što je upravljanje prisutnošću na digitalnoj platformi ili koordinacija odgovora na optužbe. Digilantizam svoje značenje crpi iz niza društvenih aktera koji ili izravno sudjeluju u događajima ili ih komentiraju. Stoga vokabular koji se koristi igra formativnu ulogu u potvrđivanju i osporavanju onoga što se smatra prihvatljivim. Na temelju toga može se zaključiti bitna točka u vezi digilantizma - to nije slučajni ili izolirani događaj, već koordinirani napad na određenog pojedinca i/ili instituciju. Neposredne posljedice, bile namjerne ili nenamjerne, mogu biti narušavanje javnog ugleda označene osobe i/ili institucije, kao

mation and harm innocent parties (Huey et, all, 2012; Nhan et al., 2017)

To navigate the complex concept of digital activism, it is important to understand the motives and effects of digital activism. The motivation of the perpetrator is a useful criterion to distinguish digital vigilantism from some other forms of cybercrime, such as cyberbullying (Smallridge et al., 2016). In Loveluck (2019), the definition of digital vigilantism indicates that the motivation of digital vigilantes has to do with justice, order, or safety. With this in mind, Loveluck (2019:4) offered a definition of digilantism that reflects the goals and mechanisms of 'digilantes': "Direct online actions of targeted surveillance, deterrence, or punishment, usually relying on public condemnation or excessive unwanted attention, carried out in the name of justice, order, or security".

Loveluck's concept emphasises three critical elements of digital vigilantism: (1) its condemnatory nature (Trottier, 2019), (2) the idea of citizen policing (Chang and Poon, 2017; Huey et al., 2013), and (3) punishment (Byrne 2013; Jane, 2017; Gabdulhakov, 2018; Chang and Poon, 2017). In other words, digital vigilantism has both an informative and a punitive purpose (Trottier, 2017).

Cases of digilantism are usually characterised by spontaneous and unreflective activities, as well as coordinated actions. However, the capabilities of social platforms, such as their connectivity (van Dijck and Poell, 2013), suggest that planned coordination can follow spontaneous action and vice versa. In other words, some activities can be spontaneous, such as the immediate recording and uploading of content and sharing and commenting on that content. Other aspects, however, require thoughtful planning, such as managing a presence on a digital platform or coordinating a response to allegations. Digilantism derives its meaning from a range of social actors who either directly participate in the events or comment on them. Therefore, the vocabulary used plays a formative role in asserting and contesting what is considered acceptable. Based on this, an important point regarding digilantism can be deduced - it is not a random or isolated event, but a coordinated attack on a spe-

i onih povezanih s njima, poput njihovih obitelji, političkih stranaka ili poslodavaca (Trotier, 2013; Trotier, 2020).

Nadalje, digitalni vigilantizam također predstavlja posebne izazove za sustav kaznenog pravosuđa. Aktivnostima digitalnih osvetnika nedostaje kontrola (Trottier, 2017; Chia, 2019) budući da ne postoje norme koje reguliraju te radnje (Chang i Poon, 2017). Digilantizam se percipira kao "bezakonje" jer digilanti ne zahtijevaju pravni autoritet za svoje postupke (Dunsby i Howes, 2019), čime digilantizam pomiče pravnu presumpciju nevinosti u korist presumpcije krivnje (Gabdulhakov, 2018). Ovaj nedostatak kontrole i regulacije u digitalnom svijetu odražava se i u širenju glasina koje u nekim slučajevima mogu dovesti do teških posljedica kao što je ubojstvo (Bakker, 2017). Budući da građani nemaju formalnu obuku o policijskim postupcima digilantne istrage mogle bi ugroziti pravne postupke, kao što su pravila o isključenju koja se odnose na nezakonito pribavljene dokaze. Ideja je građanskog policijskog rada problematična, budući da digilanti uključeni u "društvenu pravdu" također mogu biti motivirani osobnim razlozima (Chang i Poon, 2017), a ne težnjom za „pravdom".

USPON DIGILANTIZMA

Podrijetlo digilantizma može se pratiti unatrag do općeg razvoja interneta i digitalnih tehnologija. Kako je internet postao dostupniji, a platforme društvenih medija sve popularnije, pojedinci i grupe pronalazili su nove načine da izraze svoje neslaganje, traže pravdu i riješe pitanja za koja su smatrali da ih tradicionalne vlasti ne rješavaju na odgovarajući način (Castells, 2008). Internet omogućuje da velika količina informacija dopre do velikog broja ljudi u isto vrijeme. Moć, snaga i sloboda, koje je teško postići u stvarnom svijetu, motiviraju *netizene* (građani interneta, tj., *netizeni,* izvedenica od engleskim termina „Internet" i „citizen") da sudjeluju u *netilantizmu*, koji se može promatrati kao nova vrsta građanske policije. Uzbuđenje zbog promjene identiteta u *cyber* svijetu, gdje korisnici interneta mogu registrirati brojne račune (ili profile), a da drugi ne znaju njihov pravi identitet, jedan je od razloga za *netilan-*

cific individual and/or institution. The immediate consequences, whether intended or unintended, can be damage to the public reputation of the labelled person and/or institution, as well as those associated with them, such as their families, political parties, or employers (Trotier, 2013; Trotier, 2020).

Furthermore, digital vigilantism also poses particular challenges for the criminal justice system. The activities of digital vigilantes lack oversight (Trottier, 2017; Chia, 2019), since there are no norms regulating these actions (Chang and Poon, 2017). Digilantism is perceived as "lawlessness" because 'digilantes' do not require legal authorisation for their actions (Dunsby and Howes, 2019). Thus, digilantism shifts the legal presumption of innocence in favour of the presumption of guilt (Gabdulhakov, 2018). This lack of control and regulation in the digital world is also reflected in the spread of rumours, which in some cases can lead to serious consequences such as murder (Bakker, 2017). As citizens lack formal training in policing procedures, diligent investigations could jeopardise legal procedures, such as exclusionary rules regarding illegally obtained evidence. The idea of citizen policing is problematic as vigilantes who advocate for "social justice" may also be motivated by personal reasons (Chang and Poon, 2017), rather than the pursuit of "justice".

RISE OF DIGILANTISM

The origins of digilantism can be traced back to the general development of the internet and digital technologies. As the internet became more accessible and social media platforms more popular, individuals and groups found new ways to voice their dissent, seek justice, and address issues that they felt were not being adequately addressed by traditional authorities (Castells, 2008). The Internet allows for a large amount of information to reach many people simultaneously. Power, strength, and freedom that are difficult to achieve in the real world motivate netizens (citizens of the internet, i.e., netizens, a derivation of the English terms "Internet" and "citizen") to participate in 'netilantism', which can be seen as a new kind of civil police. The excitement of changing identi-

tizam (Chang i Poon, 2017; Fei-Yue, Zeng, Hendler, Zhang, Feng, Gao, Wang i Lai, 2010; Kling, 2000). *Online* platforme omogućuju i olakšavaju digilantizam kroz sposobnost internetskih tražilica da ljudima olakšaju pristup većini internetskih informacija kako bi dodatno kaznili društvene prijestupnike provođenjem virtualnog suđenja (Zook i Graham, 2007.)

Znanstvenici i stručnjaci u području računalnog kriminaliteta i računalne sigurnosti slažu se da tradicionalne policijske ovlasti više nisu dovoljne za istraživanje računalnog kriminaliteta i osiguravanje internetske sigurnosti (Broadhurst i Chang, 2013; Chang, 2012) pa je hitno potrebno uvođenje distribuiranog modela „računalne policije" ili *wikificiranog* modela za istraživanje računalnog kriminala (Brenner, 2007; Chang, 2013). Međutim, kako obični građani nisu formalno obučeni o policijskim metodama, uključujući prikupljanje dokaza i zaštitu prava građana, netilantizam bi mogao ugroziti i olakšati društvenu pravdu.

Porastu digilantizma može se pripisati nekoliko čimbenika (Barthel i Harrison, 2009; Barak, Nissim i Suler, 2008; Suler, 2004; Jenkins, 2006):

a) Osnaživanje kroz tehnologiju - pristupačnost digitalnih alata i platformi omogućuje pojedincima prikupljanje informacija, mobilizaciju podrške i poduzimanje radnji. Ovo tehnološko osnaživanje dovelo je do novog oblika aktivizma koji nadilazi geografske granice.

b) Anonimnost i učinak dezinhibicije - relativna anonimnost koju nudi internet omogućuje pojedincima da djeluju bez straha od neposrednih posljedica. To može dovesti do učinka dezinhibicije koji rezultira time da se ljudi upuštaju u ekstremnije ili odvažnije akcije na mreži nego što bi to učinili u izvanmrežnom okruženju.

c) Uloga društvenih medija - platforme društvenih medija pružaju globalnu pozornicu za pitanja i pritužbe. Aktivisti, haktivisti i ostali digilanti koriste se ovim platformama za podizanje svijesti, organiziranje kampanja i vršenje pritiska na pojedince, tvrtke ili institucije.

d) Uspon računalnog aktivizma – Međupovezanost digitalnog svijeta potaknula je računalne aktivnosti u kibernetičkom svijetu, gdje korisnici interneta mogu registrirati brojne račune (ili profile) bez da drugi znaju njihov pravi identitet, jedan je od motiva za 'netilantism' (Chang and Poon, 2017; Fei-Yue, Zeng, Hendler, Zhang, Feng, Gao, Wang and Lai, 2010; Kling, 2000). Online platforms enable and facilitate digilantism through the ability of internet search engines to facilitate access to more information in order to further punish social offenders by conducting virtual trials (Zook and Graham, 2007).

Scholars and experts in the field of cybercrime and cybersecurity agree that traditional police powers are no longer sufficient to investigate cybercrime and ensure internet security (Broadhurst and Chang, 2013; Chang, 2012), leading to the introduction of a distributed "computer police" model or the Wikipedia model for cybercrime research (Brenner, 2007; Chang, 2013). However, as ordinary citizens are not formally trained in policing methods, including evidence collection and the protection of citizens' rights, 'netilantism' could both threaten and facilitate social justice.

The rise of digitalisation can be attributed to several factors (Barthel and Harrison, 2009; Barak, Nissim and Suler, 2008; Suler, 2004; Jenkins, 2006):

a) Empowerment through technology - access to digital tools and platforms enable individuals to gather information, mobilise support, and act. This technological empowerment has led to a new form of activism that transcends geographical boundaries.

b) Anonymity and disinhibition effect - the relative anonymity offered by the Internet allows individuals to act without fear of immediate consequences. This can lead to a disinhibition effect that results in people engaging in more extreme or daring actions online than they would in an offline environment.

c) Role of social media - Social media platforms provide a global stage for issues and complaints. Activists, hacktivists, and other 'digilantes' use these platforms to raise awareness, organise campaigns, and put pressure on individuals, companies, or institutions.

nalnu aktivnost, gdje se pojedinci koriste svojim tehnološkim vještinama za promicanje društvenih ili političkih ciljeva. Ovaj aktivizam može imati različite oblike, od razotkrivanja korupcije do zagovaranja socijalne pravde.

Iako je oduvijek bilo moguće osuditi druge za njihove postupke, digilantizam podrazumijeva aktivno i pasivno sudjelovanje pojedinaca i različitih vrsta organizacija. Današnje medijske kulture dopuštaju gotovo svakome da manipulira i iskorištava vidljivost mete za niz društvenih, kulturnih, ekonomskih i političkih svrha. Digilantizam se stoga može opisati i kao mračna strana *online* angažmana kroz srodne prakse kao što su *vitriol* (eng., vitriol, najbliži prijevod bi bio govor mržnje ili otrovni sarkazam) ili *trolanje* (orig., trolling, namjerno ostavljanje zlonamjernih komentara na digitalnim platformama s ciljem izazivanja uznemirenosti kod čitatelja). Međutim, ključna je briga u ovom području to što digitalni vigilantizam nije samo problematičan ili devijantan. Umjesto toga, može se shvatiti kao standardizirani način komunikacije koji može naići na podršku javnosti pod određenim uvjetima što može dovesti do još jednog shvaćanja digilantizma - oblik organiziranja pojedinaca i institucija koji skreću pozornost na druge i upotrebljavaju ga za vlastitu korist (Trotier, 2019).

TEORIJSKA I KONCEPTUALNA OBJAŠNJENJA DIGILANTIZMA

Digitalni vigilantizam rastući je fenomen u kojem se pojedinci ili grupe koriste digitalnim platformama za provođenje pravde, razotkrivanje počinitelja ili kažnjavanje navodnih prijestupnika izvan formalnog pravnog sustava. Ova praksa djeluje na raskrižju nekoliko teorijskih i konceptualnih okvira, uključujući teoriju kolektivne akcije, društvenu kontrolu i *online* dezinhibicijski učinak. Ovi okviri pomažu objasniti kako i zašto se pojedinci mobiliziraju na internetu u digilantne aktivnosti, etičke dileme koje se javljaju kao produkt tih aktivnosti i društveni učinak takvih radnji. Analizirajući digilantizam kroz ove leće, dobivamo uvid u dinamiku moći, kulturne norme i psihološke čimbenike koji promiču ovaj sve prevladavajući oblik digitalne pravde.

d) Rise of computer activism – The interconnectedness of the digital world has led to computer activism, where individuals use their technological skills to promote social or political goals. This activism can take on various forms, from exposing corruption to advocating for social justice.

Although it has always been possible to condemn others for their actions, digilantism presupposes the active and passive participation of individuals and various types of organisations. Today's media culture allows almost anyone to manipulate and exploit a target's visibility for a variety of social, cultural, economic, and political purposes. Digilantism can therefore also be described as the dark side of online engagement through related practises such as vitriol (Eng., vitriol, the closest translation would be hate speech or toxic sarcasm) or trolling (orig., trolling, deliberately leaving malicious comments on digital platforms with the aim of unsettling the reader). However, an important concern in this area is that digital vigilantism is not just problematic or deviant. Instead, it can be understood as a standardised way of communicating that can gain public support under certain conditions, which can lead to a different understanding of digilantism - a form of organising individuals and institutions to draw attention to others and use it to their own advantage (Trottier, 2019)

THEORETICAL AND CONTEXTUAL EXPLANATIONS OF DIGILANTISM

Digital vigilantism is a growing phenomenon in which individuals or groups use digital platforms to enforce justice, expose wrongdoers, or punish alleged offenders outside the formal legal system. This practise operates at the intersection of several theoretical and conceptual frameworks, including collective action theory, social control, and the online disinhibition effect. These frameworks help to explain how and why individuals mobilise online to engage in vigilantism, as well as the ethical dilemmas and social impact of such actions. By analysing digilantism through these lenses, we gain insight into the power dynamics, cultural norms, and psychological factors that promote this increasingly prevalent form of digital justice.

Teorija društvene kontrole tvrdi da se društveni poredak održava kroz neformalne društvene kontrole i zajedničke norme. U kontekstu digilantizma, pojedinci mogu osjećati snažan osjećaj moralne obveze da djeluju protiv uočenih nepravdi, osobito kada se formalne vlasti smatraju neučinkovitima. Uključivanjem u digitalni vigilantizam vjeruju da provode društvene norme i smatraju počinitelje odgovornima (Trottier, 2017; Cheong i Gond, 2010).

Teorija kolektivnog djelovanja naglašava ulogu kolektivnog ponašanja u postizanju zajedničkih ciljeva. U digilantizmu se internetske zajednice često brzo mobiliziraju kako bi odgovorile na pritužbe, koristeći se društvenim medijima kako bi prikupile podršku i pojačale svoju poruku (Van Laer, 2014; Loveluck, 2019; Kavada, 2015). Kolektivni bijes može motivirati pojedince da sudjeluju u *online* kampanjama sramoćenja ili uznemiravanja (Cheong i Gong, 2010; Krim, 2005).

Digilantizam se također može razumjeti kroz objektiv crowdsourcinga, gdje pojedinci udružuju svoje znanje i resurse kako bi prikupili informacije o meti. Ova kolektivna inteligencija može dovesti do brzog širenja informacija i omogućiti istrage vođene zajednicom, iako također može dovesti do širenja dezinformacija i naštetiti nevinim stranama (Huey et al., 2012.; Nhan et al., 2017.)

U nekim se kontekstima digilantizam javlja kao odgovor na uočene nepravde u formalnom pravosudnom sustavu (Cheong i Gong, 2010). Oni koji se osjećaju marginalizirano ili obespravljeno mogu se okrenuti digitalnim platformama u potrazi za pravdom, vjerujući da su ih tradicionalni načini iznevjerili. To naglašava ulogu digitalnog jaza, budući da pristup tehnologiji i internetskim platformama može osnažiti pojedince da traže alternativne oblike pravde (Trottier, 2019.; Van Laer, 2014.).

Internetsko okruženje često pruža razinu anonimnosti koja može dovesti do učinka dezinhibicije, gdje se pojedinci ponašaju onako kako možda ne bi razmišljali u interakcijama licem u lice. To može potaknuti agresivne ili štetne radnje protiv percipiranih počinitelja, budući da nedostatak neposrednih posljedica može ohrabriti osvetničko

Social control theory posits that social order is maintained through informal social controls and shared norms. In the context of digilantism, individuals may feel a strong sense of moral obligation to act against perceived injustices, particularly when formal authorities are seen as ineffective. By engaging in digital vigilantism, these individuals believe that they are enforcing social norms and holding offenders accountable (Trottier, 2017; Cheong and Gond, 2010).

The Collective Action theory emphasises the role of collective behaviour in achieving shared goals. In digilantism, online communities often mobilise quickly to address grievances and they leverage social media to rally support and amplify their message (Van Laer, 2014; Loveluck, 2019; Kavada, 2015). The collective outrage can motivate individuals to participate in online shaming or harassment campaigns (Cheong and Gong, 2010; Krim, 2005).

Digilantism can be also understood through the lens of crowdsourcing, where individuals pool their knowledge and resources to gather information about a target. This collective intelligence can lead to the rapid dissemination of information and enable community-driven investigations, although it may also lead to the spread of misinformation and harm innocent parties (Huey et al., 2012; Nhan et al., 2017)

In some contexts, digilantism emerges as a response to perceived injustices in the formal justice system (Cheong and Gong, 2010). Those who feel marginalised or disenfranchised may turn to digital platforms to seek justice, believing that traditional avenues have failed them. This underscores the role of the digital divide, as access to technology and online platforms can empower individuals to pursue alternative forms of justice (Trottier, 2019; Van Laer, 2014).

The online environment often provides a level of anonymity that can lead to a disinhibition effect, where individuals engage in behaviours that they might not consider in face-to-face interactions. This can encourage aggressive or harmful actions against perceived wrongdoers, since the lack of immediate consequences can embolden vigilante

ponašanje (Suler, 2004; Chang i Poon, 2017; Zimmerman i Ybarra, 2016).

Digilantizam se može promatrati kao reakcija na neravnoteže moći, gdje pojedinci ili grupe pokušavaju povratiti moć ciljajući na one koje doživljavaju kao tlačitelje ili zločince. To odražava šira društvena pitanja nejednakosti, gdje se marginalizirani glasovi nastoje potvrditi u sustavu koji smatraju nepravednim (Trottier, 2017).

Kulture i etički okviri mogu oblikovati prihvaćanje i prevalenciju digilantizma. U nekim je društvima kolektivna akcija protiv percipiranih počinitelja društveno prihvatljivija, dok se u drugima može smatrati neetičkom ili kontraproduktivnom (Chang i sur., 2016; Gies i Bortoluzzi, 2021).

Ukratko, digitalni vigilantizam složen je i višeslojan fenomen koji se prožima s različitim teorijskim i konceptualnim okvirima. Uspon digilantizma često je potaknut uočenim propustima pravosudnog sustava, neravnotežom moći i kulturnim normama, pri čemu sudionici vjeruju da podržavaju društvene vrijednosti pozivajući na odgovornost počinitelje. Međutim, to izaziva značajna etička pitanja, kao što je mogućnost dezinformacija, nanošenje štete nevinim osobama i dezinhibicija uzrokovana anonimnošću. S porastom digilantizma, ključno je razumjeti njegov utjecaj na pravdu, moć i društveni poredak. To je osobito istinito jer odražava šira pitanja nejednakosti i uloge digitalnih platformi u oblikovanju moderne pravde.

TIPOLOGIJA DIGILANTIZMA

Loveluck (2019:2-15) pruža najdetaljniju studiju i tipologizaciju digilantizma, analizirajući oko 50 različitih slučajeva digitalnog vigilantizma iz različitih dijelova svijeta i dijeleći prakse digilanata u četiri kategorije: **označavanje** (orig., flagging), **istraživanje** (orig., investigating), **uhođenje** (orig., hounding) i **organizirano curenje podataka** (orig., organized leaking).

Označavanje je kategorija niskog intenziteta u kojoj se posramljuje ponašanje bez pružanja svih potrebnih informacija ili se informacije o određenoj meti prikazuju ciljano manjkave. Obično se provodi dijeljenjem slika ili tekstova o nedo-

behaviour (Suler, 2004; Chang and Poon, 2017; Zimmerman and Ybarra, 2016).

Digilantism can be seen as a reaction to power imbalances, where individuals or groups attempt to reclaim power by targeting those they perceive as oppressors or wrongdoers. This reflects broader societal issues of inequality, where marginalised voices seek to assert themselves in a system they view as unjust (Trottier, 2017).

Diversity in culture and ethical frameworks can shape the acceptance and prevalence of digilantism. In some societies, collective action against perceived wrongdoers is more socially acceptable, while in others, it may be viewed as unethical or counterproductive (Chang et. al., 2016; Gies and Bortoluzzi, 2021).

To summarise, digital vigilantism is a complex and multi-layered phenomenon that intersects with various theoretical and conceptual frameworks. The rise of digilantism is often fuelled by perceived failures of the justice system, power imbalances and cultural norms, with participants believing that they are upholding societal values by holding wrongdoers accountable. However, this raises significant ethical concerns, such as the potential for misinformation, harm to the innocent, and disinhibition caused by anonymity. With the rise of digilantism, it is crucial to understand its impact on justice, power, and social order. This is especially true as it reflects broader issues of inequality and the role of digital platforms in shaping modern justice.

TYPOLOGY OF DIGILANTISM

Loveluck (2019:2-15) offers the most detailed study and typology of digilantism by analysing about 50 different cases of digital vigilantism from different parts of the world and dividing the practises of digilantes into four categories: flagging, investigating, hounding (or stalking), and organised leaking.

Flagging or labelling is a low-intensity category in which a behaviour is shamed without providing all the necessary information, or in which information about a particular target is presented as intentionally deficient. This is usually done by

ličnom ponašanju popraćenog slikama ili drugim „dokazima“. Tipični slučajevi uključuju kršenje pravila parkiranja, vandalizam, kršenje pisanih i nepisanih normi i slično. Istraživanje uključuje imenovanje, traženje i pružanje informacija za identifikaciju mete koja je prekršila pravilo. Korak dalje od istražnih praksi je uhođenje, koje “ne samo da […] kombinira istražnu dimenziju s kaznenom dimenzijom, već uključuje i dugotrajniju mobilizaciju protiv određene mete, potaknutu intenzivnim bijesom” (Loveluck, 2019:15). Naposljetku, organizirano curenje obično se fokusira na sustavne probleme, cilja posebno na institucije i organizacije i uključuje dobro strukturiranu organizaciju za prikupljanje dokaza i prosljeđivanje inkriminirajućih informacija (Loveluck, 2019:22).

Iako ova podjela uvelike supsumira fenomenologiju digilantizma, napretkom tehnologije pojavili su se još neki od oblika koji mogu uključivati jedan ili više aspekata digilantizma prema Loveluckovoj podjeli.

Doxxing je praksa istraživanja i objavljivanja privatnih ili identificiranja podataka o pojedincu ili organizaciji na internetu bez njihova pristanka (Anderson i Wood, 2022). Ove informacije mogu uključivati prava imena, adrese, telefonske brojeve, adrese e-pošte, brojeve osiguranja, financijske informacije i druge osobne podatke koje su uobičajeno nedostupne široj javnosti. Izraz “doxxing” izveden je iz riječi “dokumenti” (orig., documents) i potječe iz internetske kulture. Često se rabi kao oblik internetskog uznemiravanja, osvete ili zastrašivanja. Velik dio akademske literature o *doxxingu* ispituje tu praksu kao oblik digilantizma, tj., kao jednu od mnogih aktivnosti sličnih vigilantizmu koje se provode putem interneta (Colton, Holmes i Walwema, 2017; Marwick, 2013; Phillips 2011; Trottier, 2020). Iako se *doxxing* ponekad povezuje s digilantizmom aktivista koji žele otkriti identitet ili lokaciju političkih protivnika (Mohammed, 2017), također se može potaknuti raznim drugim motivacijama (Anderson i Wood, 2021), što uključuje ucjenu (Khanna, Zavarsky i Lindskog, 2016), smanjenje prisutnosti pojedinaca ili institucija na digitalnim platformama (Jones, 2016), kontrola ili upravljanjem tuđim ponašanjem (Freed, Palmer, Minc-

sharing images or text about misbehaviour, accompanied by pictures or other “evidence”. Typical cases include parking violations, vandalism, violations of written and unwritten standards, and so on. Investigations involve naming, searching, and providing information in order to identify a target who has violated a rule. One step beyond investigative practises is stalking, which “not only [...] combines an investigative dimension with a criminal dimension, but also involves a longer-term mobilisation against a specific target, fuelled by intense anger” (Loveluck, 2019:15). Hounding involves investigation with a punitive intent, or more precisely, with the intent of naming and shaming. Finally, organised leaking tends to focus on systemic problems, targeting institutions and organisations, and involves a well-structured organisation for gathering evidence and sharing incriminating information (Loveluck, 2019:22).

Although this categorisation largely summarises the phenomenology of digilantism, with the advance of technology, some other forms have emerged that may include one or more aspects of digilantism according to the categorisation in Loveluck (2019).

Doxing is the practise of researching and publishing private or identifying information about an individual or organisation on the internet without their consent (Anderson and Wood, 2022). This information can be real names, addresses, phone numbers, email addresses, insurance numbers, financial data, and other personal information that is not typically available to the public. The term “doxing” is derived from the word “documents” and comes from internet culture. It is often used as a form of online harassment, revenge, or intimidation. Much of the academic literature on doxing examines the practise as a form of vigilantism, i.e., one of many vigilantism-like activities conducted over the Internet (Colton, Holmes, & Walwema, 2017; Marwick, 2013; Phillips 2011; Trottier, 2020). Although doxing is sometimes associated with activism by activists seeking to uncover the identity or location of political opponents (Mohammed, 2017), it can also be driven by a variety of other motivations (Anderson and Wood,

hala, Levy, Ristenpart i Dell, 2018; Dragiewicz, Burgess, Matamoros-Fernandez, Salter, Suzor, Woodlock i Harris, 2018), odmazdu i narušavanje ugleda (Massanari, 2017; Trottier, 2020), objavljivanje informacija percipiranih kao javni interes (Colton, i sur., 2017) i nenamjerno objavljivanje informacija o drugima (McNealy, 2017).

Doxxing može imati razne negativne posljedice za označenu metu, uključujući uznemiravanje, uhođenje, krađu identiteta, gubitak posla, pa čak i fizičku ozljedu. Mnoge platforme društvenih medija i internetskih stranica imaju pravila protiv *doxxinga* i mogu suspendirati ili zabraniti pristup korisnicima koji se bave takvim ponašanjem.

Online **posramljivanje (orig.,** ***online shaming*****)** odnosi se na fenomen u kojem se pojedinci ili grupe mogu koristiti platformama društvenih medija da javno posrame nekoga za koga vjeruju da je počinio prekršaj. To može uključivati objavljivanje snimaka zaslona, osobnih podataka ili drugih detalja kako bi se potaknulo druge da djeluju protiv navodnog počinitelja. Na primjer, De Vries (2015.) upotrijebio je šest fokusnih grupa kako bi istražio kako učenici percipiraju iskustvo posramljivanja na internetu. Rezultati su pokazali da studenti vjeruju da određene radnje privlače pozornost javnosti kako bi potaknule promjenu ponašanja (De Vries, 2015). Arvanitidis (2016:23) naglašava da je vrijeđanje i javno sramoćenje slično "životu u virtualnom zatvoru – bez pravila, propisa ili zaštite od zlostavljanja". Međutim, posramljivanje na internetu također može dovesti do sinergije nacionalizma, populizma i mizoginije. Istraživanje koje je proveo Huang (2023) pokazalo je da posramljivanje putem interneta može dovesti do nacionalističkog digitalnog vigilantizma, gdje je bijes ljudi usmjeren ne samo na pojedince, već i na „neprijateljske" vlade, apstraktne koncepte ili proizvode. Nadalje, može dovesti i do rodno obilježene populističko-nacionalističke mobilizacije (Huang, 2023; Volkova, Lukyanova i Kulakova, 2022), što internetskom posramljivanju daje još jednu dimenziju koju je potrebno dodatno istražiti.

Haktivizam je relativno nova konstrukcija, ali i pojava, nastala kombinacijom riječi haker i aktivist (Betlej, 2023), a često se naziva i "elek-

2021), including blackmail (Khanna, Zavarsky, & Lindskog, 2016), reducing the presence of individuals or institutions on digital platforms (Jones, 2016), controlling or directing the behaviour of others (Freed, Palmer, Minchala, Levy, Ristenpart, & Dell, 2018; Dragiewicz, Burgess, Matamoros-Fernandez, Salter, Suzor, Woodlock, & Harris, 2018), retaliation and defamation (Massanari, 2017; Trottier, 2020), disclosure of information deemed to be in the public interest (Colton, et al., 2017), and the unintentional disclosure of information about others (McNealy, 2017).

Doxing can have a variety of negative consequences for the tagged target, including harassment, stalking, identity theft, loss of employment, and even physical harm. Many social media platforms and websites have policies against doxing and can suspend or block users who engage in such behaviour.

Online shaming refers to the phenomenon where individuals or groups can use social media platforms to publicly shame someone who they believe has committed an offence. This may include posting screenshots, personal information, or other details to encourage others to act against the alleged offender. For example, De Vries (2015) used six focus groups to investigate how students perceive the experience of feeling shame or being shamed by others online. The results showed that students believe that certain actions attract public attention to encourage behavioural change (De Vries, 2015). Arvanitidis (2016:23) emphasised that insulting and public shaming is akin to "living in a virtual prison – without rules, regulations or protection from abuse". However, online shaming can also lead to a synergy of nationalism, populism, and misogyny. Research conducted by Huang (2023) showed that online shaming can lead to a nationalist digital vigilantism, where the anger of the people is directed not only to individuals, but also to the "enemy" governments, abstract concepts, or products. Furthermore, it can also lead to gendered populist-nationalist mobilisation (Huang, 2023; Volkova, Lukyanova and Kulakova, 2022), which gives online shaming another dimension that needs to be studied further.

tronička građanska neposlušnost" (orig., Electronic Citizen Disobedience). Pojam haktivizam prvi je upotrijebila grupa "Cult of the Dead Cow" (cDc) 1996 (Betlej, 2014). Mediji su popularizirali izraz 'haktivizam' tijekom sukoba na Kosovu 1998.-1999., kada su aktivisti iz cijelog svijeta pokrenuli tzv., Denial of Service (u daljnjem tekstu DoS) napade i uništili ili preuzeli mnoge internetske stranice prosvjedujući protiv rata na Kosovu i uključenih zemalja. No haktivizam se u potpunosti razvio tek početkom 21. stoljeća, uglavnom kroz aktivistički i hakerski kolektiv 'Anonymous', labavo organizirana međunarodna mreža aktivista i haktivista koji je osnovan 2003. Neke skupine se bave haktivizmom, tj., koriste se tehnikama hakiranja kako bi dobili neovlašten pristup sustavima ili informacijama i razotkrili ono što smatraju korupcijom ili neetičkim ponašanjem od kojih je najpoznatija skupina. Dva su najčešća oblika haktivizma narušavanje mrežne stranice i napadi uskraćivanjem usluge. Postoje dva oblika napada uskraćivanjem usluge: uskraćivanje usluge (DoS), koji uključuje jednog napadača ili grupu, i distribuirani napadi uskraćivanja usluge (orig., Distributed Denial of Service, u daljnjem tekstu DDoS), koji uključuju više izvora napada (Chowriwar, Madhulika, Prajyoti, Parpelli i Sambhe, 2014; Ghazali i Hassan 2011). Neke skupine provode DoS i DDoS napade na mrežne stranice ili internetske usluge za koje smatraju da se neetično ponašaju. Bez obzira na motivaciju za ovakvom vrstom ometanja rada ciljanih platformi DoS i DDoS, napadi su nezakoniti i mogu uzrokovati kolateralnu štetu.

Haktivizam se obično tumači kao neka vrsta kombinacije hakiranja i društveno-političke aktivnosti (Ireland, 2022), odnosno kao manifestacija *online* samoorganizacije, društvene mobilizacije usmjerene na postizanje specifičnih ciljeva za opće društveno dobro. Ove aktivnosti stoga imaju za cilj donijeti određene društvene promjene. Danas se haktivizam definira i kao kulturni i civilizacijski pokret koji se sastoji od kombiniranja političkog aktivizma s tehnološkim dostignućima kako bi se manifestirao otpor prema djelovanju u prostoru općenito shvaćene politike (Coleman, 2014). Fokus je na drugom aspektu ovih inicijati-

Hacktivism is a relatively new construct, but also a phenomenon created by combining the words 'hacker' and 'activist' (Betlej, 2023), and it is often referred to as "electronic citizen disobedience" (orig., Electronic Citizen Disobedience). The term 'hacktivism' was first used by the group "Cult of the Dead Cow" (cDc) in 1996 (Betlej, 2014). The media popularised the term 'hacktivism' during the Kosovo conflict in 1998-1999, when activists from around the world launched so-called Denial of Service (DoS) attacks and destroyed or took over many websites protesting against the war in Kosovo and the countries involved. However, hacktivism developed further at the beginning of the 21st century, mainly through the activist and hacker collective 'Anonymous', a loosely organised international network of activists and hacktivists founded in 2003. Some groups engage in hacktivism, which is the use of hacking techniques to gain unauthorised access to systems or information in order to expose what they believe to be corruption or unethical behaviour for which the group is best known. The two most common forms of hacktivism are website defacement and denial of service attacks. There are two forms of denial of service attacks: Denial of service (DoS), which involves a single attacker or group, and distributed denial of service (DDoS) attacks, which involve multiple attack sources (Chowriwar, Madhulika, Prajyoti, Parpelli, and Sambhe, 2014; Ghazali and Hassan 2011). Some groups carry out DoS and DDoS attacks against websites or internet services that they believe are behaving unethically. Regardless of the motivation behind this type of disruption of targeted platforms, DoS and DDoS attacks are illegal and can cause collateral damage.

Hacktivism is usually interpreted as a kind of combination of hacking and socio-political activity (Ireland, 2022), i.e., a manifestation of online self-organisation and social mobilisation aimed at achieving specific goals for the general social good. These activities thus aim to bring about certain social changes. Today, hacktivism is also defined as a cultural and civilisational movement that consists of combining political activism with technological achievements to manifest resistance

va, odnosno kriminalnim aktivnostima u kibernetičkom prostoru (Banks, 2017; Beck, 2016).

Cyber crowdsourcing, poznat na kineskom kao "renrou sousou", doslovno "potraga za ljudskim mesom" (orig., Human Flesh Search, u daljnjem tekstu HFS), prvi se put pojavio na području Narodne Republike Kine početkom 2000-ih te je zahvatio područje tzv., Velike Kine, tj. Narodnu Republiku Kinu, Hong Kong i Republiku Kinu (Tajvan). Najlakše ga je opisati kao vrstu kolektivne *online* akcije usmjerene na pronalaženje činjenica o određenim događajima i/ili objavljivanje detalja o određenoj osobi (Cheung, 2009; Herold, 2011; Ong, 2012). Uključuje praćenje i objavljivanje informacija na internetu koje bi mogle pomoći u rješavanju zločina ili otkriti osobne podatke o pojedincu koji je navodno sudjelovao u korupciji ili neetičkom ponašanju (Ong, 2012). Ovaj oblik oblik digilantizma temelji se na opisanom konceptu netilantizma te može imati više oblika djelovanja. Primjerice, kampanje uznemiravanja putem interneta oblik je u kojem pojedinci ili grupe mogu pokrenuti *online* kampanje uznemiravanja protiv osobe ili organizacije za koju vjeruju da je učinila nešto loše. To mogu biti koordinirani napori da se računi društvenih medija preplave negativnim komentarima, lažnim optužbama ili drugim oblicima digitalnog zlostavljanja. Nadalje, može uključivati širenje lažnih optužbi ili glasina o pojedincima ili organizacijama, putem društvenih medija, internetskih foruma ili drugih digitalnih kanala i može dovesti do štete po ugled ili nekog drugog oblika štete. Također se može upotrebljavati za identifikaciju pojedinaca u događajima koji privlače pozornost javnosti, kao što su ljubavne afere slavnih. Chang i Poon (2015) tvrde da netizen koji se uključi u digilantizam 1) percipira formalni pravosudni sustav kao neučinkovit i stoga nastoji postići društvenu pravdu popravljajući nedostatke u tom sustavu; 2) vjeruje da on ili ona ima sposobnost poboljšati društvo djelujući kao neformalni pas čuvar društva; i 3) upotrebljava internet i platforme društvenih mreža kao novo sredstvo za postizanje socijalne pravde i kažnjavanje devijanata koji bježe formalnom pravosudnom sustavu.

to action in the space of commonly understood politics (Coleman, 2014). The focus is on another aspect of these initiatives, namely criminal activity in cyberspace (Banks, 2017; Beck, 2016).

Cyber crowdsourcing, known in Chinese as "renrou sousou", literally "search for human flesh" (orig., Human Flesh Search, hereafter referred to as HFS), first appeared on the territory of the People's Republic of China in the early 2000s and conquered the so-called Greater China, i.e., the People's Republic of China, Hong Kong and the Republic of China (Taiwan). It can be most simply described as a kind of collective online action aimed at finding facts about specific events and/or publishing details about a specific person (Cheung, 2009; Herold, 2011; Ong, 2012). It involves tracking down and publishing information online that could help solve a crime or reveal personal information about an individual who has allegedly engaged in corrupt or unethical behaviour (Ong, 2012). This form of digilantism is based on the previously described concept of 'netilantism' and can take on various forms. Internet harassment campaigns, for example, are a form in which individuals or groups can launch online harassment campaigns against an individual or organisation who they believe has done something wrong. These can be coordinated efforts to flood social media accounts with negative comments, false accusations, or other forms of digital abuse. It may also involve the spreading of false accusations or rumours about individuals or organisations via social media, online forums, or other digital channels, which may result in reputational or other harm. It can also be used to identify individuals in events that attract public attention, such as celebrity love affairs. Chang and Poon (2015) argued that a netizen who engages in digilantism 1) perceives the formal justice system as ineffective and therefore, seeks to achieve social justice by correcting the system's flaws; 2) believes that he or she has the ability to improve society by acting as an informal watchdog of society; and 3) uses the Internet and social networking platforms as a new means to achieve social justice and punish deviants who escape the formal justice system.

Izvorno, HFS je bio samo mala grupa ljudi koji su tražili informacije o određenim incidentima, ali sada je više poput online lova na ljude (u tom smislu se često koristi izraz „man hunt“ ili „head hunt“). Veliki broj uključenih korisnika interneta učinio ga je alatom sposobnim za cenzuru i kažnjavanje ponašanja koje se smatra društveno nemoralnim, necivilizirani ili nezakonitim. HFS se temelji na ideji da je osoba koja se koristila internetom sigurno ostavila tragove koje drugi mogu otkriti. Korisnici interneta koji se bave *cyber crowdsourcingom*, odnosno HFS-om, opisani su kao najtalentiraniji detektivi i bolji od FBI-a kada je riječ o pronalaženju kriminalaca (Xiao, 2011)

Iako HFS može pružiti koristi i prilike, postoje i negativni učinci koje ne treba zanemariti. Većina korisnika interneta dobrovoljno sudjeluje u HFS-u jer vjeruju da je njihova odgovornost pomoći u održavanju socijalne pravde (Liu i Hao, 2009). HFS ponekad uključuje crno-bijelo moralno prosuđivanje bez brige o temeljnim detaljima incidenta (Chen, 2009). Korisnici interneta također mogu koristiti HFS za manipuliranje razumijevanjem drugih korisnika interneta o određenim problemima davanjem lažnih informacija ili širenjem glasina. Zbog različitih motiva korisnika interneta, pružene informacije mogu u početku biti selektivne ili pristrane (Liu i Ling, 2012; Hao, 2009; Chen, 2011). To može uključivati ispitivanje javno dostupnih informacija, analizu slika ili videozapisa i dijeljenje rezultata na internetu. Iako to može dovesti do otkrivanja legitimnih problema, također izaziva zabrinutost zbog dezinformacija i potencijalne štete nevinim ljudima. Također, takve aktivnosti mogu dovesti do invazije na privatnost, lažnih optužbi i uplitanja u službene postupke provedbe zakona.

Još jedna aktivnost koja svoje korijene vuče daleko prije pojave interneta jest ***swattting***. To je opasan oblik digitalne osvetničke pravde u kojem netko lažno prijavljuje ozbiljan incident, kao što je situacija s taocima ili nasilni zločin, na lokaciji označene mete, kojim se agencije za provođenje zakona prevare da nepotrebno rasporede svoje specijalne jedinice (orig., SWAT - Special Weapons and Tactics) kao rezultat zlonamjerne pri-

Originally, HFS involved a small group of people looking for information about specific incidents, but now, it is more of an online manhunt (the term “manhunt” or “headhunt” is often used in this sense). The large number of internet users involved in HFS has made it a tool capable of censoring and punishing behaviour that is considered socially immoral, uncivilised, or illegal. HFS is based on the idea that a person who has used the Internet must have left traces that others can discover. Internet users who engage in cyber crowdsourcing or HFS have been described as the most talented detectives, even better than the Federal Bureau of Investigation (FBI), when it comes to finding criminals (Xiao, 2011).

Although HFS can offer benefits and opportunities, there are also negative effects that should not be overlooked. Most internet users voluntarily participate in HFS because they believe it is their responsibility to help maintain social justice (Liu and Hao, 2009). HFS sometimes involves a black and white moral judgement without caring about the underlying details of the incident (Chen, 2009). Internet users can also use HFS to manipulate other users’ understanding of certain issues by providing false information or spreading rumours. Due to the different motives of internet users, the information provided may initially be selective or biased (Hao, 2009; Chen, 2011). This may include checking publicly available information, analysing images or videos, and sharing the results online. While this may lead to the discovery of legitimate problems, it also raises concerns about misinformation and potential harm to innocent people. In addition, such activities can lead to invasion of privacy, false accusations, and interference with official law enforcement efforts.

Another activity that has taken root well before the advent of the Internet is swatting. Swatting is a dangerous form of digital law enforcement in which someone falsely reports a serious incident, such as a hostage situation or violent crime, at the location of a specific target, causing law enforcement to unnecessarily deploy their Special Weapons and Tactics (SWAT) units, because of malicious deception (Enzweiler, 2015). This not only jeopardises the target, but also wastes valuable

jevare (Enzweiler, 2015). To ne samo da dovodi metu u opasnost, već i gubi dragocjene resurse i može imati ozbiljne pravne posljedice. Počinitelji su motivirani da počine napade iz osvete drugom hakeru, iz zabave, dosade ili kao obred prijelaza među određene hakerske skupine (Romaniuk i Lorenzo, 2023). FBI procjenjuje da se godišnje održi 400 ovakvih poziva (Statt, 2017). Ovi pozivi neopravdano troše policijske resurse i FBI procjenjuje da prosječni prijevarni poziv košta policiju oko 10.000 dolara (McCartney, 2013).

ETIČKI I KAZNENOPRAVNI IZAZOVI DIGILANTIZMA

Ako pogledamo dosadašnje specifičnosti digilantizma, možemo zaključiti da ovaj fenomen može biti moćan alat za razotkrivanje kaznenih djela i privođenje njihovih počinitelja pravdi. Međutim, postoji nekoliko etičkih aspekata koji se mogu istaknuti kada se govori o problematičnoj prirodi digilantizma.

Jedan od najvažnijih etičkih problema povezanih s digilantizmom nedostatak je odgovarajućeg kazneno-pravnog postupka. U pravnom sustavu, osobe optužene za nedjela imaju pravo na pošteno suđenje, pravno zastupanje i presumpciju nevinosti dok im se ne dokaže krivnja. U sustavu digitalne "pravde", ove zaštite često zaobilaze *online* zajednice ili pojedince koji donose nepromišljene prosudbe na temelju ograničenih informacija. Nedostatak odgovarajućeg postupka može dovesti do toga da nevini ljudi ili organizacije budu nepravedno napadnuti i potkopava načela poštenog pravosudnog sustava.

Digilantizam često dovodi do toga da navodni počinitelji budu javno razotkriveni, što često rezultira zadiranjem u njihovu privatnost. Osobni podaci kao što su adrese, telefonski brojevi i informacije o zaposlenju mogu se široko dijeliti na platformama društvenih medija. Na primjer, Curt Schilling, poznati umirovljeni igrač bejzbola u SAD-u, uzeo je stvari u svoje ruke nakon što je njegova kći postala meta internetskog nasilja i seksualnog uznemiravanja na Twitteru. Schilling je identificirao devet osoba odgovornih za uvredljive poruke i javno podijelio njihova imena, s

resources and can have serious legal consequences. Perpetrators are motivated to commit attacks out of revenge against another hacker, for fun, boredom, or as a rite of passage in certain hacker groups (Romaniuk and Lorenzo, 2023). The FBI estimates that there are 400 such calls a year (Statt, 2017). These calls unnecessarily consume police resources and the FBI estimates that the average fraudulent call costs police approximately $10,000 (McCartney, 2013).

ETHICAL AND CRIMINAL JUSTICE CHALLENGES OF DIGILANTISM

If we look at the specifics of digilantism based on research conducted so far, we can conclude that this phenomenon can be a powerful tool when used to expose wrongdoing and bring criminals to justice. However, there are several ethical aspects that must be emphasised when talking about the problematic nature of digilantism.

One of the most important ethical problems associated with digilantism is the lack of due process. In the legal system, people accused of wrongdoing have the right to a fair trial, legal representation, and the presumption of innocence until proven guilty. In the digital "justice" system, these protections are often circumvented by online communities or individuals who make rash judgements based on limited information. The lack of due process can lead to innocent people or organisations being unfairly targeted and this undermines the principles of a fair justice system.

Digilantism often leads to alleged offenders being publicly exposed, often resulting in an invasion of their privacy. Personal information such as addresses, phone numbers, and employment information can be widely shared on social media platforms. For instance, Curt Schilling, a well-known retired baseball player in the U.S., took matters into his own hands after his daughter became a target of cyberbullying and sexual harassment on Twitter. Schilling identified nine individuals responsible for the abusive messages and publicly shared their names, along with their high schools and their parents' email addresses. His actions led to serious consequences for the offenders, with

njihovim srednjim školama i e-mail adresama njihovih roditelja. Njegovi su postupci doveli do ozbiljnih posljedica za prijestupnike, pri čemu je jedan suspendiran sa sveučilišta, a drugi je izgubio posao (Chang, 2018.). Drugi primjer strašnih posljedica digilantizma primjer je vezan za bombaški incident u Bostonu. Sunil Tripathi, 22-godišnji student koji je nestao, pogrešno je identificiran kao glavni osumnjičenik u ovom slučaju. Njegovo tijelo otkriveno je tek nakon što je osumnjičeni uhićen. Dok su se korisnici interneta kasnije *online* ispričavali njegovoj obitelji, početna identifikacija njega kao glavnog osumnjičenika nanijela je veliku štetu obitelji tijekom potrage za njihovim nestalim sinom (Lee, 2013.). Ovo postavlja etička pitanja o pravu na privatnost i potencijalnoj šteti pojedincima koji su lažno optuženi ili koji se već suočavaju s pravnim posljedicama za svoje postupke.

Kolateralna šteta također je identificirana kao ozbiljan problem povezan s digilantizmom. Napadi uskraćivanjem usluge (DDoS) mogu dovesti do kolateralne štete, često pogađajući nedužne strane, budući da se vješti hakeri koriste zaraženim računalima (zombijima) za pokretanje svojih napada. Protuhakiranje također može nenamjerno oštetiti te nedužne sustave. DDoS napadi mogu poremetiti ključne vladine usluge i infrastrukturu, kao što je prikazano u 'kibernetičkom napadu u Estoniji', koji je ciljao na različite vladine mrežne stranice i institucije (Chang, Zhong i Grabosky, 2016.). Nadalje, netilantizam tj., digilantizam, može rezultirati kolateralnom štetom kada se osobni podaci o metama i njihovim suradnicima dijele javno. Na primjer, u slučaju gospodina Wang Feia, uznemiravanje njegove obitelji i radnog mjesta uslijedilo je nakon otkrivanja njegove izvanbračne afere, što je u konačnici dovelo do tragičnog samoubojstva njegove supruge (Chang i Leung, 2015.).

Anonimnost i nedostatak odgovornosti u digitalnom okruženju čine ljude osjetljivima na pogreške i pogrešnu identifikaciju. Nevini ljudi mogu biti lažno optuženi i suočeni s ozbiljnim posljedicama, a da se njihova krivnja ne dokaže ili potvrdi. U nedostatku formalnog pravnog okvira, *freelanceri* često imaju malo ili nimalo odgovornosti. Decentralizirana priroda *online* zajednica

one being suspended from university and another losing their job (Chang, 2018). Another example of terrible consequences of digilantism is the example related to the Boston bombing incident. Sunil Tripathi, a 22-year-old university student who had gone missing, was incorrectly identified as the primary suspect in the case. His body was discovered only after the actual suspect had been apprehended. While internet users later issued apologies online to his family, the initial identification of him as the main suspect inflicted significant distress on the family during their search for their missing son (Lee, 2013). This raises ethical questions about the right to privacy and the potential harm to individuals who are falsely accused or those who are already facing legal consequences for their actions.

Collateral damage has been also identified as a serious issue related to digilantism. DDoS attacks can lead to collateral damage, often affecting innocent parties, since skilled hackers use infected computers (zombies) to launch their attacks. Counter-hacking efforts can also inadvertently harm these innocent systems. DDoS attacks can disrupt critical government services and infrastructure, as exemplified by the 'Estonia cyber-attack,' which targeted various government websites and institutions (Chang, Zhong & Grabosky, 2016). Furthermore, 'netilantism' or online vigilantism can result in collateral damage when personal information about targets and their associates is publicly shared. For instance, in the case of Mr. Wang Fei, the harassment of his family and workplace followed the disclosure of his extramarital affair, ultimately leading to his wife's tragic suicide (Chang & Leung, 2015).

Anonymity and lack of accountability in the digital environment make people vulnerable to mistakes and misidentification. Innocent people can be falsely accused and face serious consequences without their guilt being proven or confirmed. In the absence of a formal legal framework, freelancers often have little or no accountability. The decentralised nature of online communities makes it difficult to hold individuals or groups accountable for their actions. The speed at which information spreads online can exacerbate these

otežava pozivanje pojedinaca ili grupa na odgovornost za njihove postupke. Brzina kojom se informacije šire *online* može pogoršati te probleme i otežati ispravljanje pogrešaka nakon što se dogode.

Sudjelovanje građana u sigurnosti i usklađenosti može spriječiti stalne napore organa za provođenje zakona i potencijalno dovesti do neuspjeha kaznenih istraga. Učinkovite istrage zločina moraju se pridržavati određenih zakonskih procedura. Dok netilantistička skupina Letzgo Hunting tvrdi da su njihovi dokazi bili ključni u osudi nekih počinitelja, postoje pitanja o prihvatljivosti takvih dokaza na sudu (Hill i Wall, 2015.). Nadalje, neki oblici budnosti mogu poremetiti obavještajne operacije koje se oslanjaju na pomni nadzor, slično 'praćenju hrpe gupija u pokušaju da namame i namotaju veliku ribu' (Michaels, 2010.). Bez profesionalne obuke, privatne istrage digilanata mogle bi nenamjerno upozoriti kriminalce.

Zbog digilantizma mogu eskalirati sukobi u stvarnom svijetu. Ono što počinje *online* optužbama, može brzo eskalirati u sukobe u stvarnom svijetu i dovesti do fizičkog nasilja. Granica između *online* aktivizma i posljedica u stvarnom svijetu može postati zamagljena, izazivajući etičku zabrinutost o odgovornosti onih koji iniciraju ili sudjeluju u digitalnoj osvetničkoj pravdi.

PREVENCIJA DIGITALNOG VIGILANTIZMA: STRATEGIJE ZA PREVENCIJU I ODGOVORNO *ONLINE* PRAVOSUĐE

Kako bi se učinkovito borile protiv digitalnog vigilantizma, *online* platforme moraju poboljšati svoje napore u moderiranju sadržaja korištenjem ljudskih moderatora i naprednih AI tehnologija. Ti bi sustavi trebali moći prepoznati i brzo ukloniti štetan sadržaj, uključujući pozive na uznemiravanje, *doxxing* ili objavljivanje privatnih podataka. Platforme bi trebale implementirati mehanizme brze reakcije kako bi se uhvatile ukoštac sa štetnim ponašanjima čim se otkriju, poput širenja dezinformacija ili organiziranja kampanja uznemiravanja. Također bi trebalo razviti sustave prilagođene korisnicima za prijavu štetnog sadržaja

problems and make it difficult to correct mistakes once they have occurred.

Citizen participation in security and compliance can hinder ongoing law enforcement efforts and potentially lead to the failure of criminal investigations. Effective crime investigations must adhere to certain legal procedures. While the netilantism group Letzgo Hunting claims that their evidence was crucial in the conviction of some offenders, there are questions about the admissibility of such evidence in court (Hill and Wall, 2015). Furthermore, some forms of vigilantism can disrupt intelligence operations that rely on careful surveillance, akin to 'monitoring a bunch of guppies in an effort to lure in and reel in the big fish' (Michaels, 2010). Without professional training, digilantes' private investigations could inadvertently alert criminals.

Digilantism has the potential to escalate conflicts in the real world. What starts with online accusations can quickly escalate into real-world conflicts and lead to physical violence. The line between online activism and real-world consequences can become blurred, raising ethical concerns about the accountability of those who initiate or participate in digital retributive justice.

MITIGATING DIGITAL VIGILANTISM: STRATEGIES FOR PREVENTION AND RESPONSIBLE ONLINE JUSTICE

To effectively combat digital vigilantism, online platforms need to improve their content moderation efforts by utilising both human moderators and advanced artificial intelligence (AI) technologies. These systems should be able to recognise and quickly remove harmful content, including calls for harassment, doxing, or the publication of private information. Platforms should implement rapid response mechanisms to tackle harmful behaviours as soon as they are detected, such as the spread of misinformation or the staging of harassment campaigns. User-friendly systems for reporting harmful content related to digital vigilantism should also be developed to promote a transparent reporting process that builds trust in the platform's response system.

povezanog s digitalnim vigilantizmom kako bi se promicao transparentan postupak prijave koji gradi povjerenje u sustav odgovora platforme.

Osim toga, obrazovni programi trebali bi promicati digitalno građanstvo naglašavanjem važnosti odgovornog *online* angažmana te mogućih rizika i posljedica sudjelovanja u aktivnostima osvete. Kampanje podizanja javne svijesti trebale bi se usredotočiti na pravne posljedice sudjelovanja ili promicanja internetskog vigilantizma, uključujući internetsko zlostavljanje, uznemiravanje i invaziju na privatnost. Ove bi kampanje također trebale istaknuti opasnosti djelovanja na temelju neprovjerenih ili pogrešnih informacija, što može dovesti do toga da nevini ljudi budu nepravedno ciljani.

Odgovorno izvješćivanje novinara i medija ključno je za suzbijanje porasta digitalnog vigilantizma. Medijska pokrivenost kaznenih slučajeva ili pitanja socijalne pravde mora izbjegavati senzacionalizam koji bi mogao potaknuti budnost. Etičke prakse prijavljivanja, uključujući oprezno izvješćivanje i izbjegavanje legitimiranja osvetničkih radnji, ključne su za sprječavanje eskalacije internetskog uznemiravanja i mafijaškog ponašanja.

Vlade, sa svoje strane, moraju povećati povjerenje javnosti u pravosudni sustav osiguravajući da se zločini temeljito istražuju i da pravosudni sustav radi transparentno. Kada javnost ima povjerenja u učinkovitost pravosudnog sustava, manje je iskušenja pribjeći osvetničkoj pravdi. Agencije za provođenje zakona trebale bi biti transparentnije u svom radu i istragama kako bi smanjile potrebu javnosti da pravdu uzme u svoje ruke.

Alati umjetne inteligencije mogu se razviti za praćenje *online* ponašanja u potrazi za znakovima digitalnog vigilantizma, kao što su koordinirani napadi, razmjena informacija velikih razmjera ili ponašanje slično mafijaškom ciljanju pojedinaca. Jačanje zaštite privatnosti na internetu, uključujući enkripciju, alate za anonimiziranje i zaštitne mjere protiv otkrivanja osobnih podataka, može spriječiti pojedince da budu meta internetskih mafijaša. Osim toga, platforme bi trebale primjenjivati algoritme koji ograničavaju širenje štetnog sadržaja, kao što su *doxxing* ili kampanje uznemi-

In addition, educational programmes should promote digital citizenship by emphasising the importance of responsible online engagement and the potential risks and consequences of participating in vigilante activities. Public awareness campaigns should focus on the legal consequences of promoting or participating in online vigilantism, including cyberbullying, harassment, and invasion of privacy. These campaigns should also highlight the dangers of acting on unverified or misleading information, which can lead to innocent people being unfairly targeted.

Responsible reporting by journalists and the media is essential to curb the rise of digital vigilantism. Media coverage of criminal cases or social justice issues must avoid sensationalism that could incite vigilantism. Ethical reporting practises, including cautious reporting and avoiding the legitimisation of vigilante actions, are crucial when it comes to preventing the escalation of online harassment and mob behaviour.

Governments, for their part, must increase public confidence in the justice system by ensuring that crimes are thoroughly investigated and that the justice system operates transparently. When the public has confidence in the effectiveness of the justice system, there is less temptation to resort to vigilante justice. Law enforcement agencies should be more transparent in their operations and investigations to reduce the public's desire to take justice into their own hands.

AI tools can be developed to monitor online behaviour for signs of digital vigilantism, such as coordinated attacks, large-scale information sharing, or mafia-like behaviour targeting individuals. Strengthening online privacy protections, including encryption, anonymisation tools, and safeguards against the disclosure of personal data, can help prevent individuals from being targeted by online mobs. In addition, platforms should use algorithms that limit the spread of harmful content, such as doxing or harassment campaigns, by demoting such content in search results and news feeds.

Fostering a constructive online environment is crucial. Online communities should be encour-

ravanja, snižavanjem takvog sadržaja u rezultatima pretraživanja i *feedovima* vijesti.

Poticanje konstruktivnog internetskog okruženja također je ključno. Internetske zajednice treba poticati na promicanje dijaloga temeljenog na uzajamnom poštovanju i aktivno obeshrabrivanje osvetničke pravde. Utjecajne osobe, čelnici zajednice i moderatori trebali bi intervenirati u rasprave koje se kreću prema budnosti i usmjeriti razgovor prema odgovornom ponašanju.

Trening empatije i programi rješavanja sukoba za *online* korisnike mogu pomoći u smanjenju agresivnog ponašanja i želje za osvetom. Kampanje za podizanje svijesti trebale bi educirati korisnike o mrežnom učinku dezinhibicije koji se javlja kada anonimnost dovede do ponašanja koje ne bi ispoljavali izvan mreže. Pojašnjavanje pravih posljedica *online* radnji može djelovati kao sredstvo odvraćanja od ponašanja nalik osvetnici.

Žrtve digitalnog vigilantizma trebaju imati pristup sveobuhvatnoj podršci, uključujući pravno i psihološko savjetovanje, kako bi im se pomoglo nositi s emocionalnim i pravnim posljedicama svojih napada. Vlade i organizacije mogle bi uspostaviti timove za brzi odgovor kako bi pomogle žrtvama internetskog vigilantizma pružanjem pravnih savjeta, pomoći u kibernetičkoj sigurnosti i platforme za brzo prijavljivanje incidenata.

Iako *crowdsourcing* može biti vrijedan alat za istrage ili podizanje svijesti, mora se provoditi etički. Treba uspostaviti jasne smjernice za zaštitu privatnosti i sprječavanje zlouporabe informacija. Internetske zajednice treba obeshrabriti da provode "građanske istrage" bez provjerenih dokaza i umjesto toga treba ih poticati na suradnju s vlastima.

Cilj je ovih strategija uhvatiti se ukoštac s temeljnim uzrocima digitalnog vigilantizma, poboljšati odgovornost platforme, provesti zakonske posljedice i promicati obrazovanje javnosti kako bi se suzbilo štetno ponašanje i stvorilo sigurnije, odgovornije digitalno okruženje.

ZAKLJUČAK

Digilantizam predstavlja izazovno područje koje zahtijeva dodatna istraživanja radi njegovog

aged to promote dialogue based on mutual respect and actively discourage vigilante justice. Influential figures, community leaders, and moderators should intervene in discussions that drift towards vigilantism and steer the conversation towards responsible behaviour.

Empathy training and conflict resolution programmes for online users can help reduce aggressive behaviour and the urge to retaliate. Awareness campaigns should educate users about the online disinhibition effect that occurs when anonymity leads to behaviours that they would not exhibit offline. Once the real consequences of online actions are made clear, they can act as a deterrent to vigilante-like behaviour.

Victims of digital vigilantism should have access to comprehensive support, including legal and psychological counselling, in order to help them deal with the emotional and legal consequences of their attacks. Governments and organisations could set up rapid response teams to help victims of online vigilantism by providing legal advice, cybersecurity assistance, and a platform for rapid incident reporting.

Whilst crowdsourcing can be a valuable tool for investigations or awareness raising, it must be conducted ethically. Clear guidelines should be established to protect privacy and prevent the misuse of information. Online communities should be discouraged from conducting "citizen investigations" without verified evidence and instead be encouraged to co-operate with the authorities.

These strategies aim to tackle the root causes of digital vigilantism, improve platform accountability, enforce legal consequences, and promote public education to curb harmful behaviour and create a safer, more responsible digital environment.

CONCLUSION

Digilantism is a tricky subject that requires further research in order to better understand its complexities and possible consequences. Throughout history, vigilantism has always been a reaction to the perceived inadequacies of formal justice sys-

boljeg razumijevanja kako bismo se nosili s njegovim kompleksnostima i potencijalnim posljedicama. Kroz povijest, vigilantizam je bio odgovor na percipirane nedostatke formalnih pravosudnih sustava, a digitalna era donosi nove dimenzije ovom fenomenu.

Pojavom digilantizma, internet postaje prostor gdje građani preuzimaju ulogu izvršitelja pravde, često motivirani nedostacima formalnih pravosudnih sustava ili željom za društvenom promjenom. Digilantizam, kao posljedica te dinamike, obuhvaća širok spektar aktivnosti, uključujući označavanje, istraživanje, uhođenje, organizirano curenje podataka, *doxxing* i *online* posramljivanje.

Nadalje, specifični oblici digilantizma, poput *doxxinga* i *online* posramljivanja, imaju značajan utjecaj na živote označenih pojedinaca, uključujući rizike poput uznemiravanja, krađe identiteta, gubitka posla i fizičke ozljede. S obzirom na brzi razvoj tehnologije i rastući utjecaj interneta, potrebno je sustavno istraživanje i regulacija ovakvih oblika aktivizma kako bi se zaštitila prava pojedinaca i održala ravnoteža između slobode izražavanja i zaštite od zloupotrebe.

Definirajući digilantizam kao aktivnosti koje se koriste digitalnim alatima i *online* platformama za ostvarivanje pravde izvan formalnih sustava, važno je razumjeti njegove motive i implikacije. Motivacije pojedinaca ili grupa koje se bave digilantizmom mogu varirati od puke dosade, preko brige za sigurnost zajednice do želje za osvetom ili ideologijama aktivizma. Međutim, unatoč potencijalnim pozitivnim motivima, digilantizam nosi i etičke probleme, s nedostatkom kontrole i mogućnošću zloupotrebe digitalnih alata. Nedostatak formalne obuke i nadzora, karakterističan za aktivnosti digitalnih vigilanata, može rezultirati ozbiljnim posljedicama i sukobima s pravnim sustavom. Također, različite motivacije pojedinaca u digilantizmu, od političkih ciljeva do osobnih razloga, dodatno kompliciraju tumačenje njihovih aktivnosti.

Povezanost s društvenim medijima, mogućnost anonimnosti te moć i sloboda dostupni na internetu doprinose porastu digilantizma. Važno je razlikovati i proučavati različite oblike digilantizma, zato što svaki od ovih oblika ima svoje katems, and the digital age adds new dimensions to this phenomenon.

With the rise of digilantism, the Internet becomes a space where citizens take on the role of enforcers of justice, often motivated by the inadequacies of the formal justice system or the desire for social change. As a result of this dynamic, digilantism encompasses a wide range of activities, including tagging, research, stalking, organised leaks, doxing, and online shaming.

In addition, certain forms of bullying, such as doxing and online shaming, have a significant impact on the lives of those targeted including risks such as harassment, identity theft, loss of employment, and physical harm. Given the rapid development of technology and the growing influence of the Internet, systematic research and regulation of these forms of activism is necessary to protect the rights of individuals and maintain a balance between freedom of expression and protection from abuse.

When defining digilantism as activities that utilise digital tools and online platforms to achieve justice outside the formal justice system, it is important to understand the motivations and impacts. The motivations of individuals or groups engaging in vigilantism can range from mere boredom to concerns for community safety, and from revenge to ideologies of activism. Despite the potentially positive motives, digilantism harbours ethical problems due to the lack of control and the possibility of misuse of digital tools. The lack of formal training and supervision that characterises digital vigilante activities can lead to serious consequences and conflicts with the legal system. The different motivations of individual members of digital vigilante groups, ranging from political goals to personal reasons, can complicate the interpretation of their activities.

The connection to social media, the possibility of anonymity, and the power and freedom offered by the internet contribute to the rise of digilantism. It is important to distinguish and study different forms of digilantism, as each of these forms have its own characteristics and consequences,

rakteristike i posljedice, od niskog intenziteta do organizirane akcije protiv institucija.

Ovo područje također postavlja izazove za pravni sustav, s nedostatkom kontrole i regulacije u *online* svijetu. Pojava digilantizma potiče raspravu o potrebi novih pristupa u istraživanju *cyber* kriminaliteta i osiguravanju internetske sigurnosti, uzimajući u obzir promjene u tehnologiji i društvenim dinamikama.

Zaključno, razumijevanje digilantizma zahtijeva multidisciplinarni pristup koji uključuje kriminologiju, kibernetičku sigurnost, društvene medije i etiku. Samo kroz holistički pristup možemo razviti učinkovite strategije za suočavanje

ranging from low intensity digilantism to organised actions against institutions.

Digital vigilantism also poses a challenge to the legal system due to the lack of control and regulation in the online world. The emergence of digilantism is prompting a discussion about the need for new approaches to investigating cybercrime and ensure cybersecurity, while considering the changes in technology and social dynamics.

To summarise, understanding digilantism requires a multidisciplinary approach encompassing criminology, cyber security, social media, and ethics. Only through a holistic approach can we develop effective strategies to address the challenges posed by this complex phenomenon, striking a balance between justice, freedom of expression, and the protection of individual rights.

s izazovima koje donosi ova složena pojava, uravnotežujući pravdu, slobodu izražavanja i zaštitu prava pojedinaca.

REFERENCES

Anderson, B., Wood, MA. (2022). Harm imbrication and virtualised violence: Reconceptualising the harms of doxxing. *International Journal for Crime, Justice and Social Democracy, 11*(1), 196-209. https://doi.org/10.5204/ijcjsd.2140

Arvanitidis, T. (2016). Publication bans in a Facebook age: How internet vigilantes have challenged the youth criminal justice act's 'secrecy laws' following the 2011 Vancouver Stanley Cup Riot. *Canadian Graduate Journal of Sociology and Criminology*, *5*(1), 18–32.

Baker, J. (2017). Lynching, Public Violence and Internet in Indonesia. U M. Pfeifer (ur.) *Global Lynching and Collective Violence. Asia, Africa and Middle East – Volume I* (str. 10-33). Oxford University Press.

Banks, J. (2017). Radical criminology and the techno–security–capitalist complex. U: Steinmetz K, Nobles M.R. (ur.) *Technocrime and Criminological Theory* (str. 102-115), Routledge, New York:,

Barak, A., Nissim, M. B., & Suler, J. (2008). Fostering empowerment in online support groups. *Computers in Human Behavior*, *24*(5), 1867-1883. https://doi.org/10.1016/j.chb.2008.02.004

Barthel, B., Harrison, T. M. (2009). Wielding new media in Web 2.0: Exploring the history of engagement with the collaborative construction of media products. *New Media & Society*, *11*(1-2), 155-178. https://doi.org/10.1177/1461444808099580

Beck, C. (2016). Web of resistance: Deleuzian digital space and hacktivism. *Journal for Cultural Research*, *20*(4): 334–349. https://doi.org/10.1080/14797585.2016.1168971

Betlej, A. (2014). Hacktivists and War on Internet, (U:) S. Partycki (ur.), *Perspektywy rozwoju społeczeństwa sieciowego w Europie Środkowej i Wschodniej (*pp. 183-190*)*, Wydawnictwo KUL, Lublin.

Broadhurst, R., Chang, L. Y. C. (2013). Cybercrime in Asia: Trends and challenges. U J. Liu, B. Hebenton, i S. Jou (ur.), *Asian Handbook of Criminology* (str. 49-64). New York, NY: Springer.

Brown, R. (1975). *Strain of Violence*. NY: Oxford University Press

Burrows, W. (1976). *Vigilante*. NY: Harcourt Brace Jovanovich.

Byrne, D. N. (2013). 419 digilantes and the frontier of radical justice online. *Radical History Review,* (117): 70-82. https://doi.org/10.1215/01636545-2210464

Calabro, S.M. (2018). From the message board to the front door: Addressing the offline consequences of race- and gender-based doxxing and swatting. *Suffolk University Law Review*, *51*(1): 55-73.

Castells, M. (2008). Interview with Manuel Castells. *Chinese Journal of Communication*, *27*(1), 3-6. https://doi.org/10.5070/BP327124502

Chang, L. Y. C. (2013). Formal and informal modalities for policing cybercrime across the Taiwan Strait. *Policing & Society*, *23*(4), 540-555. https://doi.org/10.1080/10439463.2013.780221

Chang, L. Y. C., Poon, R. (2017). Internet Vigilantism: Attitudes and Experiences of University Students Toward Cyber Crowdsourcing in Hong Kong. *International Journal of Offender Therapy and Comparative Criminology*, *61*(16), 1912-1932. https://doi.org/10.1177/0306624X16639037

Chang, L. Y. C., Zhong, Y. & Grabosky, P. (2016). Citizen Co-Production of Cyber Security: Self-Help, Vigilantes, and Cybercrime. *Regulation and Governance*, 10(1), 101-104. https://doi.org/10.1111/rego.12125

Chang, L.Y.C (2018). Internet Vigilantism: Co-production of security and compliance in the digital age. (U) L.Y.C. Chang, R. Brewer (eds.) Criminal Justice and Regulation Revisited: Essays in Honour of Peter Grabosky. Routledge Frontiers of Criminal Justice. (pp. 205-223). Routledge, New York

Chang, L.Y.C., Leung, A.K.H. (2015). An Introduction to Cyber Crowdsourcing (Human Flesh Search) in the Greater China Region. (U:), R.G. Smith, R.CC Cheung, L.Y.C. Lau, (eds.) *Cybercrime Risks and Responses. Palgrave Macmillan's Studies in Cybercrime and Cybersecurity*. (pp. 240-250). Palgrave Macmillan, London. https://doi.org/10.1057/9781137474162_16

Chang, L.Y.C., Zhong, Y. & Grabosky, P. (2016). Citizen co-production of cyber security: Self-Help, Vigilantes, and Cybercrime. Regulation & Governance, 12(1), 101-114. DOI: 10.1111/rego.12125

Chen, S. F. (2011). Discussion on Mechanisms of Monitoring Freedom of Speech Freedom and Human Flesh Searching, *Journalism Lover,* 18: 42–44.

Cheong, P. H., Gong, J. (2010). Cyber vigilantism, transmedia collective intelligence, and civic participation. *Chinese Journal of Communication*, 3(4), 471–487. https://doi.org/10.1080/17544750.2010.516580

Cheung, A.S. Y. (2009). China Internet Going Wild: Cyber-hunting Versus Privacy Protection. *Computer Law and Security Review,* 25: 275–279. https://doi.org/10.1016/j.clsr.2009.03.007

Chowriwar, S.S., Madhulika S.M., Prajyoti P.S., Parpelli, S. and Sambhe, N. (2014). Mitigating Denial-of-Service Attacks Using Secure Service Overlay Model. *International Journal of Engineering Trends and Technology*, *8*(9), 479–83. https://doi.org/10.14445/22315381/IJETT-V8P284

Clarke, R. V. (2004). Technology, criminology and crime science. *European Journal on Crime Policy and Research*, *10*(1), 55–63. https://doi.org/10.1023/B:CRIM.0000037557.42894.f7

Coleman G. (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso Books.

Colton J.S., Holmes, S. and Walwema, J. (2017). From noobguides to #OpKKK: Ethics of anonymous' tactical technical communication. *Technical Communication Quarterly, 26*(1), 59-75. https://doi.org/10.1080/10572252.2016.1257743

De Vries, A. (2015). The use of social media for shaming strangers: Young people's views. U: T.H. Bui i R.H. Sprague (ur.): *2015 48th Hawaii International Conference on System Sciences* (str. 2053–2062). Kauai, HI: IEEE. doi: 10.1109/HICSS.2015.215

Dragiewicz, M., Burgess, J., Matamoros-Fernandez, A., Salter, M., Suzor, N.P., Woodlock, D. and Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, *18*(4), 609-625. https://doi.org/10.1080/14680777.2018.1447341

e Silva, K. K. (2018). Vigilantism and cooperative criminal justice: Is there a place for cybersecurity vigilantes in cybercrime fighting? *International Review of Law, Computers & Technology, 32*(1), 21-36. https://doi.org/10.1080/13600869.2018.1418142

Enzweiler, M.J. (2015). Swatting Political Discourse: A Domestic Terrorism Threat. Notre Dame Law Review, 90(5):2001-2038.

Fei-Yue W., Zeng, D., Hendler, J.A., Zhang, Q., Feng, Z., Gao, Y., Wang, H., i Lai, G., (2010). A Study of the Human Flesh Search Engine: Crowd-Powered Expansion of Online Knowledge. *Computer, 43*(8): 45-53. https://doi:10.1109/MC.2010.216.

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. & Dell, N. (2018). A stalker's Paradise: How intimate partner abusers exploit technology. U: R. Mandryk i M. Hancock (ur.) *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (str.1-13). New York: Association for Computing Machinery. https://doi.org/10.1145/3173574.3174241

Gabdulhakov, R. (2018). Citizen-led justice in Post-Communist Russia: From comrades' courts to dotcomrade vigilantism. *Surveillance & Society, 16*(3), 314-331. https://doi.org/10.24908/ss.v16i3.6952

Ghazali, K. W. M. & Rosilah, H. (2011). "Flooding Distributed Denial of Service Attacks—A Review." *Journal of Computer Science*, *7*(8): 1218 – 1223.

Gies, L. & Bortoluzzi, M. (2021). Online Vigilantism and Media Justice: Cultural Constructions of Morality and Legitimacy in Digital Spaces. *Media, Culture & Society*, 43(6), 55-72. https://doi.org/10.1007/s13347-016-0216-4

Goldsmith, A., Brewere, R. (2014). Digital drift and the criminal interaction order. *Theoretical Criminology, 19*(1), 112–130. https://doi.org/10.1177/136248061453864

Hao, L. Y. (2009). A Study on Cyber Violence and Human Flesh Search. *Journal of Teaching and Researching Exploration, 5:*220

Henry, N., Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse, 19*(2), 195-208. https://doi.org/10.1177%2F1524838016650189

Herold, D.K. (2011). Human flesh search engines: Carnivalesque riots as components of a „Chinese democracy". U D.K. Herold i P. Marlot (ur.) *Online Society in China: Creating, Celebrating, and Instrumentalising the Online Carnival* (str. 127-145). Routledge. https://doi.org/10.5204/ijcjsd.2140

Hill, G., Wall, D. (2015). How online vigilantes make paedophile policing more difficult. https://theconversation.com/how-online-vigilantes-make-paedophile-policing-more-difficult-42562. Retreived on 08.10.2024.

Huang, Q. (2023). The discursive construction of populist and misogynist nationalism: Digital vigilantism against unpatriotic intellectual women in China. Social Media+ Society, 9(2), 1-13. https://doi.org/10.1177/205630512311708

Huey, L., Nhan, J., & Broll, R. (2013). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice*, 13(1), 81–97. https://doi.org/10.1177/17488958124480

Ireland, L. (2022). We are all (not) Anonymous: Individual- and country-level correlates of support for and opposition to hacktivism. *New Media & Society,* Online First. https://doi.org/10.1177/14614448221122252

Jane, E. A. (2017). Feminist digilante responses to a slut-shaming on Facebook. *Social Media+ Society*, *3*(2), 1-10. https://doi.org/10.1177/205630511770599

Jenkins, H. (2006). *Convergence culture: Where old and new media collide*. New York: New York University Press.

Johnston, L. (1996). What is vigilantism? *British Journal of Criminology, 36*(2), 220–236.

Jones, A. (2016). I get paid to have orgasms: Adult webcam models' negotiation of pleasure and danger. *Signs: Journal of Women in Culture and Society, 42*(1), 227-256. https://doi.org/10.1086/686758

Kavada, A. (2015). Creating the collective: social media, the Occupy Movement and its constitution as a collective actor. *Information, Communication & Society*, 18(8), 872–886. https://doi.org/10.1080/1369118X.2015.1043318

Khanna, P., Zavarsky, P. & Lindskog, D. (2016). Experimental analysis of tools used for doxing and proposed new transforms to help organizations protect against doxing attacks. *Procedia Computer Science,* 94: 459-464. https://doi.org/10.1016/j.procs.2016.08.071

Krim, J. (2005). Subway fracas escalates into test of the internet's power to shame. Washington Post. Retrieved October 13, 2024, from http://www.washingtonpost.com/wp-dyn/content/article/2005/07/06/AR2005070601953.html?referrer=emailarticle

Lee, D. (2013): Boston bombing: How internet detectives got it very wrong. http://www.bbc.com/news/technology-22214511, pristupljeno dana 08.10.2024.

Loveluck, B. (2019). The many shades of digital vigilantism. A typology of online self-justice. *Global Crime*, 21(3–4), 213–241. https://doi.org/10.1080/17440572.2019.1614444

Lunceford, B. (2009). Cyberwar: The Future of War? P. Haridakis, B.S. Hugenberg i S.T. Wearden (ur.) *War and the Media: Essays on News Reporting, Propaganda and Popular Culture*, (pp. 238–251). Jefferson, NC: McFarland.

Marwick, A. (2013). There's no justice like angry mob justice: Regulating hate speech through internet vigilantism. *AoIR Selected Papers of Internet Research,* 14: 1-16.

Marwick, A. E., Lewis, R. (2017). Media Manipulation and Disinformation Online. https://datasociety.net/library/media-manipulation-and-disinfo-online/. Retrieved on 13.10.2024

Matamoros-Fernández, A. (2017). Platformed racism: The mediation and circulation of an Australian race-based controversy on Twitter, Facebook and YouTube. *Information, Communication & Society*, *20*(6), 930-946. https://doi.org/10.1080/1369118X.2017.1293130

McCartney, A. (2013). Lawmakers to call for stiffer penalties to stop swatting. Preuzeto 20.04. 2024 s https://www.police1.com/legal/articles/lawmakers-to-call-for-stiffer-penalties-tostop-swatting-kBEu1N5vD4My3uDr/.

McNealy, J. (2017). Readers react negatively to disclosure of poster's identity. *Newspaper Research Journal*, *38*(3), 282-292. https://doi.org/10.1177%2F0739532917722977

Michaels, J. (2010). Deputizing homeland security. *Texas Law Review*, 88, 1435–1473.

Mohammed, F. (2017). Is doxxing the right way to fight the "alt-right"? JSTOR Daily, August 30. Preuzeto 10.04.2024 s https://daily.jstor.org/is-doxxing-the-right-way-to-fight-the-alt-right/.

Nhan, J., Huey, L., and Broll, R. (2017). Digilantism: An analysis of crowdsourcing and the Boston Marathon bombings. *British Journal of Criminology*, 57(2), 341–361. https://doi.org/10.1093/bjc/azv118

Ong, R. (2012). Online vigilante justice Chinese style and privacy in China. *Information & Communication Technology Law, 21*(2), 127-145. https://doi.org/10.1080/13600834.2012.678653

Phillips, W. (2011). LOLing at tragedy: Facebook trolls, memorial pages and resistance to grief online. *First Monday, 16*(12). https://firstmonday.org/article/view/3168/3115

Powell, A., Stratton, G., and Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. Routledge.

Romaniuk, S., Lorenzo, R. (2023). Swatting. U S. Romaniuk, M. Catino and C. Martin (eds.) *The Handbook of Homeland Security* (pp. 848-853). CRC Press. https://doi.org/10.4324/9781315144511

Smallridge, J., Wagner, P., i Crowl, J. N. (2016). Understanding cyber-vigilantism: A conceptual framework. *Journal of Theoretical & Philosophical Criminology, 8*(1), 57-70.

Statt, N. (2017). Swatting over Call of Duty game results in deadly police shooting of Kansas man. Retreived from 17.04.2024. s https://www.theverge.com/2017/12/29/16830626/call-of-duty-swatting-prank-kansas-man-dead-police-shooting.

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, *7*(3), 321-326. https://doi.org/10.1089/1094931041291295

Tanner, S., Campana, A. (2019). Watchful citizens" and digital vigilantism: A case study of the far right in Quebec. *Global Crime, 21* (3-4), 262-282. https://doi.org/10.1080/17440572.2019.1609177

Trottier, D. (2012). *Social Media as Surveillance: Rethinking Visibility in a Converging World*. Farnham: Ashgate.

Trottier, D. (2014). Police and user-led investigations on social media. *Journal of Law, Information and Science, 23*(1), 75–96.

Trottier, D. (2017). Digital vigilantism as weaponisation of visibility. *Philosophy & Technology, 30*(1), 55–72. https://doi.org/10.1007/s13347-016-0216-4

Trottier, D. (2019). Digital Vigilantism as Networked Harrassment: How Sharing Affordances Create Opportunities for Harmful Publicity. *Surveillance & Society*, 17(1/2), 155-162. doi: 10.1007/s13347-016-0216-4

Trottier. D. (2020). Denunciation and doxing: Towards a conceptual model of digital vigilantism. *Global Crime, 21*(3-4), 196-212. https://doi.org/10.1080/17440572.2019.1591952

Van Laer, J. (2014). Activists "Online" and "Offline": The Internet as an Information Channel for Digital Vigilantes. *Mobilization: An International Quarterly*, 19(4), 439-455. https://doi.org/10.17813/maiq.15.3.8028585100245801

Volkova, A. V., Lukyanova, G. V., and Kulakova, T. A. (2022). Gender Dimension of Digital Vigilantism in Russia. *RUDN Journal of Political Science*, 24(1), 120-135.

Wall, D.S. (2001). Cybercrimes and the Internet. U D.S. Wall (ur.) *Crime and the Internet* (pp. 1-17). Routledge.

Xiao, P. (2011). An Analysis of the Phenomenon of Internet Mass Hunting. *Journal of Hunan University, 25*(1): 156–60.

Yardley, E., Lynes, A. G. T., Wilson, D., and Kelly, E. (2018). What's the deal with "websleuthing"? News media representations of amateur detectives in networked spaces. *Crime, Media, Culture: An International Journal, 14*(1), 81–109. https://doi.org/10.1177/1741659016674045

Zimmerman, A., Ybarra, M. (2016). Online Aggression: The Influence of Anonymity and Social Norms on Reactive and Proactive Aggression. *Psychology of Popular Media Culture*, 5(3), 181-193. https://psycnet.apa.org/doi/10.1037/ppm0000038

Zook, M., Graham, M. (2007). The creative reconstruction of the Internet: Google and the privatization of cyberspace and digiplace. *Geoforum, 38*(6), 1322-1434. https://doi.org/10.1016/j.geoforum.2007.05.004