Hakeri i pirati u umreženom društvu

Andrišić, Mirna

Sveučilište J. J. Strossmayera u Osijeku

Filozofski fakultet Osijek

Preddiplomski studij Informatologije

Mirna Andrišić

Hakeri i pirati u umreženom društvu

Završni rad

Mentor: izv. prof. dr. sc. Boris Badurina

Osijek, 2021.

Sveučilište J. J. Strossmayera u Osijeku

Filozofski fakultet Osijek

Preddiplomski studij Informatologije

Mirna Andrišić

Hakeri i pirati u umreženom društvu

Završni rad

Područje društvenih znanosti, informacijske i komunikacijske znanosti, grana informatologija

Mentor: izv. prof. dr. sc. Boris Badurina

Osijek, 2021.

Prilog: Izjava o akademskoj čestitosti i o suglasnosti za javno objavljivanje

IZJAVA

Izjavljujem s punom materijalnom i moralnom odgovornošću da sam ovaj rad samostalno napravio te da u njemu nema kopiranih ili prepisanih dijelova teksta tuđih radova, a da nisu označeni kao citati s napisanim izvorom odakle su preneseni. Svojim vlastoručnim potpisom potvrđujem da sam suglasan da Filozofski fakultet Osijek trajno pohrani i javno objavi ovaj moj rad u internetskoj bazi završnih i diplomskih radova knjižnice Filozofskog fakulteta Osijek, knjižnice Sveučilišta Josipa Jurja Strossmayera u Osijeku i Nacionalne i sveučilišne knjižnice u Zagrebu.

U Osijeku, datum 17. 06. 2021. Mirna Andrišić _____, 0122228740

ime i prezime studenta, JMBAG

Sažetak

Teško je zamisliti svijet bez računalne tehnologije i interneta jer je taj izum omogućio međunarodnu povezanost i dostupnost informacija, kao jedne od osnovnih potreba društva. Utjecaj tehnologije je uvelike promijenio i obogatio društveni život zajednice, a da nije bilo hakera ne bi bilo ni računala. Prve hakere je povezivala ljubav o stvaranju sigurnog okruženja na mreži i razvijanja hakerske, odnosno programerske zajednice u kojoj vrijede određene etičke vrijednosti koje svaki haker treba usvojiti. Primarni pokretač svake poslovne organizacije postaju materijalna sredstva i osobna korist, no etički hakeri i pirati se još uvijek drže svojih etičkih vrijednosti i ciljeva zajedničkog povezanog svijeta. Mediji prikazuju hakere i pirate kao najveće kršitelje zakona u digitalnom okruženju, no često se zanemaruju njihovi pokretački motivi koje nastoje ispuniti kao zajednica. Piratstvo je najpopularniji oblik krađe intelektualnog vlasništva u svijetu, koji je imao posljedice na razna područja intelektualnog sadržaja, no u isto je vrijeme omogućilo veću dostupnost i povezanost sadržaja sa korisnicima. Cilj ovog rada je povećati svijest o prednostima i nedostacima interneta, koji se ukorijenio u sve aspekte ljudskog djelovanja, ali i proširiti znanje o hakerima i digitalnim piratima, te ujedno otkriti kakav su utjecaj imali na današnje umreženo društvo. U sljedećim poglavljima više će se saznati o hakerima i piratima, njihovim počecima i djelovanju s obzirom na digitalne trendove. Također, na temelju istraživanja iz literature opisati će se i prikazati kakav je utjecaj tehnologija i razvoj interneta imala na društvo, koje se danas zove umreženo.

Ključne riječi: hakeri, piratstvo, umreženo društvo, internetska sigurnost, percepcija hakera i pirata

Sadržaj

1. Uvod

Digitalno je doba započelo sa željom povezanosti svih ljudi diljem svijeta. Prije dvadeset godina nije se moglo niti zamisliti kakav će svijet biti u budućnosti, razmišljalo se samo o pozitivnim stranama tehnologije i napretku cijelog društva. U današnje vrijeme cijelo društvo ovisi o prijenosu i širenju informacija, koje su postale intelektualni kapital. Ubrzo smo, kao umreženo društvo, postali toliko ovisni o internetu i konzumiranju informacija, da nismo uočili kakav je utjecaj tehnologija ostavila na nas. Svi naši podaci, sve interakcije, podijeljeni sadržaji, posjećene stranice, pa i naša lokacija, su pohranjeni na internetu i zajedno čine naš osobni digitalni identitet (Great Hack, 2019: 2:40).[1] Granice između računala i ljudi su se zamaglile, ljudi ujedno žive i u virtualnom i u fizičkom svijetu te su kao takvi postali isprepletani.[2] Sve oko nas povezano je internetom, od pametnog asistenta (Siri, Alexa) koji nam postavlja alarme za buđenje i informira nas o najbitnijim novostima iz cijelog svijeta, do pametnih hladnjaka koji znaju koje namirnice treba kupiti u trgovini. Prekid rada usluge informacijskih i komunikacijskih tehnologija može ugroziti životne standarde i potresti cijeli svijet. Slika budućnosti u kojoj svijetom vladaju roboti, nije daleko. No, nisu samo pametni uređaji opasni, već se sve više putem medija naglašava prijeteća opasnost hakera i pirata. Temeljne hakerske, ali i piratske ideološke vrijednosti su povezanost i dostupnost cijelog digitalnog okruženja. Rastom prisutnosti pojedinaca na internetu, ujedno rastu i prilike cyber kriminala i zloupotrebe osobnih podataka. Svaki korisnik treba biti upoznat s pozitivnim i negativnim stranama interneta, te promicati i držati se etičkih vrijednosti ponašanja.[3]

Cilj ovog rada je povećati svijest o utjecaju interneta koji se ukorijenio u sve aspekte ljudskog djelovanja, ali i proširiti znanje o hakerima i digitalnim piratima, te ujedno otkriti kakav su utjecaj imali na današnje umreženo društvo. U sljedećim poglavljima više će se saznati o hakerima i piratima, njihovim počecima i djelovanju s obzirom na digitalne trendove. Također, na temelju istraživanja iz literature opisati će se i prikazati kakav je utjecaj tehnologija i razvoj interneta imala na društvo koje se danas zove umreženo, povezano i informacijsko.

[1] Usp. Amer, K.; Noujaim, J. The Great Hack. Netflix, 2019.

[2] Usp. Beale, Sara Sun; Berris, Peter. Hacking The Internet of Things: Vulnerabilities, dangers, and legal responses. // Duke Law & Technology Rewiev 16(2018). str. 162.

[3] Usp. Jaquet-Chiffelle, David-Oliver; Loi, Michele. Ethical and Unethical Hacking, 2019. str. 180-182.

2. Hakeri

2.1. Definiranje i podjela hakera

Uobičajeno je pročitati članak ili vijest o hakerima koji zaobilaze sigurnosne zamke privatnih i poslovnih mreža, kako bi u konačnici ukrali osobne podatke, onesposobili programe i stvoriti ogromnu financijsku štetu, no nisu svi hakeri opasni. Početkom 60-tih godina skupina strastvenih programera počela se nazivati hakerima, a sredinom 80-tih godina mediji su taj termin počeli povezivati uz računalne kriminalce, koje Pekka Himanen naziva krekeri.[4] Prvi su hakeri usvojili čvrste etičke vrijednosti i najčešće su bili studenti željni znanja i napredovanja u programiranju. Podržavali su slobodu govora, jednakost i demokraciju. Povezivala ih je ljubav prema tehnologiji, proširivanju znanja o programiranju i stvaranje virtualnog okruženja gdje su svi jednaki. Priželjkivali su dan kada će sve informacije biti besplatne i dostupne svima, a oni će biti ti koji će obezbijediti slobodno i sigurno virtualno okruženje.[5] To su bili prvi tragovi hakerske etike, poznate i pod nazivom „nethic“, koje se mnoštvo hakera i dalje drži i smatra je temeljnom vrijednosti koju svi hakeri trebaju usvojiti.[6] Ubrzo su se hakeri počeli udruživati u hakerske skupine, te su zajedno učili programirati i upoznavati čari interneta. Njihovi motivi su u većini slučajeva nevini, ali nekolicina hakera su svoje vještine hakiranja upotrebljavali za ostvarenje osobnih ciljeva.[7] Početkom 21. stoljeća dolazi do preokreta gdje ideološke i etičke vrijednosti postaju sekundarne, a materijalne i ekonomske primarne vrijednosti koje motiviraju hakere na rad.

Današnji hakeri definiraju se kao programerski stručnjaci usredotočeni na slabosti softvera, hardvera i računalne mreže. Međutim, po Pekki Himanenu, hakeri ne moraju imati veze s računalima, već oni mogu biti stručnjaci ili entuzijasti bilo kojeg područja. Postoji nekoliko vrsta hakera: *white hats* (bijeli šeširi), *grey hats* (sivi šeširi), *black hats* (crni šeširi), etički hakeri, haktivisti, *pen testers*, *script kiddies* itd. Vrste hakera nastale su na temelju znanja ili sposobnosti koje posjeduju i s pomoću kojih djeluju, te moralnih vrijednosti kojih se drže i koje mogu biti etički, zakonski ili osobno uvjetovane. Neki hakeri, kao što su *script kiddies*, ne moraju imati opsežno znanje o programiranju i tehnologiji, već koriste skripte i kodove za stvaranje programa

[4] Usp. Himanen, Pekka. Hakerska etika i duh informacijskog doba. Zagreb : Naklada Jesenski i Turk, 2002. str. 4.

[5] Nav. dj. Jaquet-Chiffelle, David-Oliver, str. 180-182.

[6] Nav. dj. Himanen, Pekka, str. 85.

[7] Usp. Radziwill, Nicole et. al. The Ethics of Hacking: Should It Be Taught? str. 3.

koje su stvorili iskusniji hakeri. Hakerski ciljevi mogu biti: dobronamjerni (stvaranje sigurnog digitalnog okruženja), ideološki (etičke vrijednosti i političko mišljenje), individualni (napredovanje vlastitih sposobnosti), i zlonamjerni (krađa podataka, cyber kriminal). Svaki hakeri imaju odgovarajuće principe i vrijednosti kojih se drže i poštuju prilikom ostvarivanja zadanih ciljeva. Haktivisti su hakeri koji iskorištavaju svoje programske sposobnosti i poznavanje internetskih sustava kako bi promicali vlastitu ideologiju, političko mišljenje ili neki drugi cilj za koji se zalažu. Haktivisti mogu djelovati samostalno ili u skupini, kao npr. Anonymous. Najčešća podjela hakera je na temelju njihovih etičkih vrijednosti i pridržavanja zakona i propisa, te se dijele na bijele, sive i crne šešire. White hats ili bijeli šeširi imaju vrlo visoke etičke vrijednosti i strogo se pridržavaju zakona, štite softver, hardver i internetsku mrežu od crnih hakera, poznatih po Pekki Himanenu i kao krekeri. Pen testers su bijeli hakeri, specijalizirani za ispitivanje sigurnosti klijentovog računalnog sustava. Etički hakeri su također podvrsta bijelih šešira, koji se pridržavaju službenih pravila i zakona koja štite klijenta i njegovu imovinu. Za takvu vrstu hakera najvažnije je uspostaviti i održati klijentovo povjerenje kako bi mogli uspješno upasti u računalni sustav, bez kršenja zakonskih propisa. Etički haker je naziv koji navodi na potpuno drugačiju sliku od stvarnosti, te bi točniji naziv bio „pouzdan i vjerodostojan haker“, a njegove vrijednosti poslovno, a ne etički orijentirane. Sve etičke vrijednosti, prema Jaquet-Chiffelleu, mogu se podijeliti u tri sloja: vrijednosti na osobnoj razini (perspektiva hakera), vrijednosti na poslovnoj razini (perspektiva tvrtke) i vrijednosti na društvenoj razini (globalna perspektiva). Etički hakeri prilikom „napadanja“ klijentovog sustava mogu otkriti poslovne tajne ili osobne podatke zaposlenika, no potpisivanjem ugovora haker se obvezuje na poslovnu šutnju.[8]

Black hats ili crni šeširi djeluju radi osobne koristi i redovito krše zakone i propise. Primaran je cilj crnih hakera pronaći i iskoristiti slabosti računalnih sustava, kako bi zloupotrebljavali osjetljive podatke i programe pogođenih organizacija i pojedinaca. Hakeri, koji se nalaze između bijelih i crnih šešira, nazivaju se grey hats ili sivi šeširi. Njihove namjere nisu zlonamjerne i nisu usmjereni prema ostvarivanju profita, ali za uspješno postizanje vlastitih ciljeva odbacuju zakone i etičke vrijednosti. Naposlijetku, postoje i hakeri koji mogu biti crni ili sivi šeširi, a poznati su po nezakonitom i neovlaštenom ulaženju i provaljivanju u računalne sustave. Kao rezultat tehnološkog napretka i sve raširenije prisutnosti digitalnih korisnika, uočio se i sve veći broj hakerskih napada, ali i novih vrsta hakera: cyber kriminalci, špijunski hakeri i hakeri

[8] Nav. dj. Jaquet-Chiffelle, David-Oliver, str. 182-190.

financirani od strane države. Cyber kriminalci idu korak dalje od crnih šešira, s ciljevima i motivacijom izbijanja cyber ratova.[9]

2.2. Hakerska radna etika

Od samih početaka hakeri se zalažu za korištenje, testiranje i razmjenu slobodnog znanja i programa te mogućnost zajedničke suradnje s drugim strastvenim programerima, radi dobivanja najboljih i najefikasnijih rezultata. Etička je dužnost hakera olakšati pristup informacijama i osigurati okruženje u kojem pojedinci imaju slobodu izražavanja i stvaranja u svrhu napredovanja znanja i opće dobrobiti čovječanstva. Haker je termin koji u osnovi ne mora biti vezan uz programiranje. Ukoliko pojedinac ima želju i strast za napredovanjem, istraživanjem i odgovornošću u bilo kojem zanimanju, onda se također može reći da je haker. Himanen uspoređuje hakersku radnu etiku s protestantskom, koja gleda na rad kao dužnost i obvezu koju pojedinac treba obaviti što kvalitetnije radi ostvarenja materijalnih i nematerijalnih sredstava. Za razliku od protestantske etike, hakerska je fleksibilnija s obzirom na strogost i efikasnost obavljenog zadatka, ali je uočena sličnost u strasti za obavljanjem posla. Hakeri nastoje ispuniti svoje strasti pa čak i ako to znači rješavanje monotonih zadataka i ulaganjem značajnog napora pri ostvarivanju ciljeva. Hakeri su usvojili fleksibilno radno vrijeme, odnosno optimizirali su vrijeme najbolje učinkovitosti rada i sačuvali vrijeme za zabavu. Posao nosi određenu odgovornost, no od ključne je važnosti osigurati mjesta za zabavu i slobodu kretanja van poslovnog okruženja. Neki hakeri u svoje slobodno vrijeme razvijaju programe i rješenja koje dijele s drugima, te na taj način razvijaju kvalitetu zajednice i okupljaju strastvene stručnjake koji će potom zajednički testirati i unaprijediti program. Besplatan pristup informacijama koje su proizveli drugi pojedinci, a zadržavanje znanja i iskustava za vlastite potrebe smatra se neetičkim ponašanjem hakera. Dvije temeljne obveze kojih se svi trebaju držati su: pravilno navođenje izvora te objavljivanje ideja i rezultata u korist znanstvene zajednice. Eric Raymond uspoređuje otvoreni poslovni model hakera s tržnicom, gdje svatko ima pristup informacijama i može izraziti svoje mišljenje te sudjelovati u izgradnji novih projekata i ideja, dok je zatvoreni poslovni model usporedio s katedralom, gdje je sav posao isplaniran, te je vidljiv samo završni produkt. Pojam nethic savršeno povezuje i opisuje ključnu

[9] Isto.

vrijednost umreženog društva, koje se može razvijati i surađivati samo ako se poštuju određene vrijednosti u internetskom okruženju.[10]

Manuel Castelss navodi da se od informacijskih stručnjaka zahtjeva konstantno usavršavanje vlastitih znanja i sposobnosti jer se svijet ubrzano kreće, dok se društvene promjene svakim danom mijenjaju. Razlikuje se sedam vrijednosti osobnog razvoja: odlučnost, optimalnost, fleksibilnost, stabilnost, industrija, novac i rezultat odgovornosti. Usvajanjem navedenih vrijednosti osobnog razvoja hakeri postaju motivirani prema ispunjavanju specifičnih ciljeva, a vrijednost koja najviše motivira ljude na rad je novac, dok ostale vrijednosti pomažu u ostvarenju postavljenih ciljeva.[11] Svijet je postao previše orijentiran prema ostvarivanju materijalnih sredstava, te se kao takvo naziva kapitalističko društvo. Neki hakeri odbacuju etičke vrijednosti ako to znači da će ostvariti više novaca i većeg statusa u društvu. Takvi postupci sve više udaljavaju hakere od njihovih prvotnih vrijednosti, te ne predstavljaju dobar primjer ponašanja na internetu mladim korisnicima.

Steven Levy navodi osam obilježja hakerske etike: pristup računalima, sloboda informacija, promoviranje decentralizacije, vrednovanje sposobnosti, umjetnost hakiranja i pozitivan utjecaj računala. Već je i prije spomenuta važnost slobodnog pristupa informacijama i kako svatko treba imati jednaka prava na znanje, ali se često zaboravlja da neki pojedinci još uvijek ne posjeduju računala i internetsku vezu ili ne znaju koristiti novu tehnologiju, odnosno nisu informatički i informacijski pismeni. Potrebno je svima osigurati računalnu opremu i mrežu kako bi postali dio umreženog društva koji se svakim danom sve više širi. Također, promicanje besplatne razmjene i dijeljenja informacija ostvaruje se otvornim sustavom bez bilo kakvih društvenih, tehnoloških, socijalnih i drugih osobnih razlika. Hakeri se vrednuju na temelju programerskih sposobnosti prema stručnim kriterijima, a ne po rasi, spolu, stupnju obrazovanja ili socijalnom položaju. Na hakiranje se počelo gledati i kao novom umjetnošću, jer postoje različiti stilovi, odnosno načini pisanja kodova, u čemu je prepoznata ljepota stvaranja i pisanja što kraćih kodova. Utjecaj tehnologije je uvelike promijenio i obogatio društveni život zajednice, a da nije bilo hakera ne bi bilo ni računala. Hakeri su bili ti koji su prepoznali potencijal računala i utjecaj koji će imati na život pojedinca u budućnosti. Oni predstavljaju uzor korektnog ponašanja drugim korisnicima, usvajanjem etičkih vrijednosti i zalaganjem za primarne ciljeve djelovanja. Da su svi

[10] Nav. dj. Himanen, Pekka, str. 6-100.
[11] Nav. dj. Himanen, Pekka, str. 113-127.

korisnici računala usvojili hakersku etiku i koristili tehnologiju u svrhu razvijanja novih ideja, svijet bi danas bio napredniji i povezaniji.[12]

2.3. Hakerski napadi

Hakeri su u prošlosti bili odgovorni za različite vrste napada, kao što su: terorizam, krađa osobnih podataka, napadanje državnih sustava itd. Poznato je da hakerski napadi ugrožavaju sigurnost iznimnoj količini uređaja koji su povezani s internetom, a neki od njih su: prijevozna sredstva (automobili, avioni, vlakovi), kućanski aparati (hladnjaci, sigurnosne kamere), medicinski uređaji itd. 2015. godine hakeri su uspjeli ući u sustav automobila marke Jeep Cherokee, te su uspjeli upravljati autom, onemogućiti kočenje i ugasiti motor. Na svu sreću, nije bilo većih posljedica, osim što je napad ukazao na nedostatke sigurnosti automobila, kao i nedostatnu spremnost stručnjaka koji su radili na sustavu. Nakon tog hakiranja, automobilska kompanija Fiat odlučuje opozvati proizvodnju 1.4 milijun automobila, kako ne bi došlo do sličnih hakerskih napada u budućnosti. No, samo zaustavljanje proizvodnje nije dovoljno u rješavanju hakerskog problema. Cilj ovog napada bio je ozlijediti ljude i napraviti štetu, no svejedno je skrenuo pozornost na nedostatke automobila i njegovog sustava, koji se zatim mogu popraviti i usavršiti.[13] Hakere, kojima je cilj ozlijediti pojedince, potrebno je kazniti zakonom. Potrebno je osmisliti međunarodne mjere i propise, koji su jednaki u svim zemljama, tako da se ljudski životi ne bi dovodili u opasnost. Još jedan sličan slučaj hakerskog napada dogodio se u Poljskoj kada je četrnaestogodišnji dječak, u šali, uspio provaliti u sustav upravljanja vlakovima i promijenio smjer nekoliko tračnica, uzrokujući iskakanje i sudaranje vlakova, ali i ozljede putnika.[14] Ovaj primjer služi kao dokaz da hakerski napad može počiniti bilo tko, pa tako i maloljetnici, koji ne shvaćaju i ne prepoznaju težinu opasnosti i posljedica do kojih može doći kao rezultat njihovih postupaka.

U većini slučajeva cilj hakerskih napada su poticanje društvenih, političkih ili ekonomskih šteta s trajnim učinkom, no neki napadi se događaju u svrhu podizanja svijesti internetskog osiguranja, te su oni uzrokovani etičkim hakerima ili haktivistima. 2020. godine etički su hakeri napali 28,000 printera i putem njih isprintali upute za sprječavanje budućih hakiranja. Hakiranje

[12] Usp. Levy, Steven. Hackers : heroes of the computer revolution. Garden City, N.Y. : Anchor Press/Doubleday, 1984. str. 27-38.

[13] Nav. dj. Beale, Sara Sun, str. 164-165

[14] Isto.

printera pokazalo se kao dobar potez u jačanju sigurnosti jer je pomoću tražilice Shodan, alat kojim se služe hakeri i istraživači sigurnosti, identificirano više od 800,000 printera za koje se ispostavilo da su lak plijen za hakiranje.[15] Sličan napad haktivista dogodio se i 2018. godine kada je napadnuto više od 100,000 printera, na kojima je isprintana poruka da je printer hakiran, kako ga zaštititi i zapratiti najvećeg YouTuber-a po imenu PewDiePie. Na isprintanim uputama preporuča se redovito ažuriranje uređaja koji su povezani na printer, preuzimanje najnovijih sigurnosnih programa i odspajanje uređaja sa interneta. Etički hakeri također, iako im je bio cilj pomoći iz opravdanih razloga, napadaju i krše zakon zauzimajući ulogu procjenitelja kvalitete i sigurnosti. Hakeri su mogli uništiti printere, no odlučili su unaprijediti kvalitetu sigurnosti i na isprintanim papirima ostavili svoje kontakt podatke ukoliko vlasnici printera zatrebaju dodatnu pomoć oko zaštite uređaja. Činjenica je da su hakeri napali printere, no mrežni stručnjaci su trebali na vrijeme predvidjeti potencijalne probleme i slabosti vlastite organizacije i opreme.[16]

Za svakodnevnu uporabu u privatnom ili poslovnom okruženju koristi se tehnologija, koja je po cijeni prilično povoljna sa svim potrebnim značajkama, no nedovoljno zaštićena i kvalitetna. Neka obilježja nedovoljne zaštite su nemogućnost: promjene jednostavnih zadanih lozinki uređaja, automatsko ažuriranje sustava, ne prepoznavanje virusa koji su zahvatili uređaj itd.[17] Kako bi se u budućnosti što više zaštitili od hakerskih napada potrebno se informirati kako hakeri napadaju i kako spriječiti njihove napade, odnosno koje mjere je potrebno poduzeti za osiguravanje privatnih podataka i uređaja od strane hakera.

2.3.1. Zloupotreba osobnih podataka

Kao što je već navedeno, tehnološki razvoj utjecao je na stvaranje novog društva, potaknuo je društvene promjene koje utječu na sve aspekte ljudskog djelovanja u povezanom okruženju. Internet postaje sve brži, dostupniji i jednostavniji za uporabu, pogotovo mlađim generacijama koje su odrasle s pametnim mobitelima i društvenim mrežama. Informacije se nalaze svuda oko nas, te su u digitalno vrijeme postale glavni izvor prihoda divovskim internetskim velesilama, Google i Facebook. Tvrtke pokušavaju ostvariti profit posjedovanjem informacija putem patenata,

[15] Usp. Mathews, Lee. Nearly A Million Printers At Risk Of Attack, Thousands Hacked To Prove It. Forbes, 2020.

[16] Usp. Tidy, Joe. PewDiePie printer hackers strike again. BBC, 2018.

[17] Nav. dj. Beale, Sara Sun, str. 167.

autorskih prava i intelektualnog vlasništva. Sustav koji čuva te informacije sličan je zatvoru kojem nitko nema pristup, za razliku od otvorenosti i dostupnosti za koju se hakeri i pirati bore.[18] Clough ističe da s obzirom na povećanu uporabu tehnologije, a pogotovo društvenih mreža, svakim danom smo izloženiji opasnostima interneta.[19] Svakim specijaliziranim pretraživanjem informacija, oblikuje se digitalni identitet pretraživača, te se stvaraju ciljani oglasi na temelju informacija prikupljenih u profilu pretraživača.[20] Svatko može pristupiti beskrajnom mnoštvu osobnih podataka, koji plutaju na internetu samo je potrebno znanje i sposobnosti za njihovo pronalaženje i naposlijetku zloupotrebu. Zloupotrebom osobnih podataka smatra se bilo kakvo neovlašteno i nezakonito korištenje tuđih podataka u svrhu daljnje prodaje na tržištu ili za ostvarenje osobnih motiva hakera.

Mnoge tvrtke, institucije i pojedinci su nažalost bili žrtva hakerskog napada. U Tablici 1. prikazano je pet najvećih hakerskih napada prema broju ukradenih korisničkih podataka. Jedan takav napad zahvatio je tvrtku Adobe 2013. godine kada je ukradeno tri milijuna zapisa o kreditnim karticama potrošača i njihovi prijavni podaci (korisničko ime i lozinka). Kasnije je utvrđeno da je broj ukradenih podataka puno veći od zabilježenog. 2015. godine Adobe je bio primoran svojim korisnicima platiti novčanu odštetu od 1.1 milijuna dolara zbog kršenja i nepoštovanja njihovih prava i osobnih podataka. No, ipak najveća krađa i zloupotreba podataka zahvatila je poznatu internetsku tražilicu Yahoo. Tvrtku su napali hakeri koji su se predstavili kao hakeri sponzorirani od strane države, te su preuzeli osobne podatke 500 milijuna korisnika. Yahoo je bio žrtva još nekoliko hakerskih napada nakon toga, te je naposlijetku doživio slom 2017. godine. Na Tablici 1 nalazi se popis najvećih krađa osobnih podataka u svijetu iz čega je vidljivo da je Yahoo najviše pogođen.[21]

Tablica 1. Najveći hakerski napadi po CSO[22]

	Tvrtka	*Godina*	*Opseg napada*
1.	Yahoo	2013. – 2014.	3 milijarde korisničkih računa
2.	Sina Weibo	2020.	538 milijuna korisničkih računa
3.	Marriott International	2014.-2018.	500 milijuna korisničkih računa

[18] Nav. dj. Himanen, Pekka, str. 45.

[19] Usp. Drew, J. A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. // Journal of Criminological Research, Policy and Practice 6, 1(2020). str. 18.

[20] Nav. dj. Amer, K.; Noujaim, J. The Great Hack. Netflix, 2019.

[21] Usp. Swinhoe, Dan. The 15 biggest data breaches of the 21st century**.** CSO, 2021.

[22] Tablica prikazuje pet najvećih hakerskih napada prema broju ukradenih korisničkih podataka (Swinhoe, D.)

4.	Adult Friend Finder	2016.	412.2 milijuna korisničkih računa
5.	My Space	2013.	360 milijuna korisničkih računa

Facebook je kao najpoznatija društvena mreža nekoliko puta bila suočena s hakerskim napadima i krađom osobnih podataka dvije milijarde svojih korisnika.[23] Najnoviji napad dogodio se u travnju ove godine kada je 533 milijuna mobilnih brojeva i drugih osobnih podataka Facebook korisnika ukradeno i objavljeno od strane hakera. No, slučaj koji se dogodio 2019. godine imao je najveće financijske i etičke posljedice za Facebook i njegove korisnike.[24] Cambridge Analytica je tvrtka odgovorna za prikupljanje osobnih podataka američkih glasača u svrhu prikupljanja i upravljanja informacijama koje potencijalni glasači dobivaju na društvenim mrežama. Na temelju podataka koje pojedina osoba postavlja na svoj profil različitih društvenih mreža (Facebook, Twitter, Instagram), oblikovali su se oglasi koji iznose lažne informacije o Trumpovim protukandidatima. Mark Zuckerberg, osnivač Facebook-a, je pojasnio da nije bio obaviješten o prirodi poslovanja Cambridge Analyticae, ali šteta je već bila učinjena. Otkriveno je da društvena mreža nije na adekvatan način zaštitila podatke svojih korisnika, već ih je otvoreno izložila i time na jednostavan način omogućila njihovu zloupotrebu (The Great Hack, 2019: 52:00).[25]

Naše ponašanje na internetu je predvidljivo. Svaki pojam koji smo ikada pretraživali, svaku stranicu koju smo posjetili, svaka narudžba, zabilježena je u našim mobitelima i računalima.[26] Na temelju našeg digitalnog otiska i mrvica koje ostavljamo na internetu izbacuju nam se reklame, koje su dizajnirane i personalizirane isključivo za naše oči (The Great Hack, 2019: 10:02).[27] Od iznimne je važnosti zaustaviti daljnje zloupotrebe osobnih podataka pojedinaca. Nakon svakog preuzimanja aplikacije ili posjećivanja stranice prihvaćamo uzimanje naših podataka, IP adrese, kolačića itd., ali ne znamo gdje ti podaci odlaze. Kao što je bio slučaj s Cambridge Analyticom, koja je na temelju glasačkih profila upravljala oglasima na Facebook-u i neizravno utjecala na potencijalne glasače. Treba se razviti svijest u umreženom društvu da njihovi podaci na internetu nikada neće u potpunosti biti sigurni i kako bi se zaštitili od moguće zloupotrebe trebaju redovito mijenjati lozinke, ažurirati sustav i instalirati antivirusne programe itd.

[23] Nav. dj. Drew, J. str. 18.

[24] Usp. Holmes, A. 533 million Facebook users' phone numbers and personal data have been leaked online. Insider, 2021.

[25] Nav. dj. Amer, K.; Noujaim, J. The Great Hack. Netflix, 2019.

[26] Nav. dj. Himanen, Pekka, str. 98-100.

[27] Nav. dj. Amer, K.; Noujaim, J. The Great Hack. Netflix, 2019.

2.4. Zakoni i propisi

Za razliku od ostalih zločina, koji su fizičke prirode, istraživanje i kažnjavanje računalnih napada je značajno teže, jer ne postoji fizički dokaz i trag koji upućuje na određenog prekršitelja zakona. Moguće je pratiti digitalne mrvice i otiske, ali zbog iznimne količine korisnika interneta i potencijalnih počinitelja potraga postaje iscrpljujuća, s obzirom na financijske i ljudske resurse osigurane za istragu, te se vremenom gubi trag i pronalazak postaje nemoguć. Najčešći dokazi koji upućuju na određene počinitelje su lokacija računala sa kojeg se vršilo hakiranje u obliku IP adrese, koja je zabilježena na napadnutom računalu. Ponekad su postupci istrage etički upitni, jer krše iste one zakone kao i hakeri, odnosno pokušavaju pronaći počinitelja ponovnim hakiranjem.[28] Istraga ovakve prirode je dugotrajan proces, ali to ne znači da treba odustati, jer je potrebno kazniti kršenje zakona u svim oblicima, u suprotnom će hakeri nesmetano surfati internetom i nastaviti napadati sve dok ne postignu cilj s iznimnim posljedicama na cjelokupno virtualno društvo.

Zakon Computer Fraud and Abuse Act (CFAA) nastao je u svrhu kažnjavanja hakera koji namjerno i neovlašteno napadaju privatno i poslovno vlasništvo, što uključuje programe, podatke, kodove ili naredbe, te uzrokuju značajnu štetu i posljedice. Zakon, u užem smislu, zabranjuje neovlašten pristup: podacima o nacionalnoj sigurnosti (10 godina zatvora), podacima organizacija putem osiguranog računala (1-5 godina zatvora), trgovanje lozinkama (1 godina zatvora), računalna prijevara i oštećivanje računala (5 godina zatvora).[29, 30] Još neki od zakona su The Stored Communications Act, koji štiti podatke elektroničke komunikacije (e-pošta, SMS, *chat*-ovi društvenih mreža), The Electronic Communications Privacy Act, koji zabranjuje presretanje komunikacije tj. štiti "podatke u pokretu" i The Defend Trade Secrets Act, koji zabranjuje pristup i širenje nacionalnih podataka zaštite.[31] Poštivanjem navedenih zakona stvara se slika hakera koji predstavljaju uzor ponašanja na internetu za buduće programere i internetske korisnike. Svi hakeri se trebaju držati zakonskih propisa, a ukoliko se ne slažu s njima ne bi trebali ilegalno djelovati i kršiti zakon, već je potrebno udružiti snage i osmisliti plan putem kojeg će se boriti za veću dostupnost sadržaja, transparentnost i opća prava..

[28] Nav. dj. Beale, Sara Sun, str. 189-191.
[29] Nav. dj. Beale, Sara Sun, str. 169.
[30] Usp. FindLaw. Hacking Laws and Punishments, 2019.
[31] Isto.

3. Piratstvo

3.1. Pirati nekada i sada

U prošlosti su se termini pirati i piratstvo koristili prilikom opisivanja najvećih kradljivaca na moru, a danas se ti termini povezuju uz tzv. digitalne pirate, koji za razliku od tradicionalnih pirata surfaju internetom. Originalni su pirati bili aktivni od 15. do 18. stoljeća. Živjeli su na moru te su napadali druge brodove i mornare s ciljem krađe njihovih ljudskih i financijskih resursa.[32] Uspoređujući pirate iz prošlosti i sadašnjosti uviđaju se sličnosti u cilju, odnosno motivima iza krađe. Danas su najaktivniji digitalni pirati koji ilegalno reproduciraju digitalne sadržaje kao što su: filmovi, programi, knjige i glazba, radi njihove prodaje zainteresiranim potrošačima i veću dostupnost digitalnog sadržaja.[33] Uz termin piratstva, mogu se nalaziti i pridjevi digitalni ili internetski pirati. Krajem 20. stoljeća najčešći oblik piratstva bila je krivotvorina DVD-a, CD-a, poznatih marki odjeće i drugih poznatih proizvoda, odnosno kopiranje fizičkih medija. Početkom 21. stoljeća taj se trend mijenja i piratstvo se seli u digitalne vode, kao i ostatak svijeta. Pirati pronalaze i pristupaju originalnom sadržaju, koji potom kopiraju i dijele s internetskom zajednicom na nekoliko načina: snimanjem filmova u kino dvoranama, kopiranjem originalnih DVD-a, otkrivanjem originalnih kopija i pomoću streaming usluga.[34] Također je bitno napomenuti da je glavni pokretač pirata, pa tako i hakera, povećanje dostupnosti sadržaja i transparentnosti samog postupka dobivanja i preuzimanja sadržaja. Pirati nastoje osigurati zajedničko okruženje u kojem svi korisnici imaju pristup besplatnom sadržaju, no vlasti ne prihvaćaju takvo ponašanje kao dobronamjerno zbog narušavanja autorskih prava. Vodeće se vlasti i pirati nastavljaju boriti oko uloge autorskog prava, za koje pirati smatraju da nije adekvatno u novo vrijeme kada informacije trebaju biti dostupne, spremne na korištenje i daljnje izmjene.[35]

Piratstvo predstavlja svaki oblik neovlaštenog i nezakonitog korištenja i širenja autorskih djela, koja su zaštićena autorskim pravima na različitim medijima. Postoje različite podjele piratstva na temelju: okruženja, sadržaja, etičkih (osobnih/moralnih) vrijednosti i ostalih motiva iz kojih piratiziraju. Okruženje u kojem pirati pružaju sadržaj korisnicima može biti fizičko ili

[32] Usp. Royal Museums Greenwich. The Golden Age of Piracy.

[33] Usp. Piracy. Cambridge Dictionary.

[34] Usp. Smart protection. How does online piracy of movies and TV series actually work?, 2019.

[35] Usp. Fredriksson, Martin. Copyright Culture and Pirate Politics. // Cultural Studies 28, 5-6(2014). str. 9-10.

digitalno. Fizičko se piratstvo odnosi na prodaju neovlaštenih fizičkih medija korisnicima uživo, tj. u četiri oka, dok se digitalno piratstvo veže uz internetsku reprodukciju i dostupnost ilegalnog sadržaja korisnicima. Piratizirani sadržaj podrazumijeva različite vrste medija, u kojima se ono može pojaviti, a neki od najčešćih su: pdf, torrent, mp3 ili mp4 dokumenti. Također, na temelju motiva, odnosno svrhe njihovog piratiziranja, postoje sivi i crni pirati. Sivo piratstvo se definira kao neovlašteno korištenje i dijeljenje krivotvorenog izvornog sadržaja u svrhu povezivanja i stvaranja jednog zajedničkog okruženja u kojem se korisnicima sve nalazi na dodir ruke. Neovlaštena reprodukcija izvornog sadržaja i dijeljenje široj javnosti u svrhu osobne koristi i zanemarujući zakonske odredbe naziva se crno piratstvo.[36] Na temelju razne literature o piratima, razlikuju se dvije vrste glazbenih pirata, štedljivci i istraživači. Štedljivci su karakterizirani kao pirati koji smatraju da su cijene pjesama i albuma preskupe, pa zato preuzimaju legalno glazbu, dok pirati istraživači preuzimaju glazbu zbog pronalaženja zanimljivih pjesama, koje bi potencijalno u budućnosti legalno kupili.[37]

3.2. Neovlašteno dijeljenje i preuzimanje sadržaja

Dijeljenje sadržaja definira se kao proces distribucije informacija putem pametnih uređaja i interneta između skupine korisnika, poznate još i kao P2P mreže. Najpoznatije stranice ili tražilice piratskog sadržaja su: The Pirate Bay, Kick-Ass Torrents i TorrentReactor, na kojima se mogu pronaći torrent datoteke i potom se preuzeti putem protokola BitTorrent. Navedene stranice ne prihvaćaju pravnu odgovornost, jer smatraju da piratski sadržaji nisu uistinu pohranjeni na njihovoj domeni.[38] Nakon pribavljanja kopije originala, pirati postavljaju kopiju na neku od piratskih stranica u nadi da će korisnici odlučiti preuzeti njihov ilegalan sadržaj, na temelju čega bi u konačnici ostvarili profit. Piratske domene mogu imati nekoliko web stranica na kojima pohranjuju digitalni sadržaj. Web stranice su jednostavno dizajnirane kako bi dočarale sliku pristupačnog i user-friendly sučelja u kojem korisnici imaju potpunu slobodu interakcije, no u pozadini stranice vrebaju određene opasnosti.[39]

[36] Usp. Stop krivotvorinama. Krivotvorenje i piratstvo.

[37] Usp. Dörr, J. et. al. Music as a Service as an Alternative to Music Piracy? // *Business & Information Systems Engineering* 5 (2013). str. 383.

[38] Usp. Cox, J.; Collins, A. Sailing in the same ship? differences in factors motivating piracy of music and movie content. // Journal of Behavioral and Experimental Economics 50(2014). str. 70-71.

[39] Nav. dj. Smart protection.

Razlikuju se dvije metode distribucije piratskog sadržaja: Peer to Peer (P2P) i piratske domene. Naziv P2P označava metodu dijeljenja i razmjene datoteka putem raznih P2P mreža, odnosno prenošenje sadržaja s različitih osobnih računala i njihovo povezivanje pomoću Bit Torrent protokola. Druga je metoda postavljanje i slobodan pristup kopiranim datotekama na piratskim domenama. Postoji nekoliko načina kojima pirati mogu ostvariti zaradu: naknadom web stranice, oglašavanjem, oglasnim prijevarama, prodajom korisničkih podataka i članarinom Premium korisnika. Svakim preuzimanjem pirati dobivaju određenu naknadu od strane domene, na principu broja pregleda od strane javnosti, i Premium korisnika, koji dodatno naplaćuju usluge zbog bolje kvalitete sadržaja i brzine preuzimanja. Također, jedna od negativnih strana s kojom mnogi korisnici nisu upoznati je činjenica da pirati imaju pristup osobnim podacima svakog korisnika i da njihove profile, ukoliko to žele, mogu prodati zainteresiranim kupcima.[40] No, nisu svi pirati uspješni u krađi podataka i kopiranju umjetničkih radova. Porastom reproduciranog digitalnog sadržaja, autori ugrađuju jedinstveni nevidljivi vodeni žig u medijske datoteke, koji se može prepoznati samo pomoću profesionalnih računalnih programa. Na taj način vlasnici mogu jednostavno utvrditi tko koristi, kopira te na kojim platformama objavljuje izvorni sadržaj. Primjerice, kada YouTube korisnik objavi kopirani video, sustav za prepoznavanje žiga obrađuje i uspoređuje žig, kako bi utvrdio postoji li podudaranje s drugim žigovima unutar baze podataka.[41]

Digitalno je doba promijenilo prirodu ljudskog ponašanja što je rezultiralo stvaranjem novih obrazaca potrošnje i korištenja digitalnog sadržaja u odnosu na fizički.[42] CD-ovi i DVD-ovi su postali dio prošlosti, a zamijenili su ih digitalni mediji mp3 i mp4. Internet je dostupan svima i kao takav omogućuje pretraživanje i pristup digitalnim podacima i datotekama, čiji autori nisu uvijek poznati i vjerodostojni. Pojavom i razvijanjem internetskih usluga i informacija koje plutaju internetom ljudi konzumiraju trenutne informacije plitke tematike, neovisno o njihovoj kvaliteti, provjerljivosti i autorstvu. Sve većem broju internetskih korisnika preuzimanje digitalnog sadržaja postaje uobičajeno i dio njihove svakodnevice. No, nije svako preuzimanje sadržaja negativno. Određeni autori žele omogućiti pristup i daljnju reprodukciju vlastitih djela svima i time promovirajući svoj rad i širiti sadržaj većem broju ljudi. Naravno, samim preuzimanjem određenih sadržaja postiže se traženost djela pa na taj način piratstvo može poslužiti kao dobar alat u razvijanju riječi i znanja. Kao prilog pozitivnim stranama navodi se izjava Jeff Bewkesa, koji priznaje da je serija Game of Thrones najraširenija serija na svim piratskim stranicama i kao takva

[40] Usp. Varsani, Jayesh. Fighting against digital piracy in the streaming age. Cartesian, 2019.

[41] Nav. dj. Smart protection.

[42] Usp. Dilmperi, A.; King, T.; Dennis, C. Pirates of the web: The curse of illegal downloading. Journal of Retailing and Consumer Services 18, 2(2011). str. 133-135.

dostupna većem broju ljudi, te se promovira kao odlična serija, koju svatko treba pogledati pa barem i preko piratskih stranica. Mediji stvaraju negativnu sliku pirata koji svakodnevno krše zakon i narušavaju sigurnost interneta, ali se zanemaruju ciljevi koji stoje iza takvih postupaka. Pirati nastoje omogućiti transparentnost, dostupnost i dijeljenje sadržaja s drugim korisnicima, koji zahtijevaju slobodan pristup sadržaju, kao jednim od osnovnih ljudskih prava. Piratstvo je postalo društveno prihvatljivo, iako je ilegalno, jer promiče povezanost i dostupnost svih sadržaja. Povećava se broj ljudi koji se zalažu za ciljeve piratstva i podupiru piratske stranke, čime se slika piratstva kao zločina mijenja u etičko piratstvo, koje nije u potpunosti tamno.[43]

Podaci istraživanja (Cox J. & Collins, A.) ukazuju na to da ljudi stariji od 30 godina, zbog većih prihoda, kupuju glazbu, filmove i knjige, dok mlađi ljudi, zbog manjih prihoda i većeg poznavanja interneta i tehnologije u prosjeku više preuzimaju digitalne sadržaje. Mlađe generacije, koje su odrasle s internetom, ne prepoznaju neovlašteno preuzimanje sadržaja kao kršenje zakona i navode kako industrija zarađuje previše novaca i da su cijene digitalnog sadržaja preskupe. Istraživanje je, također, pokazalo da samo 5% generacije Y smatra piratstvo kao etički i moralno neprimjerenom aktivnosti, ipak većina mladih potrošača nema osjećaj krivnje prilikom preuzimanja ilegalnog sadržaja, te vjeruju kako bi digitalni sadržaj trebao biti besplatan i dostupan svima na korištenje, što ide u prilog piratskim motivima djelovanja. Rezultati navedenog istraživanja pokazali su kako se pirati ne boje kršenja zakona, odnosno ne vjeruju da mogu biti uhvaćeni i kažnjeni za svoje postupke, koji su imali značajne posljedice za filmsku i glazbenu industriju.[44] Poznavajući činjenicu da je sadržaj dostupan besplatno, mnogi se odlučuju za takvo korištenje, no time ujedno povećavaju mogućnost sigurnosnih rizika njihovim ilegalnim preuzimanjem.[45]

Filmoljupci žele pogledati što veći broj filmova, koji ponekad nisu dostupni u njihovoj zemlji ili se ne prikazuju na velikim ekranima. Kako bi smanjili udaljenost između sebe i filmova, spas pronalaze na internetu, na stranicama koje su krcate filmovima i koje naizgled izgledaju pristupačne i legalne. Ilegalni filmovi su često lošije kvalitete, zvuka i slike, pune virusa koji mogu napasti osobno računalo i lažnih oglasa čiji je cilj zavarati korisnika. Takve stranice narušavaju zadovoljstvo gledanja, odnosno odvlače pozornost i uništavaju iskustvo konzumiranja sadržaja. Svjesni opasnosti i negativnih strana piratiziranja, sve više korisnika prestaje upotrebljavati ilegalne usluge takve vrste i odlučuju se za kupovinu originalnog sadržaja ili korištenje streaming

[43] Usp. Ravenscraft, Eric. How Piracy Benefits Companies, Even If They Don't Admit it. Lifehacker, 2014.
[44] Nav. dj. Cox, J.; Collins, A. str. 70.
[45] Nav. dj. Dilmperi, A., str. 141-142.

usluga.[46] Također, ljubitelji glazbe motivirani su zadovoljavanjem potrebe za slušanjem što većeg broja pjesama, otkrivanja novih umjetnika i žanrova, te dijeljenja pronađenog sadržaja s drugima, a ne namjernom željom kršenja zakona.[47] Ponekad je teško prevagnuti između odabira vlastitih potreba i želja, te moralne odgovornosti dijeljenja i preuzimanja sadržaja na internetu. Nakon svakog ilegalnog preuzimanja stvara se navika i pojedinci svoje postupke više ne percipiraju kao kršenje zakona. Međutim, u istraživanju autora Dilmperi, A., King, T. i Dennis, C., rezultati pokazuju da ilegalno preuzimanje glazbe pojedincima nije isto što i krađa CD-a i DVD-a iz trgovine. Krađa CD-a je ozbiljnija jer se odvija u fizičkom okruženju, gdje postoji veća šansa kažnjavanja kradljivaca od strane vlasti. Vlada, industrija i vlasnici intelektualnog sadržaja vode borbu protiv ilegalnog preuzimanja, jer time korisnici oduzimaju prihod i publicitet originalnog sadržaja. Diskografske kuće, sa željom iskorjenjivanja piratstva, odlučuju poduzimati pravne postupke protiv kradljivaca originalnih dijela ili piratske stranice na kojima se nalazi ukraden sadržaj (Usborne, 2010).[48]

3.3. Streaming vs. Piratstvo

Piratstvo je imalo velike posljedice na razna područja intelektualnog sadržaja, no najviše filmsku i glazbenu industriju. 2000. je godine profit prodaje glazbe iznosio 27 milijardi dolara, dok je deset godina kasnije taj broj pao na 15 milijardi dolara.[49] Otkazivanje serije Hanibal, dolazi u prilog razočaravajućim podacima. Naime, američka psihološka serija nalazila se među top 5 na listi ilegalnog preuzimanja 2013. godine, te se to smatra kao jedan od razloga njezinog otkazivanja.[50] Profit glazbene i filmske industrije je od iznimne važnosti za glazbenike, glumce, redatelje i ostale umjetnike, odnosno autore kreativnog sadržaja. Kao rezultat smanjenog profita i interesa javnosti za kupovinom originalnog sadržaja, pojavljuje se mogućnost gubitka ulaganja u umjetnike, njihova djela, te izbijanje negativnih promjena u stvaranju društvene i kulturne dobrobiti. Doista, piratstvo je imalo značajne posljedice na industriju, ali također je otvorilo i

[46] Usp. Jacobs, R. S.; Heuvelman, A.; Tan, M.; Peters, O. Digital movie piracy: A perspective on downloading behavior through social cognitive theory. // Computers in Human Behavior 28, 3**(2012). str.** 966-967.

[47] Usp. LaRose, R.; Kim, J. Share, steal, or buy? A social cognitive perspective of music downloading. // Cyberpsychology & Behavior 10, 2(2007). str. 268.

[48] Nav. dj. Dilmperi, A., str. 141-142.

[49] Usp. Danaher, Brett et. al. The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France. // ERN: Integration (Topic) (2014). str. 3-4.

[50] Nav. dj. Varsani, Jayesh.

mogućnost udruživanja „dobrih“ pirata u piratske stranke, stvaranje novih oblika sadržaja i širenje interesa javnosti o problematici piratstva.

U posljednjih nekoliko godina, te pogotovo za vrijeme COVID-19 epidemije, korištenje streaming usluga doživjelo je veliki porast u cijelom svijetu. Streaming usluge omogućuju pristup najnovijim i najtraženijim filmovima, serijama i glazbi. Najpoznatija svjetska streaming platforma filmova i serija je Netflix, koja je 2010. godine proširila svoje usluge iznajmljivanja filmova u streaming uslugu, koju danas koristi 148 milijuna korisnika. Streaming usluge funkcioniraju na način sličan iznajmljivanju sadržaja, ali u digitalnom obliku, koji onda mogu gledati ili slušati neodređen broj puta. Za razliku od ilegalnog preuzimanja sadržaja, koji se nakon završetka preuzimanja može gledati bilo gdje, korištenje i pristup streaming uslugama zahtjeva konstantnu povezanost s internetom. Naravno, opće poznato je da se piratiziranjem sadržaja otvaramo mnogim opasnostima, kao što su virusi, krađa podataka pa čak i zatvor ili plaćanje novčanih kazni, ali pojedinci se i dalje odlučuju za ilegalno preuzimanje naspram streamingu.[51] Naime, neke negativne strane streaming usluga su cijena i nemogućnost posjedovanja digitalnog sadržaja. Stranice streaming usluga kao što su Netflix, Disney+ i Amazon Prime, naplaćuju korisnicima mjesečno korištenje njihovih usluga i omogućuju preuzimanje sadržaja, ali samo u određenom razdoblju.

Platforma Napster, koja je bila popularna početkom 21. stoljeća, povezivala je osobna računala i omogućavala svojim korisnicima pristup digitalnim sadržajima drugih korisnika. Cilj je Napstera bio omogućiti pristup i pronalazak raznovrsne glazbe bez potrebe plaćanja korištenja njihove usluge. 2000. je godine Američko udruženje za snimanje tužilo platformu Napster, koju su koristili 44.6 milijun korisnika. Zbog nepoznavanja tehnologije, zakona, dijeljenja i preuzimanja digitalnog sadržaja, Napster je morao zaustaviti svoje poslovanje i platiti troškove pohranjivanja neovlaštene glazbe.[52] Iako je Napster izgubio bitku sa zakonom, omogućio je stvaranje i razvoj svijesti, odnosno okruženja, u kojem je digitalan sadržaj dostupan svima, u bilo kojem trenutku i to besplatno. Deset godina kasnije, slučaj Napster poslužio je kao polazna točka za nove načine širenja i preuzimanja sadržaja za korisnike u cijelom svijetu.[53] U današnje vrijeme, Spotify pruža slične usluge svojim korisnicima. Spotify sadrži gotovo sve albume i pjesme ikad objavljene, a funkcionira na principu mjesečnog plaćanja korištenja usluge slušanja glazbe ili

[51] Usp. Derakhti, A. et. al. Streaming or misbehavior, investigation on movie streaming or movie piracy. // Dyna 87, 215(2020). str. 1-5.

[52] Usp. Forde, Eamonn. Oversharing: how Napster nearly killed the music industry. The Guardian, 2019.

[53] Nav. dj. Fredriksson, Martin, str. 9-11.

besplatno slušanje, ali uz prisustvo oglasa, čije prikazivanje stvara profit platformi. Spotify ima 10 milijuna registriranih korisnika, od kojih se 7.5 milijuna odlučilo za besplatno streamanje. Kako bi držali korak s novim tehnologijama i trendovima, glazbena je industrija stvorila uslugu licenciranja digitalne glazbe, koja se može preuzeti putem interneta i koja se naplaćuje sa svakim preuzimanjem pjesme.[54]

Jedan od razloga zašto ljudi i dalje ilegalno preuzimaju sadržaj je vjerovanje da ih nitko ne može otkriti, odnosno kazniti za učinjeno, ali i visoka cijena originalnog sadržaja u odnosu na krivotvoreni. Smatraju da njihovi postupci ne mogu naštetiti ogromnim filmskim i glazbenim industrijama, koje zarađuju ogromne svote novaca i naplaćuju prevelike troškove konzumiranja sadržaja u slobodno vrijeme. Pojedinci preuzimaju sadržaj jer vjeruju da to svi rade i da je to sasvim uobičajeno ponašanje na internetu. Svatko ima slobodu nevidljivog surfanja internetom i preuzimanja sadržaja, te će ljudi nastaviti kršiti zakon sve dok se ne uspostave zakoni i kazne, koje će se u praksi redovito provoditi. Istodobno je potrebno informirati umreženo društvo o opasnostima interneta, kao što su crni hakeri ili pirati, te kako se optimalno zaštititi od njihovih napada, kako ne bi došlo do trajnih posljedica.

3.4. Autorsko pravo i piratske stranke

Piratstvo je najpopularniji oblik krađe intelektualnog vlasništva u svijetu, te je već 1976. godine zabilježen kao kazneno djelo u Zakonu o autorskim pravima. Prije inovacije osobnih računala i pametnih uređaja, samo je nekolicina pojedinaca imala sposobnost kopiranja originalnih djela, te su konačne produkte zadržavali za osobno korištenje ili užu skupinu ljudi. Zakon o autorskim pravima sprječavao je krivotvorenje onim pojedincima koji su imali određenu opremu za kopiranje sadržaja, kao naprimjer tiskarski stroj, te su oduzimanjem takve opreme zaustavljali i kažnjavali krivotvoritelje.[55] 1982. godine, zbog povećanog kršenja autorskih prava u filmskoj i glazbenoj industriji, izlazi Zakon o izmjenama i dopunama piratstva i krivotvorenja, koji je uključivao širenje sadržaja zaštićenih autorskim pravima Zakonom o zabrani elektroničke građe putem interneta.[56] 2004. godine izlazi IPRED direktiva, koja omogućuje autorima i medijskim

[54] Nav. dj. Dörr, J., str. 384-385.

[55] Usp. Hosch, William L. Piracy. Encyclopædia Britannica, 2009.

[56] Usp. Jackman, M.; Lorde, T. Why buy when we can pirate? the role of intentions and willingness to pay in predicting piracy behavior. // International Journal of Social Economics 41**,** 9(2014). str. 802.

tvrtkama mogućnost nadgledanja internetskih korisnika u svrhu sprječavanja i otkrivanja povrede autorskih prava. U Švedskoj se ta direktiva pojavila 2005. godine, te je doživjela mnoštvo kritika zbog kršenja sigurnosti korisnika na internetu. Godinu dana kasnije švedska policija uspijeva locirati tvrtku The Pirate Bay zajedno s njezinim osnivačima, koji 2009. godine bivaju osuđeni na godinu dana zatvora i novčanu kaznu od 4.5 milijuna dolara.[57] Svjetska organizacija za intelektualno vlasništvo (WIPO) osmislila je nekoliko sporazuma, pomoću kojih promiče zaštitu autorskih prava intelektualnog vlasništva na različitim medijima.[58] HADOPI ili Creation and Internet Law, je zakon protiv piratstva koji je francuska vlada usvojila 2009. godine, u svrhu promicanja širenja i zaštite intelektualnog sadržaja na internetu. Zakon se prvotno provodi slanjem upozorenja kršiteljima zakona, te ukoliko se kršenje zakona ponovno dogodi, slučaj se predaje državnom sudu koji potom određuje kaznu.[59]

Kao odgovor na sve strože zakone o intelektualnom vlasništvu i autorskom pravu, pirati se počinju udruživati u piratske stranke i boriti za slobodu informacija. Piratske se stranke osnivaju s ciljem ostvarivanja jednakosti, digitalnih prava, ukidanjem patenata, slobode informacija, reforme autorskih prava i zaštite privatnosti.[60] Prva takva piratska stranka formirana je 2006. godine u Švedskoj sa značajnim brojem članova, ali nedovoljnim političkim utjecajem.[61] U početku su piratske stranke promicale važnost digitalne razmjene, koja je posebice privlačna umreženom društvu, no ubrzo pokušavaju pojačati utjecaj putem parlamentarnih izbora.[62] 2009. je godine švedska piratska stranka doživjela uspjeh kada su na parlamentarnim izborima ostvarili 7.1% biračkih glasova te time osigurali dva mjesta u Europskom parlamentu.[63] Te je godine uočen izniman rast od 18,000 članova unutar stranke, a jedan od mogućih razloga je slučaj The Pirate Bay, u kojem su pirati kažnjeni zbog narušavanja autorskih prava, pa se sve više pojedinaca odlučuje boriti protiv strogih zakona piratstva. Nakon povećanja članstva 2010. godine je u Belgiji uspostavljena vodeća Međunarodna piratska stranka (PPI), radi podržavanja i promoviranja suradnje i komunikacije između svih piratskih stranaka.[64, 65] Unutar PPI djeluje 39 piratskih stranaka, a jedna od njih je i hrvatska piratska stranka. Uppsala Deklaracija potpisana je na

[57] Nav. dj. Fredriksson, Martin, str. 9-10.
[58] Nav. dj. Jackman, M.; Lorde, T., str. 802.
[59] Nav. dj. Danaher, Brett, str. 5.
[60] Usp. BBC News. Pirate Parties: From digital rights to political power, 2011.
[61] Nav. dj. Fredriksson, Martin, str. 10-11.
[62] Nav. dj. BBC News.
[63] Nav. dj. Fredriksson, Martin, str. 10-11.
[64] Nav. dj. BBC News.
[65] Usp. Pirate Parties International.

konferenciji 2009. godine na kojoj su se sve piratske stranke, koje su dio PPI, okupile i složile o zajedničkim ciljevima za koje se trebaju boriti, ne samo za sebe, već za ukupno informacijsko društvo. Piratske stranke smatraju da autorsko pravo nije u skladu s današnjim digitalnim okruženjem jer sprječava stvaranje, napredovanje i razmjenu informacija. Umreženo društvo zahtjeva dostupnost sadržaju, te se bori protiv navedenih zakona o autorskom pravu i piratstvu, smatrajući da su ti zakoni i odredbe preoštre i da nisu svi oblici piratstva negativni, kao što mediji prikazuju.[66] Uspjeh švedske piratske stranke potaknuo je formiranje sličnih u više od 60 zemalja, koje su ostvarile značajne promjene u društvu i politici, pa je tako i njemačka piratska stranka 2011. godine osvojila 8.9% biračkih glasova. Međunarodni rast interesa javnosti za piratske stranke i zauzimanje za njihove ciljeve otvorenosti i transparentnosti, može se pripisati želji za promjenama u digitalnom okuženju i borbi za slobodnim znanjem, kao jednim od temeljnih ljudskih prava. Prednost koju piratske stranke posjeduju tehnološku spremnost, otvoreni stranački sustav i uspješno motiviranje javnosti na podržavanja njihovog rada putem društvenih mreža, na kojima mogu pratiti sve njihove informacije o reformi autorskog prava i patenata. Usprkos željama medija za širenjem negativne slike pirata javnosti kao kršiteljima zakona, ono često ima obrnuti ishod, te ga javnost ne smatra kao ozbiljnim zločinom. Lawrence Lessig opisuje kulturno čitanje i korištenje kao zajednički čin stalnog izmjenjivanja umjetničkog djela koje treba biti dostupno svima na upotrebu, što ide u korist ciljevima za koje se piratske stranke bore.[67]

U literaturi *Why buy when we can pirate?*, autori Jackman i Lorde navode nekoliko metoda kojima se može smanjiti ili u potpunosti ukloniti piratiziranje sadržaja, a to su: vođenje tužbi protiv piratskih stranica ili P2P mreža, pružanje alternativnih legalnih streaming usluga, blokiranje pristupa piratskim stranicama i informiranje o posljedicama piratstva. Svaka od navedenih metoda su se u praksi isprobale i pokazale pozitivne rezultate, no nisu u potpunosti uspjele otkloniti fizičko i digitalno piratstvo.[68] Nije dovoljno samo navesti mjere i propise kojih se treba držati, ako ih se u praksi neće shvaćati ozbiljno. Svi oblici piratstva, koji narušavaju autorsko pravo, trebaju biti kažnjeni, a zakon i kazne trebaju biti transparentni, odnosno jasno objašnjeni široj javnosti kako bi saznali koje posljedice nastaju kao rezultat njihovog nesmetanog ponašanja na internetu. U provedenom istraživanju Brett Danahera utvrđeno je da su, nakon uvođenja zakona HADOPI, iTunes brojke tjedne prodaje i slušanja glazbe povećane za 90,000 jedinica sadržaja. Pretpostavlja

[66] Usp. Uppsala Declaration.
[67] Nav. dj. Fredriksson, Martin, str. 10-11.
[68] Nav. dj. Jackman, M., str. 802-803.

se da nekolicina pirata odustaje od ilegalnog preuzimanja i počinje koristiti alternativne legalne streaming usluge, kao što su Deezer, YouTube, Netflix, MaaS i Spotify.[69]

4. Zaključak

Kakav bi život bio bez interneta i tehnologije? Kako je tehnologija utjecala na društvo? Jesmo li postali ovisni o brzim informacijama i društvenim mrežama? Navedena su samo neka od pitanja o kojima se svakodnevno raspravlja i problematizira u današnjem društvu. Teško je zamisliti svijet bez računalne tehnologije i interneta, jer je taj izum omogućio međunarodnu povezanost i dostupnost informacijama kao jedne od osnovnih potreba društva. Naravno, da nije bilo hakera ne bi bilo ni interneta. Prve hakere je povezivala ljubav o stvaranju sigurnog okruženja na mreži i razvijanja hakerske, odnosno programerske zajednice u kojoj vrijede određene etičke vrijednosti koje svaki haker treba usvojiti. Pod utjecajem filmske percepcije hakera i crnih hakerskih napada pojavila se stigma u društvu na spomen riječi haker. Uistinu je od velike važnosti preventivno se zaštititi od hakera i potencijalnih napada, pogotovo u digitalnom dobu, ali hakeri se ne bi trebali generalizirati. Svaki korisnik interneta treba pratiti obrazac ponašanja na internetu i čvrsto se držati etičkih vrijednosti dijeljenja i korištenja digitalnog sadržaja. Pirati se također bore za ostvarenje ciljeva dostupnosti svog sadržaja na slobodno korištenje, ali je slika pirata u medijima potpuno drugačija. Piratstvo je procvjetalo izumom interneta, čime su se otvorila vrata mnoštvu zainteresiranih potrošača piratskog sadržaja. Kao društvo koje ima sve na dodir ruke, naviknuti smo na dostupnost traženih sadržaja, neovisno jesu li to izvorna ili piratizirana djela.

[69] Nav. dj. Danaher, Brett, str. 19.

Internet pruža određenu sigurnost i nevidljivost korisnika, odnosno njihovog ponašanja, pa pojedinci često odbacuju etičke vrijednosti kojih se drže u fizičkom okruženju. Jedan od načina kako i hakeri i pirati mogu proaktivno sudjelovati u društvenom životu je udruživanje u političke stranke putem kojih će se boriti za svoje ciljeve legalnim sredstvima, kako bi digitalno okruženje postalo mjesto u kojem svatko može dijeliti i koristiti sadržaj neovisno o autorskim pravima i ostalim zakonskim odredbama vezanih uz intelektualno vlasništvo. Ukoliko želimo uživati u pozitivnim stranama interneta i tehnologije, potrebno je omogućiti virtualno okruženje u kojem će svi korisnici biti ujedinjeni u promoviranju sigurnosti interneta.

5. Literatura

Knjige

1. Himanen, Pekka. Hakerska etika i duh informacijskog doba. Zagreb : Naklada Jesenski i Turk, 2002.
2. Levy, Steven. Hackers : heroes of the computer revolution. Garden City, N.Y. : Anchor Press/Doubleday, 1984.

Dokumentarni filmovi

3. Amer, K.; Noujaim, J. The Great Hack. Netflix, 2019.

Članci

4. Beale, Sara Sun; Berris, Peter. Hacking The Internet of Things: Vulnerabilities, dangers, and legal responses. // Duke Law & Technology Rewiev 16(2018). str. 161-204. URL: https://scholarship.law.duke.edu/dltr/vol16/iss1/6 (2021-07-10).

5. Cox, J.; Collins, A. Sailing in the same ship? differences in factors motivating piracy of music and movie content. // Journal of Behavioral and Experimental Economics 50(2014). str. 70-76. URL: https://doi.org/10.1016/j.socec.2014.02.010 (2021-07-10).
6. Danaher, Brett et. al. The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France. // *ERN: Integration (Topic)* (2014). URL: https://doi.org/10.1111/joie.12056 (2021-07-10).
7. Derakhti, A. et. al. Streaming or misbehavior, investigation on movie streaming or movie piracy. // Dyna 87, 215(2020). URL: https://doi.org/10.15446/dyna.v87n215.84541 (2021-07-10).
8. Dilmperi, A.; King, T.; Dennis, C. Pirates of the web: The curse of illegal downloading. // Journal of Retailing and Consumer Services 18, 2(2011). str. 132-140. URL: https://doi.org/10.1016/j.jretconser.2010.12.004 (2021-07-10).
9. Dörr, J. et. al. Music as a Service as an Alternative to Music Piracy? // *Business & Information Systems Engineering* 5 (2013). str. 383-396. URL: https://doi.org/10.1007/s12599-013-0294-0 (2021-07-10).
10. Drew, J. A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. // Journal of Criminological Research, Policy and Practice 6, 1(2020). str. 17-33. URL: https://doi.org/10.1108/JCRPP-12-2019-0070 (2021-07-10).
11. Fredriksson, Martin. Copyright Culture and Pirate Politics. // Cultural Studies 28, 5-6(2014). str. 1022-1047. URL: https://doi.org/10.1080/09502386.2014.886483 (2021-07-10).
12. Jackman, M.; Lorde, T. Why buy when we can pirate? the role of intentions and willingness to pay in predicting piracy behavior. // International Journal of Social Economics 41, 9(2014). str. 801-819. URL: https://doi.org/10.1108/IJSE-04-2013-0104 (2021-07-10).
13. Jacobs, R. S.; Heuvelman, A.; Tan, M.; Peters, O. Digital movie piracy: A perspective on downloading behavior through social cognitive theory. // Computers in Human Behavior 28, 3(2012). str. 958-967. URL: https://doi.org/10.1016/j.chb.2011.12.017 (2021-07-10).
14. Jaquet-Chiffelle, David-Oliver; Loi, Michele. Ethical and Unethical Hacking, 2019. URL: https://doi.org/10.1007/978-3-030-29053-5_9 (2021-07-10).

15. LaRose, R.; Kim, J. Share, steal, or buy? A social cognitive perspective of music downloading. // Cyberpsychology & Behavior 10, 2(2007). str. 267-277. URL: https://doi.org/10.1089/cpb.2006.9959 (2021-07-10).
16. Radziwill, Nicole et. al. The Ethics of Hacking: Should It Be Taught? URL: https://arxiv.org/abs/1512.02707 (2021-07-10).

Mrežni izvori

17. BBC News. Pirate Parties: From digital rights to political power, 2011. URL: https://www.bbc.com/news/technology-15288907 (2021-07-10).
18. FindLaw. Hacking Laws and Punishments, 2019. URL: https://www.findlaw.com/criminal/criminal-charges/hacking-laws-and-punishments.html (2021-07-10).
19. Forde, Eamonn. Oversharing: How Napster nearly killed the music industry. The Guardian, 2019. URL: https://www.theguardian.com/music/2019/may/31/napster-twenty-years-music-revolution (2021-07-10).
20. Holmes, A. 533 million Facebook users' phone numbers and personal data have been leaked online. Insider, 2021. URL: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 (2021-07-10).
21. Hosch, William L. Piracy. Encyclopædia Britannica, 2009. URL: https://www.britannica.com/topic/piracy-copyright-crime/E-books-and-promotional-piracy (2021-07-10).
22. Mathews, Lee. Nearly A Million Printers At Risk Of Attack, Thousands Hacked To Prove It. Forbes, 2020. URL: https://www.forbes.com/sites/leemathews/2020/08/31/800000-printers-vulnerable-28000-hacked/?sh=248dd6dfd8a9 (2021-07-10).
23. Piracy. Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/english/piracy (2021-07-10).
24. Pirate Parties International. URL: https://pp-international.net/about-ppi/statutes-of-ppi/ (2021-07-10).
25. Ravenscraft, Eric. How Piracy Benefits Companies, Even If They Don't Admit it. Lifehacker, 2014. URL: https://lifehacker.com/how-piracy-benefits-companies-even-if-they-dont-admit-1649353452 (2021-07-10).
26. Royal Museums Greenwich. The Golden Age of Piracy. URL: https://www.rmg.co.uk/stories/topics/golden-age-piracy (2021-07-10).

27. Smart protection. How does online piracy of movies and TV series actually work?, 2019. URL: https://smartprotection.com/en/media/how-does-film-series-online-piracy-work/ (2021-07-10).
28. Stop krivotvorinama. Krivotvorenje i piratstvo. URL: http://www.stop-krivotvorinama-i-piratstvu.hr/print.aspx?id=45 (2021-07-10).
29. Swinhoe, Dan. The 15 biggest data breaches of the 21st century. CSO, 2021. URL: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (2021-07-10).
30. Tidy, Joe. PewDiePie printer hackers strike again. BBC, 2018. URL: https://www.bbc.com/news/technology-46552339 (2021-07-10).
31. Uppsala Declaration. URL: https://wiki.pp-international.net/wiki/index.php?title=Uppsala_Declaration (2021-07-10).
32. Varsani, Jayesh. Fighting against digital piracy in the streaming age. Cartesian, 2019. URL: https://www.cartesian.com/fighting-against-digital-piracy-in-the-streaming-age/ (2021-07-10).