Kaznena djela počinjena uporabom računala, računalnih sustava i programa

Carević, Nevia

PRAVNI FAKULTET U ZAGREBU

KATEDRA ZA KAZNENO PRAVO

NEVIA CAREVIĆ

KAZNENA DJELA POČINJENA UPORABOM RAČUNALA, RAČUNALNIH SUSTAVA I PROGRAMA

DIPLOMSKI RAD

Mentor: prof.dr.sc MAJA MUNIVRANA

ZAGREB, srpanj 2022.

Izjava o izvornosti

Ja, Nevia Carević pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autorica diplomskog rada pod nazivom "Kaznena djela počinjena uporabom računala, računalnih sustava i programa" te da u radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristio/-la drugim izvorima do onih navedenih u radu.

_____

Nevia Carević (0066241062)

ZAHVALA

Veliko hvala mojim roditeljima i sestri na bezuvjetnoj ljubavi, podršci i strpljenju, jer ste uvijek vjerovali u mene i moj uspjeh čak i kad nisam ni sama.

SAŽETAK

Razvojem računala, uz tradicionalna kaznena djela dolazi do razvoja nove vrste kaznenih djela, a to su kaznena djela kibernetičkog kriminala. Za sam pojam računalnog kriminala ni danas ne postoji općeprihvaćena definicija, a najšire se definira prema tome da li je računalo cilj ili sredstvo uporabe. Osnovne karakteristike tih kaznenih djela su raznolikost i prilagodljivost brzom razvoju i primjeni novih tehnologija. Tijela kaznenog pravosuđa najprije su pokušala podvesti ta nova kaznena djela pod postojeća, čime su ugrožena načela zakonitosti i određenosti kaznenih djela, a javljaju se i novi pojmovi računalni podaci i programi koji se ne mogu regulirati jednako kao materijalni fizički objekti. S obzirom na globalni karakter, regulaciji se nije moglo pristupiti na nacionalnoj razini nego samo na međunarodnoj. Tako se počinju donositi brojni akti, rezolucije i preporuke, a najvažnija od njih je Konvencija o kibernetičkom kriminalu, Vijeća Europe usvojena 2001. u Budimpešti. Njen je cilj vođenje zajedničke kaznene politike usmjerene na zaštitu društva od kibernetičkog kriminala. Hrvatski Kazneni zakon je pri reguliranju kaznenih djela poštivao obveze utvrđene Konvencijom i Direktivom 2013/40/EU o napadima na informacijske sustave.

Ključne riječi: Kibernetički kriminal, računalna kaznena djela, Računalni podaci i programi, Kazneni zakon, Konvencija o kibernetičkom kriminalu, Direktiva 2013/40/EU

SUMMARY

With the development of computers, in addition to traditional criminal offenses, a new type of criminal offense is being developed, and these are criminal offenses of cybercrime. For the notion of computer crime, there is no generally accepted definition even today, but is more broadly defined according to whether a computer is target or a means of use. The basic characteristics of these criminal offenses are diversity and adaptability to the rapid development and new applications of technologies. The criminal authorities first tried to bring these new criminal offenses under the existing ones, which endangered the principles of legality and specificity of criminal offenses. New concepts, computer data and programs appeared that could not be regulated in the same way as tangible physical objects. Given the global character, the regulation could not be approached at the national level but only at the international one. Numerous acts, resolutions and recommendations are adopted. The most important is The Council od Europe, Convention on Cybercrime, adopted in 2001. in Budapest. Its goal is to pursue a common penal policy aimed at protecting society from cybercrime. In regulating criminal offenses, the Croatian Criminal code complied with the obligations set out in the Convention and the Directive 2013/40/EU on attacks against information systems.

Keywords: cybercrime, computer crimes, computer data and programs, Criminal code, Convention on Cybercrime, Directive 2013/40/EU

Sadržaj:

1. Uvod……..……1
2. Pojam i osnovna obilježja računalnog kriminala……..……3
2.1. Fenomenologija…….……..4
2.2. Počinitelji…….……5
2.3. Istraživanje…….…….6
2.4. Prevencija…….…...7
3. Kazneno-pravni aspekti računalnog kriminala……..…7
3.1. Pravna reforma i informatička tehnologija……..7
3.2. Razvoj kaznenog zakonodavstva…….,…8
3.3. Problemi pravne regulacije……..…9
3.4. Podaci o materijalnoj šteti za kaznena djela protiv računalnih sustava, programa i podataka……..,……...10
4. Međunarodni aspekti računalnog kriminala……11
4.1. Aktivnosti međunarodnih i regionalnih organizacija…….12
4.2. Konvencija o kibernetičkom kriminalu……..13
5. Pojavni oblici i klasifikacija……....15
5.1. Kaznena djela protiv računalnih sustava, programa i podataka……....16
5.1.1. Neovlašten pristup…….…...16
5.1.2. Ometanje rada računalnog sustava…….…..17
5.1.3. Oštećenje računalnih podataka…….……18
5.1.4. Neovlašteno presretanje računalnih podataka…….……18
5.1.5. Zlouporaba naprava…….……19
5.2. Računalna kaznena djela…….……..19
5.2.1. Računalno krivotvorenje…….……..20
5.2.2. Računalna prijevara……..21
5.3. Kaznena djela u svezi sa sadržajem……...……..23
5.3.1. Dječja pornografija……...23
5.3.2. Osvetnička pornografija……...25
5.3.3. Rasna i druga diskriminacija……....26
5.4. Povreda prava autora računalnog programa…….28
5.5. Cyber terorizam……....30
6. Zaključak……....33
7. Literatura……34

1. UVOD

Računalna revolucija, širenje Interneta i sve veća upotreba računala u komercijalne svrhe dovela je do razvoja nove vrste kriminala, a to je računalni kriminal *(engl. Cybercrime)*. Nema jedinstvenog stajališta u odnosu na definiciju niti u odnosu na nastanak računalnog kriminala. Neki autori smatraju da se treba povezati s razvojem elektroničkog računala sredinom prošlog stoljeća, kada se u medijima počinju pojavljivati prve informacije o zlouporabama, dok su drugi mišljenja kako je do takvih zlouporaba došlo puno ranije, već početkom devetnaestog stoljeća kada se javljaju prva mehanička računala. Naglim probojem telekomunikacijskih usluga u svakodnevni život krajem šezdesetih godina prošlog stoljeća, javljaju se tehnički visokoobrazovani počinitelji telekomunikacijskih prijevara. Nakon što su uspjeli pronaći načine i tehnička rješenja kako zloupotrijebiti telekomunikacijsku tehnologiju, ta su iskustva prenijeli na informatičku tehnologiju. Tada se pojavljuju prvi računalni počinitelji, koji su danas poznati pod nazivom *hakeri*. Razvoj računalnog kriminala treba promatrati kroz prizmu razvoja i ekonomske eksploatacije računala.[1] Prvi su se kompjuteri koristili u znanstvene i vojne svrhe, a tek potom i za poslovanje gospodarskih subjekata. Prve zlouporabe su uglavnom bile ograničene na ovlaštene korisnike koji su se s njima služili kako bi olakšali izvršenje tada već tradicionalnih kaznenih djela, a ponajprije prijevara. Njihovo se delikventno ponašanje manifestiralo ponajprije kroz manipulaciju financijskih podataka u cilju stjecanja nezakonite materijalne koristi, a rjeđe kroz namjerno uništavanja ili oštećivanje tehničke osnovice, kompjuterskih programa i podataka. Razvojem osobnih računala, i padom njihova cijena dolazi do porasta kriminala jer postaju dostupni širem krugu ljudi. Razvojem interneta i unapređenjem telekomunikacija, sve više prerasta tradicionalne granice te poprima šire regionalne, međunarodne pa čak i globalne razmjere. Tada postaje predmet proučavanja pravne znanosti i pravnih stručnjaka. Prije zakonodavnih reformi i kaznenopravne regulacije računalnog kriminala, tijela kaznenog pravosuđa morala su pribjegavati već postojećim zakonskim rješenjima koja su se odnosila najviše na krađu, prijevaru, pronevjeru, poslovne i druge tajne te zaštitu intelektualnog vlasništva. Ne uvažavajući specifičnosti i nematerijalni karakter kračunalnih programa, zaštita se pružala patentnim, a ne autorskim pravom. Dosadašnje kazneno pravo, naviknuto na pružanje zaštite materijalnim fizičkim objektima, nije moglo dati zadovoljavajuće odgovore na pitanju jesu li digitalni podatci vlasništvo. Ozbiljno je dovedeno u pitanje načelo zakonitosti, posebno u pogledu određenosti zakonskih propisa i njihovih opisa, te zabrane analogije tj. stvaranja novih kaznenih djela od strane

[1] Bača Miroslav, Uvod u računalnu sigurnost, Zagreb, Narodne novine, 2004., str.24.

sudaca.[2] Računalni ili kibernetički kriminal još nema opće prihvaćenu definiciju, ali možemo ga općenito definirati kao „ona kaznena djela koja nije moguće počiniti bez posebnog stručnog znanja ili samo ona djela koja se ne bi mogla počiniti bez korištenja računala[3].“ Za razliku od prošlosti kad je pristup računalima bio ograničen samo na ovlaštene korisnike, danas skoro pa i nema kućanstva bez računala. Slijedom tih okolnosti dolazi do toga da se tradicionalna kaznena djela izvršavaju na nove i drugačije načine, te se pojavljuju i nova kaznena djela vezana isključivo uz uporabu računala. Pravo se našlo pred pitanjem hoće li te oblike podvesti pod postojeća kaznena djela ili će ih inkriminirati kao nova kaznena djela. Reformom hrvatskog kaznenog zakonodavstva 1997. godine uvedeno je prvo pravo djelo računalnog kriminaliteta u članku 223. Kaznenog zakona pod nazivom „oštećenje i uporaba tuđih podataka.“ Budući da su navedena pitanja predstavljala goleme probleme, razvijene zemlje potaknule su niz aktivnosti kako bi se pronašla odgovarajuća zakonska rješenja. U nacionalna zakonodavstva unose se nova kaznena djela koja su se odnosila na računalni kriminalitet.[4] Vijeće Europe je već 1997. godine osnovalo Ekspertnu komisiju za kriminalitet u kibernetičkom prostoru čiji je zadatak izrada međunarodnog instrumenta za suzbijanje kriminaliteta u kibernetičkom prostoru. Vijeće Europe objašnjava da pojava razvoja informacijsko-komunikacijskih tehnologija, prije svega interneta, a time i kaznenih djela na internetu, kazneno pravo usmjereno na kompjuterski kriminalitet postaje preusko pa se kaznenopravna zaštita proširila na cijeli kibernetički prostor, te time dovela do potrebe stvaranja navedene ekspertne komisije.[5] Konvencija o kibernetičkom kriminalitetu (u daljnjem tekstu Konvencija) usvojena je na konferenciji Vijeća Europe 2001. u Budimpešti, te i danas predstavlja najvažniji dokument koji uređuje materiju računalnog kriminala. [6] U radu se nalazi osvrt na razvoj računalnog kriminala, kaznenog zakonodavstva te najvažnijih pojavnih oblika na način kako su uređeni Konvencijom te hrvatskim Kaznenim zakonom (u daljnjem tekstu KZ).

[2] Dragičević, Dražen, Kompjutorski kriminalitet i informacijski sustavi, Zagreb, Informatorov biro sustav, 2004., str.110.
[3] Ibid. str. 118.
[4] Bača, Op.cit.(bilj.1), str.33-34.
[5] Kokot, Ivica, Kaznenopravna zaštita računalnih sustava, programa i podataka, Zagrebačka pravna revija, Vol.3, No.3, 2014., str 303-330.
[6] Ibid.

2. POJAM I OSNOVNA OBILJEŽJA

Računalni kriminalitet nije uvijek bio kršenje pozitivnog prava. Tek od 1979. godine Ministarstvo Pravosuđa SAD-a je definiralo računalni kriminal kao bilo koji nelegalni akt za čije je počinjenje upotrijebljeno računalo ili računalna tehnologija.[7]

Unatoč svim nastojanjima da se odredi točan pojam, sadržaj i opseg računalnog kriminaliteta, *ne postoji općeprihvaćena definicija*. Don Parker ga definira kao „opću formu kroz koju se ispoljavaju različiti oblici kriminalne aktivnosti, forma koja će u budućnosti postati dominantna.[8] Neke od postojećih definicija su preuske jer svode računalni kriminalitet samo na ona kaznena djela koja nije moguće počiniti vez posebnog stručnog znanja ili samo ona djela koja se uopće ne bi mogla počiniti bez korištenja računala. Taber smatra da "računalni delikt mora uključivati visoko stručne operacije na računalu u okolnostima gdje do povrede ne bi moglo doći na drugi način." Encyclopedia Britanicca sadrži sličnu definiciju gdje se pod računalnim kaznenim djelima smatra "svako kazneno djelo počinjeno posredstvom posebnog znanja ili stručnog korištenja računalne tehnologije."[9] D. Krapec smatra kako "računalni kriminalitet označava sve slučajeve zloupotrebe elektronskog računala koji su pravno određeni kao kaznena djela" dok Dragičević daje definiciju računalnog kriminaliteta kao "ukupnost kaznenih djela, učinjenih na određenom području kroz određeno vrijeme, kojima se neovlašteno utječe na korištenje, cjelovitost i dostupnost, programske ili podatkovne osnovice računalnog sustava ili tajnost digitalnih podataka."[10] Definirati računalni kriminalitet je vrlo nezahvalno i teško, jer se radi o novom obliku koji još nije pravno definiran, a niti u potpunosti određen spram drugih oblika kriminala. Zakonodavstva ne poznaju pojam računalnog delikta kao posebnog kaznenog djela, stoga se prilikom njegova definiranja koristi široki pristup pri čemu se vodi računa o načinu izvršenja djela, sredstvu i posljedici kriminalnog djela. Računalni kriminalitet za potrebe ovog rada može definirati kao oblik kriminalnog ponašanja kod kojeg korištenje računala i informacijske tehnologije predstavlja način izvršenja kaznenog djela, ili se računalo upotrebljava kao sredstvo ili cilj izvršenja, a čime se ostvaruje neka u kaznenopravnom smislu relevantna posljedica.[11]

---

[7] Cyber Crime Legislation https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/Tafazzoli-cybercrime%20legislations.pdf (29. lipnja 2022.)
[8] Dragičević, Op.cit.(bilj.2), str.110.
[9] Ibid. str. 111.
[10] Bača, Op.cit.(bilj.1), str. 23.
[11] Ibid.

2.1 FENOMENOLOGIJA

Osnovne karakteristike svih pojavnih oblika obilježava velika raznolikost i prilagodljivost brzom razvoju i primjeni nove tehnologije. Prilagodljivost računala i njihova prisutnost u nekim tradicionalnim oblicima kaznenih djela daju tim oblicima sasvim drugačiji izgled dok su neka djela poput pedofilije, doživjela svoju najveću ekspanziju. Zloupotrebe se različito kvalificiraju, pa imamo situacije u kojim je računalno sredstvo zloupotrebe, dok su druge situacije one koje se odnose na djela u kojim je računalo cilj zloupotrebe.[12]

Prema uzoru na OECD, Vijeće Europe je 1989. usvojilo Preporuku br. (89)9. S obzirom da je cilj Vijeća Europe postići jedinstvo među svojim članovima, te prepoznajući važnost brzog i adekvatnog odgovora na novi izazov računalnog kriminala donesena je ova Preporuka radi usklađivanja zakona i prakse, te unapređenja međunarodne pravne suradnje. U kojoj su sadržane smjernice s prijedlozima za nacionalna zakonodavstva kojima se vladama zemalja članica preporučuje da pri izmjeni i dopuni svojih zakonodavstava uzmu u obzir minimalnu listu djela koja treba sankcionirati, a za što je postignuta opća suglasnost zemalja. Uz to trebaju izvijestiti glavnog tajnika Vijeća Europe o razvoju njihova zakonodavstva, sudske prakse, iskustava, te međunarodne suradnje u odnosu na računalni kriminal.[13] Ta lista je sadržavala sljedeća djela:

1. Računalna prijevara
2. Računalno krivotvorenje
3. Oštećenje računalnih podataka ili računalnih programa
4. Računalna sabotažu
5. Neovlašten pristup
6. Neovlašteno prisluškivanje
7. Neovlaštenu reprodukciju zaštićenih računalnih programa
8. Neovlaštenu reprodukciju topografije poluvodičkih proizvoda

Radilo se o minimalnoj listi, te je uz nju prijedlog sadržavao i dopunsku (opcijsku) listu, za koju nije postignuta zajednička suglasnost u pogledu uvođenja i sankcioniranja, već je to prepušteno državama članicama. Najveći nedostatak podjele je njena općenitost, budući da nije obuhvaćala sve objekte kojima bi trebalo pružiti zaštitu. Dok s druge strane

[12] Dragičević, Op.cit.(bilj.2) str. 124.
[13] Recommendation No. R(89)9 of the Committee of ministers to member states on computer-related crime https://rm.coe.int/09000016804f1094 (7. srpnja 2022.)

zanemaruje činjenicu da se informatička tehnologija, a s njome usporedno i računalni kriminalitet razvijaju iznimno brzo i nepredvidljivo.[14]

Također i problem „tamne brojke“ računalnog kriminaliteta jedan je od najvećih problema s kojim se susreću svi koji se bave ovom problematikom, zato što onemogućava uvid u pravo stanje na ovom području. Riječ je o pojmu kojim se u kriminologiji označava „broj realiziranih kažnjivih ponašanja za koja se ne zna zato što nisu otkrivena, a ne zato što im počinitelj nije poznat.“[15] Razlozi koji idu u prilog tome su različiti, a rezultat su specifičnosti informatičke i telekomunikacijske tehnologije, načina na koji se sva ta djela čine, te položaja njihovih počinitelja kao i odnosa žrtava prema takvim zloupotrebama. Vrlo često žrtve ovakvih napada ne prijavljuju takva djela. Ponekad nisu ni svjesne da je do napada došlo ili pak smatraju kako se on više neće ponoviti, a počinjena šteta je neznatna ili je nema. Kad su u pitanju pravne osobe jedan od razloga za neprijavljivanje leži u njihovu poslovanju, koje bi moglo biti u većoj ili manjoj mjeri dovedeno u pitanje gubljenjem povjerenja njihovih poslovnih partnera i komitenata zbog nesigurnosti njihovog informacijskog sustava. To se najviše odnosi na banke i osiguravajuća društva, a razvojem elektroničke trgovine, i na druge koji na taj način naplaćuju svoje proizvode i usluge.[16] Računalni kriminalitet je ponajprije kriminalitet urbanih sredina koje su ujedno najviše ovisne o svakodnevnoj i sveprisutnoj primjeni informatičke tehnologije, te uz to ima i globalni karakter u pogledu rasprostranjenosti njegova činjenja i u pogledu njegovih posljedica. On ne poznaje granice jer ga se može izvršiti iz bilo kojeg dijela svijeta na bilo kojem drugom mjestu gdje se nalazi računalni sustav. Globalan je također i po posljedicama koje može izazvati, a one daleko nadilaze teritorijalne i regionalne granica, pa ponekad i međunarodne.[17] Prema mišljenju stručnjaka OECD-a čak 75 do 80 posto računalnih zloupotreba nije prijavljeno.[18]

2.2 POČINITELJI

Za razliku od većine drugih kažnjivih djela gdje počinitelj ne mora imati neko veće stručno znanje da bi takva djela izvršio, počinitelji računalnih zloupotreba najčešće posjeduju takvo stručno, tehničko znanje koje im omogućava da zaobiđu sigurnosne mehanizme, pri čemu se nerijetko koriste metodama i sredstvima koje sami razvijaju, međusobno razmjenjuju

[14] Dragičević, Op.cit.(bilj.2) str. 125-6.
[15] Horvatić, Željko, Osnove kriminologije, Ministarstvo unutarnjih poslova Republike Hrvatske, Zagreb, 1988., str. 50.
[16] Dragičević, Op.cit.(bilj.2), str. 122.
[17] Bača, Op.cit.(bilj.1), str. 35.
[18] Dragičević, Op.cit.(bilj.2) str. 122.

i stalno unapređuju.[19] Zato se i naziva kriminalitetom obrazovanih ljudi jer je za njegovu realizaciju nužan, ovisno o obliku, određen stupanj znanja, a što je ta stručnost veća, teže ga je otkriti.[20] To znači da se računalna kaznena djela ne uklapaju u tradicionalno određenje, u kaznenopravnu fizionomiju počinitelja kaznenih djela. Pojavljuju se specifični tipovi počinitelja, *hackeri.* Zbog prirode računalnog kriminaliteta, koji ne poznaje zemljopisne i političke granice, s radnjom počinjenja kojoj pogoduje slobodan i nesmetan protok informacija, može se zaključiti da su počinitelji: domaći i strani državljani, uglavnom osobe sa zavidnim informacijskim, telekomunikacijskim i tehničkim znanjem, sposobni usavršavati sredstva i metode za savladavanje sigurnosnih sustava, sa razvijenom međusobnom suradnjom i stalnom stručnom izobrazbom.[21]

2.3. ISTRAŽIVANJE

Istraživanje svih pojavnih oblika računalnog kriminala obuhvaća niz mjera koje omogućuje rješenje svakog pojedinog slučaja. Danas istraživanje ima multidisciplinarni karakter, što znači da su taj vrlo zahtjevan posao uključeni stručnjaci različitih vrsta. Jedna velika razlika u odnosu na ostale vrste istraživanja jest ta što se ovdje dokazi nalazi u elektroničkom, odnosno digitalnom obliku. Istraga može započeti nadzorom računalnog sustava u kojem se dogodilo neko od kaznenih djela, ali i informativnim odnosno obavještajnim razgovorima s osobama koje se nalaze u neposrednom dodiru s napadnutim računalnim sustavom. Digitalni dokazi su izuzetno važni u razrješavanju bilo kojeg kaznenog djela koje se može počiniti uz ponoć moderne računalne tehnologije. Definirani su Zakonom o Kaznenom postupku[22] kao podatak koji je kao dokaz u elektroničkom(digitalnom) obliku pribavljen prema Zakonu. Oni se mogu pronaći u tekstu, fotografiji, audio ili video zapisu, odnosno to su dokazi koji se mogu pronaći u bilo kojem od oblika zapisa koji se mogu pohraniti u računalu. Jedna od velikih prednosti digitalnih dokaza je što su oni praktički neuništivi, a mogu se i kopirati. Čak i ako dođe do uništenja Hard diska na napadnutom računalu, posebnim je tehnologijskim postupkom moguće „vratiti“ na taj način obrisane digitalne podatke.[23]

[19] Dragičević, Op.cit.(bilj.2), str. 23.
[20] Šimundić, Slavko, Računalni kriminalitet, Pravni fakultet Sveučilišta, Split, 2009., str. 34.
[21] Pavlović, Šime, Kompjutorska kaznena djela u Kaznenom zakoniku, Hrvatski ljetopis za kazneno pravo i praksu, Zagreb, vol. 10, broj 2/2003., str. 625-664.
[22] NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19
[23] Šimundić, Op.cit.(bilj.20), str. 45-6.

2.4. PREVENCIJA

Borba protiv računalnog kriminaliteta nije jednostavna prvenstveno jer se odvija virtualnim putem te za sobom ne ostavlja neki materijalni, opipljiv dokaz. Ali računalo jako lako može postati dokazni materijal, čuvanje starih datoteka ili elektroničkih poruka uvelike može pomoći istražiteljima. Čak i ako pojedino računalo nije bilo ono koje je korišteno za samu kriminalnu aktivnost ono i dalje može sadržavati brojne informacije koje bilježe određene aktivnosti, promet te komunikaciju između računala i udaljenog servera. U većini država su davatelji Internet usluga, dužni čuvati log datoteke[24] svojih korisnika, a Direktiva(EU) 2018/1972 Europskog parlamenta i Vijeća od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija propisuje da bi sav promet elektroničke pošte trebalo čuvati minimalno 12 mjeseci. Velika rasprostranjenost i broj takvih djela u Hrvatskoj je potakla na poduzimanje određenih pravnih i institucionalnih mjera. Tako je unutar Ministarstva unutarnjih poslova osnovana Jedinica za računalni kriminalitet, unutar Hrvatske akademske i istraživačke mreže, osnovan je CERT (Computer Emergency Team), a BSA (Business Software Alliance) je osnovala svoju podružnicu i u Hrvatskoj. Svi oni usko surađuju na otkrivanju računalnih delikata te u edukaciji i podizanju svijesti korisnika.[25] No aktivnost na suzbijanju računalnog kriminala ne smije prestati. Neprekidne promjene zahtijevaju stalno preispitivanje postojećeg stanja i prilagodbe u skladu s promjenama koje se događaju u kibernetičkom prostoru. Budući da velik broj takvih djela transnacionalnog karaktera, međunarodna pravna usklađenost, suradnja i pomoć pri otkrivanju i gonjenju počinitelja temeljni je uvjet uspješne borbe protiv računalnog kriminala.[26]

3. KAZNENOPRAVNI ASPEKTI RAČUNALNOG KRIMINALA

3.1 PRAVNA REFORMA I INFORMATIČKA TEHNOLOGIJA

Pravna aktivnost na zaštiti informacijskih sustava, u prvom redu se odnosila na ona područja gdje se informatička tehnologija ponajviše koristila, a posebno na:

- Zaštitu baza podataka s podacima građana (zaštita privatnosti)
- Zaštitu od računalnih zloupotreba na području gospodarstva

[24] LOG je produžetak datoteke za automatski izrađenu datoteku koja sadrži zapis događaja iz određenih softverskih i operativnih sustava. Iako mogu sadržavati niz stvari, datoteke dnevnika često se koriste za prikaz svih događaja povezanih sa sustavom ili programom koji je stvorio.
[25] Dragičević, Op.cit.(bilj.2), str.187
[26] Ibid. str. 192.

- Zaštitu intelektualnog vlasništva (topografije poluvodičkih proizvoda, čipova i kompjutorskih programa)
- Zaštitu drugih prava i interesa čija je povreda u neposrednoj vezi s korištenjem informatičke i komunikacijske tehnologije, kao i promjenama do kojih je došlo uslijed razvoja i širenja interneta[27]

Prve reforme su se odnosile na zaštitu osobnih podataka građana, odnosno baza podataka pohranjenih na resursima informacijskih sustava državnih organa i institucija i tim je započeta zakonodavna aktivnost potaknuta sve većom primjenom informatičke tehnologije. No takva zaštita bila je ograničena jer nije pokrivala sve veći broj zloupotreba, kojima cilj nisu bili takvi podaci, odnosno informacijski sustavi u kojima su oni prikupljeni, obrađeni i pohranjeni. Sve više se počinje širiti računalni kriminalitet na području gospodarstva popraćeno novim oblicima zloupotrebe, od manipuliranja sa podatcima prilikom njihovog unosa u elektronsko računalo, preko neovlaštenog pristupa računalu i korištenja pohranjenih podataka, do njihovog mijenjanja ili brisanja, pa čak i onesposobljavanja ili uništavanja cjelokupnog sustava. Postojeće zakonodavstvo s obzirom na specifičnosti nove informatičke tehnologije, nije moglo adekvatno odgovoriti na sve učestalije zloupotrebe, radi čega se već početkom osamdesetih godina zakonodavna aktivnost proširuje na djela gospodarskog kriminaliteta, izvršena na računalnim sustavima odnosno njihovim resursima ili uz njihovu pomoć. Novi problemi na koje pravo nije moglo dati odgovor bili su vezani uz pitanje zaštite intelektualnog vlasništva u prvom redu računalnih programa i topologije čipova. Aktivnostima na zaštiti računalnih programa prethodila je praksa sudova koji su je pružali primjenom postojećih pravnih propisa. Zbog brzog razvoja informatičke tehnologije došlo je do kašnjenja pravnog normiranja pojedinih novonastalih odnosa, pa tako i na području zaštite računalnih programa.[28]

3.2 RAZVOJ KAZNENOG ZAKONODAVSTVA

Pravne reforme započete sedamdesetih godina zaštitom baza podataka s osobnim podacima građana dovele su u većini razvijenih zemalja do reformi zakonodavstva i donošenja novih zakona, odnosno nadopune postojećih. Razvoj informatičke tehnologije se širio i na druga područja, a posebno na gospodarstvo, te se informacijski sustavi sve više uvode u državni, privatni, javni i gospodarski sektor. Sa svim prednostima informatičke tehnologije, pojavljuje se i mogućnosti njezine zloupotrebe radi ostvarivanja nezakonitih

[27]Dragičević, Op.cit.(bilj.2), str. 101
[28] Ibid.

interesa. Tome je posebno pridonijelo širenje i sve veće uvođenje računalnih mreža osamdesetih godina, kad počinje eskalirati problem neovlaštenog pristupa računalnih sustavima. S tim se postavlja pitanje treba li takve zloupotrebe inkriminirati, odnosno jesu li takva ponašanja kaznena djela i može li postojeće kazneno zakonodavstvo dati odgovor na njih ili potrebno izvršiti njegovu reformu uvođenjem novih kaznenih djela. Činjenica je da nova informatička tehnologija uz sve blagodati koje pruža, omogućila da se tradicionalne kaznenopravne povrede (kao krađa, oštećenje, prijevara, krivotvorenje) izvršavaju u potpunosti na nov i bitno drugačiji način nego prije, dok s druge strane postoje i novi oblici računalnog kriminala kojima se više ne ugrožavaju tradicionalni objekti kaznenopravne zaštite, već i nova netjelesna dobra kao što su računalni programi i računalni podaci.

Promjene su se posebno odrazile na područje kaznenog prava koje zbog supsidijarnosti i fragmentarnosti kaznenopravne zaštite, te strogog načela zakonitosti, može vrlo sporo i u ograničenoj mjeri reagirati na pojave korištenje tehnologije računala u kriminalne svrhe. Razvojem novih oblika kriminala i širenjem pojma zaštićenog dobra s tjelesnih na netjelesne stvari, uvidjelo se da postojeće kazneno zakonodavstvo nije u mogućnosti dati odgovore na nove izazove i potrebe koje je pred njega stavilo informacijsko društvo. Da bi se riješilo postojeće stanje i popunile pravne praznine, umjesto pristupa proširenju opisa postojećih kaznenih djela, koji je bio kontradiktoran s načelom zakonitosti i zabranom analogije *in malam partem* u kaznenom zakonodavstvu„ mnoge zemlje donijele su nove zakone za borbu protiv računalnog kriminala.[29] Kada se razmatra uporaba novih tehnologijskih rješenja u kontekstu pravne regulative, općeniti je dojam da pravna regulativa uvijek kasni za tehnologijskim razvojem.[30]

3.3 PROBLEMI PRAVNE REGULACIJE

U pravilu je jako teško dokazati računalna kaznena djela, a jedan od najvećih razloga je virtualan svijet računala. Uz to se navode i specifičnosti računalnih sustava, kratki rok za moguće dokazivanje (mnogi računalni zapisi se s vremenom brišu) te međunarodne komponente. Čak i njihovo razumijevanje traži odgovarajuća stručna znanja, bez odgovarajućeg poznavanja tehnologije teško je uopće shvatiti bit nekih od opisanih kaznenih djela. Zato je potrebna pomoć vještaka, ali i odgovarajuća suradnja policije, državnog

[29] Dragičević, Op.cit.(bilj.2), str. 148-50.
[30] Šimundić, Op.cit.(bilj.20), str. 37.

odvjetništva i sudstva.[31] Problem pravne regulacije se vidi iz primjera sankcioniranja počinjenih kaznenih djela iz područja elektroničkog poslovanja, jer zakoni koji to reguliraju predviđaju samo novčane kazne i kratko opisuju inkriminacije. U opisima inkriminacija se ne apostrofiraju mogućnosti počinjenja kaznenih djela uz pomoć suvremenih informacijskih tehnologija što znači da se one mogu počiniti uz njihovu pomoć, ali na druge načine. Novčane kazne nisu male i zavise od slučaja do slučaja, odnosno ovise o kaznenom djelu. Najniža predviđena iznosi tisuću kuna, a najviša 100 000 kuna.[32]

3.4 PODACI O MATERIJALNOJ ŠTETI ZA KAZNENA DJELA PROTIV RAČUNALNIH SUSTAVA, PROGRAMA I PODATAKA[33]

Situacija u Hrvatskoj u pogledu materijalne štete za sva kaznena djela iz Glave kaznenih djela protiv računalnih sustava, programa, podataka Kaznenog zakona je u rapidnom porastu. U 2008. godini prema podacima MUP-a zabilježena je šteta u iznosu od 7.350.262,00 kuna, u 2019. u iznosu 4.799.195,00 kuna, u 2020. 40.125.656,00 kuna, a u prošloj godini od čak 77.816.990,00 kuna. Prema preliminarnim podacima MUP-a, u 2021. godini evidentirano je ukupno 1563 kaznenih djela kibernetičkog kriminaliteta. Kako se navodi u MUP-ovoj publikaciji *Covid i kriminalitet u 2020.*[34]*,* u 2020. prijavljeno je 1.188 kaznenih djela kibernetičkog kriminaliteta, što predstavlja pad za 59,5 % u odnosu na 2019. kada je prijavljeno 2.930 takvih djela, međutim, ne radi se o padu kriminaliteta, već je – kako u publikaciji pojašnjava MUP – tijekom 2020. došlo do usklađivanja statističkog prikaza kaznenih djela računalnog kriminaliteta s odredbom Kaznenog zakona o produženom kaznenom djelu. Naime, navedena odredba nalaže da se postupanje počinitelja, iako čini više odvojenih radnji, ne tretira statistički kao više djela, nego kao jedno produženo djelo, jer se radi o ostvarenju istih kaznenih djela. Razriješeno je 65 posto slučajeva, a jedan počinitelj prosječno počini 5,5 djela. No budući da je prošlu god obilježila i Korona kriza, zbog transformacije poslovanja na rad od kuće i online rada došlo je i do rasta računalnog kriminala. Kako bi se omogućio nesmetan rad udaljenoj radnoj snazi, mnoge tvrtke su

[31] Vojković, Goran, Štambuk-Sunjić, Marija, Konvencija o kibernetičkom kriminalu i kazneni zakon Republike Hrvatske, Zbornik radova Pravnog fakulteta u Splitu, svezak 43, br. 1, 2006, str.123-136.
[32] Šimundić, Op.cit.(bilj.20), str. 108.
[33] Covid i kriminalitet u 2020. Komentar pokazatelja sigurnosti u Republici Hrvatskoj https://mup.gov.hr/UserDocsImages/2021/04/Covid%20i%20kriminalitet%20u%202020%20-%20Komentar%20pokazatelja%20sigurnosti%20u%20Republici%20Hrvatskoj.pdf (29.lipnja 2022.)
[34] Covid i kriminalitet u 2020. Komentar pokazatelja sigurnosti u Republici Hrvatskoj, Op.cit. (bilj.33)

opustile sigurnosne mjere kako bi poslovanje mogle nastaviti nesmetano te time dodatno povećale ranjivost na napade.[35]

4. MEĐUNARODNI ASPEKTI RAČUNALNOG KRIMINALA

Brzi tehnološki razvoj sredinom stoljeća nije pratila i odgovarajuća pravna reakcija na moguće zlouporabe, kako na državnom tako ni na regionalnim ni međunarodnom planu. U razvijenim zemljama je već sedamdesetih godina započela aktivnost na izmjenama i dopunama njihovih zakonodavstava. Ubrzo se uvidjelo da zbog globalnog karaktera računalnog kriminala same promjene nacionalnih zakonodavstava nisu dovoljne, već se problemima mora pristupiti zajednički na međunarodnom nivou. Zbog toga nije izostala ni šira, regionalna i međunarodna akcija, o čemu svjedoče i aktivnosti raznih organizacija, poput Ujedinjenih naroda, OECD-a, Vijeća Europe, Europske zajednice te raznih međunarodnih udruženja za kazneno pravo.[36] Aktivnosti je započeta donošenjem brojnih preporuka, rezolucija i smjernica koje su se ponajprije odnosile na zaštitu osobnih podataka, odnosno baza podataka u kojima su pohranjeni, prevenciju gospodarskog kriminaliteta te zaštitu intelektualnog vlasništva i informacijskih sustava. U novije vrijeme i na sprječavanje širenja nezakonitih i štetnih sadržaja, kao posljedice sve većeg korištenja Interneta. Pravni teoretičari su nastojali uspostaviti harmonizaciju postojećih pravnih sustava, odnosno zakonodavstava kao i suradnju između država na istraživanju, otkrivanju, dokazivanju i suzbijanju kompjuterskog kriminaliteta. Njihova djelatnost nije prethodila reformama zakonodavstva, već se najčešće odvijala istodobno s njima, tako da njihove preporuke i smjernice nisu bile toliko efikasne zbog njihovog autoriteta, koliko je odlučujuća bila razmjena mišljenja i suradnja kompetentnih predstavnika zemalja tijekom pripremanja tih postupaka.[37]

Iako još ni danas nije postignuta opća suglasnost oko definiranja pojma računalnog kriminaliteta kao ni pojavnih oblika koje bi trebao obuhvatiti, mora se priznati da je aktivnost međunarodnih organizacija i udruženja uvelike pomogle nacionalnim zakonodavstvima da u svoje nacionalno zakonodavstvo uvedu nove oblike kaznenih djela, te da se postigne bar određeni stupanj harmonizacije. Značajan je i doprinos na razvoju međunarodne suradnje pri otkrivanju i procesuiranju počinitelja računalnog kriminaliteta.[38]

---

[35] Tijekom pandemije značajno porasle štete prouzrokovane kibernetičkim kriminalom https://faktograf.hr/2022/02/23/tijekom-pandemije-znacajno-porasle-stete-prouzrocene-kibernetickim-kriminalom/ (15. svibnja 2022.)

[36] Dragičević, Op.cit.(bilj.2), str.193.

[37] Sieber Ulrich, Computer Crime and Criminal Information Law – New Trend sin the International Risk and Information Society, Computer und Recht, 1995., str. 100.

[38] Dragičević, Op.cit. (bilj.2), str. 194.

4.1 AKTIVNOSTI MEĐUNARODNIH I REGIONALNIH ORGANIZACIJA

Prve opsežnije međunarodne aktivnosti u pravcu usklađivanja i dopune postojećih kaznenih zakonodavstava djelima računalnog kriminala poduzela je *Organizacija za ekonomsku suradnju i razvoj (OECD).* Sastavljena je Komisija koja je trebala razmotriti mogućnosti međunarodne harmonizacije kaznenih zakonodavstava. Ona je provela analizu postojećeg stanja u zemljama članicama kako bi utvrdila s kojim problemima se susreću njihova zakonodavstva. Rezultat toga rada je bio izvještaj pod nazivom *Computer-Related Crime: Analysis of Legal Police* koji je sadržavao prijedloge reformi i dopuna koje bi one trebale poduzeti u cilju sprječavanja i suzbijanja računalnog kriminaliteta. Prijedlog je sadržavao minimalnu listu zloupotreba koje bi zemlje članice trebale uzeti u obzir pri dopunama i reformama svojih kaznenih zakona. Po uzoru na Izvještaj OECD-a uslijedila je nedugo nakon toga aktivnost *Vijeća Europe* na studiji o računalnom kriminalitetu i stanju u zakonodavstvima zemalja članica. Cilj je bio da se postignu i razviju smjernice za pomoć zakonodavcima u određivanju koja bi se ponašanja trebala zabraniti, odnosno sankcionirati kaznenim pravom i kako bi to trebalo postići. [39]

Zajedničko svim preporukama i smjernicama je da se u njima ukazuje na prednosti, ali i opasnosti koje je nova tehnologija donijela, dok je stav kako se u reguliranju novonastalih odnosa kaznenopravne sankcije trebaju primijeniti samo u najozbiljnijim i najtežim slučajevima, dok prednost treba dati drugim pravnim i izvan pravnim mjerama. Mogućnost kaznenopravne regulacije ovog područja spominje se tek u *Europskoj konvenciji o zaštiti pojedinca u pogledu automatske obrade podataka* koju je 1981. usvojilo Vijeće Europe. U toj konvenciji unatoč obvezi da u svoja zakonodavstva unesu određena utvrđena osnovna načela, ostavljena je mogućnost zemljama članicama da odluče kako će osigurati pravnu zaštitu privatnosti i koja će sredstva u tom pogledu primijeniti.[40] Ujedinjeni narodi su na VIII. Kongresu UN-a o sprječavanju zločina i postupanju s delikventima, održanom 1990. u Havani, donijeli Rezoluciju kojom se od svih država članica traži da pojačaju napore u suzbijanju manipulaciju s računalima, među koje ulazi i modernizacija kaznenog prava i postupka.[41]

[39] Dragičević, Op.cit. (bilj.2), str. 198.
[40] Ibid. str. 196.
[41] Pavlović, Op.cit. (bilj.21)

Globalni karakter interneta i kaznenih djela koja se čine na njemu ili uz njegovu pomoć sve više se očituje i glede posljedica koje istodobno mogu pogoditi pojedince, skupine i organizacije u velikom broju različitih zemalja. Ako dodamo tome visoku „tamnu brojku“ računalnog kriminala te velik broj otkrivenih i neprijavljenih djela, stvarne štete i potencijalne opasnosti se mogu samo naslućivati. Problem u tome je što počinitelji ostaju često i nekažnjeni za svoja djela zato što u njihovoj zemlji ili zemlji iz koje djeluju ona nisu inkrimirana. Zbog toga su uslijedile daljne aktivnosti Vijeća Europe koje je osnovalo posebnu komisiju sastavljenu od stručnjaka s različitih područja, sa zadatkom da utvrde stanje i započnu rad na međunarodnom instrumentu za borbu protiv kriminala protiv interneta. Komisija je izradila nacrt Konvencije o kibernetičkom kriminalu. Cilj je bio da utvrdi jedinstvene kriterije i standarde kako bi se u različitim zakonodavstvima na jedinstven način sankcionirala djela počinjena u kibernetičkom prostoru. Nacrtom Konvencije predviđeno je da će stranke prihvatiti takve zakonske i druge mjere koje su nužne da bi se domaćim zakonodavstvom moglo sankcionirati počinitelje četiri skupine računalnih kaznenih djela:

1. Kaznenih djela protiv cjelovitosti, tajnosti i dostupnosti računalnih podataka i sustava (nezakonit pristup, nezakonito presretanje, ometanje sustava, ometanje podataka i zlouporaba podataka)
2. Računalnih kaznenih djela (računalno krivotvorenje i računalna prijevara)
3. Kaznenih djela u svezi sa sadržajem (dječja pornografija)
4. Kaznenih djela povrede autorskog i srodnih prava

Uz sankcioniranje navedenih djela, predviđeni su i kažnjavanje za pokušaj, poticanje, i pomaganje, te kaznena odgovornost pravnih osoba za takva djela, rješavanje nekih kazneno procesnih pitanja koja se posebno odnose na pretragu i pribavljanje dokaza, ovlaštenje redarstvenih vlasti kao i pitanja koja se odnose na mjerodavnost i izručenje počinitelja te obveze uzajamne suradnje i pomoći u otkrivanju i gonjenju počinitelja. [42]

4.2. KONVENCIJA O KIBERNETIČKOM KRIMINALU

Najvažniji dokument u ovom području je Konvencija o kibernetičkom kriminalu, Vijeća Europe koja je usvojena na konferenciji održanoj u Budimpešti 23. studenog 2001. Republika Hrvatska potpisala ju je istog dana, a ratificirala 03. srpnja 2002. U njezinoj Preambuli, između ostalog, stoji da Konvencija ima za cilj vođenje zajedničke kaznene politike usmjerene na zaštitu društva od kibernetičkog kriminala. Konvencija je stvorena u

[42]Dragičević, Op.cit. (bilj.2), str. 154-5.

okolnostima dubokih promjena nastalih digitalizacijom, konvergencijom i neprekidnom globalizacijom računalnih mreža. Nastala je zbog zabrinutosti država članica VE „zbog mogućnosti da računalne mreže i elektroničke informacije budu iskorištene za počinjenje kaznenih djela.“[43] Razlika u odnosu na Preporuku R(89)9 Vijeća Europe nije samo u obvezujućoj snazi ove Konvencije nego u sankcioniranju novih djela koja u vrijeme njezina donošenja nisu postojala ili nisu bila aktualna zbog relativno malih šteta. To se posebno odnosi na kaznena djela sadržaja koji se prezentiraju i distribuiraju putem interneta, kao i različite oblike ometanja rada sustava.[44] Dodatni protokol Konvencije o inkriminiranju djela ksenofobične i rasističke naravi počinjenih pomoću računalnih sustava sastavljen je u Strasbourgu 2003. godine. Republika Hrvatska ga je potpisala iste godine, dok je stupio na snagu 1. studenog 2008. godine.[45] Drugi dodatni protokol usvojen je na sastanku Odbora ministara Vijeća Europe, održanog 17. studenog 2021. te je otvoren za potpisivanje od 12. svibnja 2022. u okviru Međunarodne konferencije o pojačanoj suradnji i otkrivanju elektroničkih dokaza. Drugim dodatnim protokolom predviđeni su postupci za poboljšanje prekograničnog pristupa elektroničkim dokazima i visoka razina zaštitnih mjera pogledu međunarodnih prijenosa osobnih podataka, kojim će se olakšati prijenos podataka između država članica Europske Unije koje su stranke Drugog dodatnog protokola, kao i trećih država koje su stranke. Njim se također pružaju podaci za pojačanu suradnju i otkrivanje elektroničkih dokaza. Republika Hrvatska je prihvatila tekst Drugog dodatnog protokola, te je ovlašten ministar pravosuđa i uprave da ga u ime Republike Hrvatske, potpiše, podložno ratifikaciji.[46]

U prvom poglavlju navedeno je nekoliko osnovnih pojmova vezanih uz konvenciju. U drugom poglavlju prvo su opisana Kaznena djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava. U toj skupini kaznenih djela navode se: „Nezakoniti pristup“ članak 2, „Nezakonito presretanje“ članak 3, „Ometanje podataka“ članak 4, „Ometanje sustava“ članak 5, „Zlouporaba naprava“ članak 6, „Računalno krivotvorenje“ članak 7, „Računalna prijevara“ članak 8, „Kaznena djela vezana uz dječju pornografiju“ članak 9, „Kaznena djela povrede autorskih i srodnih prava“ članak 10. Nakon opisanih navedenih kaznenih djela, navode se odredbe procesnog prava, te zatim odredbe o sudbenosti. U trećem

[43] Pavlović, Op.cit. (bilj.21)
[44] Dragičević, Op.cit.(bilj.2), str. 185.
[45] NN, MU broj 7/08
[46] Odluka o pokretanju postupka za sklapanje Drugog dodatnog protokola uz Konvenciju o kibernetičkom kriminalu o pojačanoj suradnji i otkrivanju elektroničkih dokaza, Vlada republike Hrvatske, 12. svibnja 2022.

poglavlju navode se opće odredbe o međunarodnoj suradnji te posebne odredbe u okviru međunarodne suradnje.[47]

Europski parlament i Vijeće EU su 2013. donijeli Direktivu 2013/40/EU o napadima na informacijske sustave, koja se nadovezuje na Konvenciju. Njezini su ciljevi približiti zakonodavstva članica u području napada na informacijske sustave utvrđivanjem minimalnih pravila o definiranju kaznenih djela i sankcija. U njoj se ističe kako su napadi na informacijske sustave, a posebno napadi povezani s organiziranim kriminalom sve veća prijetnja, te da postoji sve veća zabrinutost zbog potencijalnih terorističkih ili politički motiviranih napada na informacijske sustave koji su dio ključne infrastrukture država članica i Unije.[48] Direktiva je u hrvatsko zakonodavstvo preuzeta Uredbom o preuzimanju Direktive 2013/40/EU o napadima na informacijske sustave i Direktive 2014/62/EU o kaznenopravnoj zaštiti eura i drugih valuta od krivotvorenja. [49] Razlog za donošenje Direktive uz Konvenciju je nedovoljna harmonizacija kaznenog prava na području napada na informacijske sustave. Ona nije u suprotnosti s Konvencijom, nego se na nju nadovezuje.[50]

5. POJAVNI OBLICI I KLASIFIKACIJA

„Reformom kaznenog zakonodavstva 1997. godine uvedeno je prvo pravo kazneno djelo računalnog kriminaliteta u članku 223. kaznenog zakona pod nazivom „oštećenje i uporaba tuđih podataka“ u Glavi XVII. Kaznena djela protiv imovine. Najveća reforma u ovom području dogodila se 2011. godine kad je donesen novi Kazneni zakon, koji je stupio na snagu 1.1.2013. godine. Njime su kaznena djela protiv računalnih sustava, programa i podataka izdvojena iz glave kaznenih djela protiv imovine u posebnu glavu XXV. Kaznena djela protiv računalnih sustava, programa i podataka. Prema obrazloženju uz Kazneni zakon, navedena kaznena djela usklađena su s Konvencijom o kibernetičkom kriminalu, U kazneno zakonodavstvo Republike Hrvatske preuzete su odredbe koje proizlaze iz obveza utvrđenih Konvencijom o kibernetičkom kriminalu i Direktivom EU o napadima na informacijske sustave.“[51]

[47] Šimundić, Op.cit. (bilj.20), str. 124.
[48] Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP
[49] NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21
[50] Kokot, Op.cit. (bilj.5)
[51] Ibid.

Prema Konvenciji kaznena djela grupirana su u četiri skupine: "kaznena djela protiv cjelovitosti, tajnosti i dostupnosti računalnih podataka i sustava", "računalna kaznena djela", "kaznena djela u svezi sa sadržajem" i "kaznena djela povrede autorskog i srodnih prava." Hrvatski zakonodavac je u istu skupinu smjestio "kaznena djela protiv cjelovitosti, tajnosti i dostupnosti podataka" i "računalna kaznena djela". Za razliku od ostalih kaznenih djela iz glave VI. KZ koji čine skupinu kibernetičkog kriminala i koji su određeni prema skupnom užem zaštitnom objektu, računalna kaznena djela određena su prema *modus operandi,* odnosno sredstvu počinjenja. Najvažnija iz skupine računalnih kaznenih djela su računalno krivotvorenja i računalne prijevare.[52] Rad će pratiti sistematizaciju prema Konvenciji, ali ću obraditi i neka "novija" kaznena djela koja su u međuvremenu postala aktualna.

5.1. KAZNENA DJELA PROTIV RAČUNALNIH SUSTAVA, PROGRAMA I PODATAKA

5.1.1 NEOVLAŠTENI PRISTUP (čl. 266. KZ)

Kazneno djelo neovlaštenog pristupa opisano je u članku 266. Kaznenog zakona.Kaznenim djelom neovlaštenog pristupa, kriminalizira se nezakoniti pristup tuđem računalnom sustavu. Njime se štiti se integritet računalnog sustava. Neovlašteni pristup se uspoređuje s povredom nepovredivosti doma. Pravno dobro nije samo povrijeđeno kad osoba bez ovlaštenja zamjeni ili ukrade podatke koji se nalaze u informacijskom sustavu, nego i kad ga samo razgledava. Pojam pristupa nije pravno definiran, ali obuhvaća i pristup internetom, bežičnim komunikacijskim sredstvom, kao i neovlašten pristup računalu koje nije spojeno ni na jednu bežičnu mrežu. Pristup sustavu putem otvorene javne veze nije neovlašten, kao ni pristup po ovlaštenju vlasnika ili korisnika sustava. Ukoliko je žrtva predala lozinku ili pristupni kod počinitelju, to neće značiti da je on neovlašteno pristupio. Zaštitni objekt kod kaznenih djela neovlaštenog pristupa je računalni sustav, bilo cijeli, bilo njegov dio.[53]. Za postojanje kaznenog djela po hrvatskom KZ, traži se samo neovlašteni pristup, te nisu postavljeni nikakvi dodatni uvjeti. Teža kazna propisana je ukoliko je kazneno djelo počinjeno u odnosu na računalni sustav ili računalne podatke tijela državne vlasti, tijela jedinica lokalne ili područne (regionalne) samouprave, javne ustanove ili trgovačkog društva od posebnog javnog interesa. Pokušaj je kažnjiv, a kazneno djela u osnovnom obliku progoni se po prijedlogu oštećene fizičke ili pravne osobe. Za razliku od odredaba Konvencije, članak 266.

[52] Kokot, Op. cit.(bilj.5)
[53] Ibid.

osim računalnog sustava, štiti i računalne podatke, koji se ne moraju nalaziti na računalnom sustavu, nego se mogu nalaziti i na nekom mediju izvan računalnog sustava.[54]

5.1.2 OMETANJE RADA RAČUNALNOG SUSTAVA (čl. 267. KZ)

Kazneno djela propisano je člankom 267. Kaznenog zakona te se sankcionira ometanje rada računalnog sustava, podataka ili programa ili računalne komunikacije koja ovlaštenim korisnicima onemogućuje nesmetano korištenje vlastite tehnologije. Ova odredba zakona usklađena je s člankom 5. Konvencije. Ometanje rada nastaje kao posljedica istovremenog slanja podataka s većeg broja računala, distribuiranim napadima uskraćivanja računalnih usluga.[55] Svrha odredbi je sankcioniranje DoS ili DDos[56] napada. Pojačan interes javnosti za pristup određenim Internet stranicama nije kažnjiv. Botnet napadi uključuju široki raspon napada koji mogu biti izvedeni prema velikom broju računala ili uključuju znatnu štetu poremećajem rada servisa, financijskim gubitkom ili gubitkom podataka. Radnja počinjenja kaznenog djela je eksplicitno određena, inkriminira neovlaštenu uporabu računalnih podataka ili programa radi ometanja rada sustava za obradu podataka. Svrha ova odredbe nije propisivanje kaznenog djela kojim bi bilo sankcionirano bilo kakvo ometanje ili otežavanje rada i korištenja sustava za obradu podataka. Rad sustava za obradu podataka mora biti ometan unosom, prijenosom, oštećenjem, brisanjem, mijenjanjem ili činjenjem neuporabljivim računalnih podataka ili programa s namjerom da se onemogući normalno funkcioniranje sustava za obradu podataka. Ometanje rada računala koje bi bilo obuhvaćeno oštećenjem fizičkih komponenti, infrastrukture, komunikacijske mreže, obuhvaćene su odredbama kojim se sankcionira oštećenje ili uništenje tuđe stvari.[57] Hrvatski Kazneni zakon nije usvojio pravno tehnička rješenja opisana u odredbama Konvencije niti ona opisana u Direktivi EU 2014/40/EU. U njima su taksativno navedeni načini na koje se sustav može omesti, i to isključivo utjecajem na podatke. Odredbe Kaznenog zakona ne sadrže posebne odredbe o načinu počinjenja kaznenog djela, te samim time obuhvaćaju i širi domet. Osim ometanja sustava manipulacijom podataka, obuhvaća i druge vrste manipulacija, uključujući i

[54] Kokor, Op.cit.(bilj.5)
[55] Sankcioniranje cyber nasilja prema novom Kaznenom zakonu https://www.iusinfo.hr/aktualno/u-sredistu/13063 (23. svibnja 2022.)
[56] DoS napadi ili Distibuted Denial of service je napad uskraćivanja usluga ili servisa kojima se korisnicima onemogućava njihovo korištenje. Ako se takav napad izvede s većeg broja računala, onda se zove DDos napad.
[57] Škrtić, Dražen, Kaznena djela računalnog kriminaliteta u novom kaznenom zakonu Republike Hrvatske, Slovenski dnevi varstvoslovja, Zbornik prispevkov, Fakulteta za varnostne vede, Ljubljana, 2012.

oštećenje ili uništenje hardvera ili druge infrastrukture. U tom dijelu dolazi do preklapanja s kaznenim djelom oštećenja tuđe stvari, pa se otvara pitanje pretjerane kriminalizacije.[58]

5.1.3 OŠTEĆENJE RAČUNALNIH PODATAKA (čl. 268. KZ)

Kazneno djelo oštećenja računalnih podataka u kaznenom zakonu opisano je u članku 268 [59]. U naslovu se koristi izraz oštećenje, za razliku od Konvencije i Direktive gdje službeni prijevod glasi ometanje. Kazneno djelo oštećenja računalnih podataka dovodi se u analogiju s kaznenim djelom ometanja rada računalnog sustava, budući da se načini počinjenja u bitnom djelu preklapaju. Oba kaznena djela mogu se počiniti oštećenjem, brisanjem, mijenjanjem ili činjenjem neupotrebljivim računalnih podataka. Ovo kazneno djelo pojavilo se kako bi se popunile pravne praznine i kako bi se računalnim podacima osigurala zaštita od oštećenja i uništenja kakvu uživaju fizički predmeti.[60] Svrha propisivanja navedenog kaznenog djela je zaštita integriteta računalnih podataka ili programa, te je nebitno da li se neovlašteno oštećenje odnosi na sve ili samo dio računalnih podataka ili programa. Cjelovitost podataka je narušena kad se program ne može koristiti za obradu u računalnom sustavu. Za postojanje kaznenog djela potrebno je utvrditi da li je bilo neovlaštenog djelovanja na integritet računalnih podataka bez obzira da li računalni podaci sadrže određene informacije ili su dio računalnog programa. U poredbenom pravu definirane su situacije u kojim je djelovanjem na integritet podataka djelo dovršeno.[61]

5.1.4 NEOVLAŠTENO PRESRETANJE RAČUNALNIH PODATAKA (čl. 269. KZ)

Neovlašteno presretanje komunikacije prema računalnom sustavu sankcionirano je člankom 269. Prema ovome članku kaznit će se tko neovlašteno presretne ili snimi nejavni prijenos računalnih podataka, uključujući i elektromagnetsku emisiju računalnog sustava ili drugome učini dostupnim tako pribavljane podatke (računalna špijunaža). Kriminalizacijom neovlaštenog presretanja zaštita se širi s podataka koji se nalaze u računalnom sustavu i na podatke u prijenosu. Podaci koji se štite su korporativni podaci, osobni podatci, podatci o broju kreditnih kartica, brojevi socijalnog osiguranja, lozinke, pristupne šifre, brojevi bankovnih računa itd. Presretanje se može napraviti i uz pomoć niskih i visokih tehnoloških

[58] Kokot, Op.cit.(bilj.5)
[59]Oštećenje računalnih podataka, članak 268. KZ, (1) Tko neovlašteno u cijelosti ili djelomično ošteti, izmjeni, izbriše, uništi, učini neuporabljivim ili nedostupnim ili prikaže nedostupnim tuđe računalne podatke ili programe, kaznit će kaznom zatvora do 3 godine.
[60] Kokot, Op.cit.(bilj.5)
[61] Škrtić, Op.cit. (bilj.57)

postupaka, od shvaćanja lozinke do ugradnje softvera za špijuniranje. Prema obrazloženju navedenom uz Konvenciju, cilj ove odredbe je izjednačavanje zaštite elektroničkog prijenosa sa zaštitom govorne komunikacije od neovlaštenog prisluškivanja i snimanja. Njegova primjena ograničena je na presretanje prijenosa podataka tehničkim sredstvima, odnosno na pribavljanje podataka za vrijeme prijenosa. Stoga se članak ne može primijeniti na podatke koji nisu u prijenosu, kao pribavljanje podataka koji se nalaze pohranjeni na tvrdom disku. Smatra se da su podaci u prijenosu sve dok nisu došli do krajnjeg odredišta, bilo sustava bilo primatelja, te se smatraju podacima u prijenosu sve dok primatelj ne ostvari pristup tim podacima. Da bi postojalo kazneno djelo potrebno je da prijenos bude nejavan, odnosni povjerljiv.[62]

5.1.5 ZLOUPORABA NAPRAVA (čl. 272. KZ)

U hrvatskom kaznenom zakonu kazneno djelo opisano je u članku 272. te se radi o kaznenom djelu izrade, nabave, prodaje, posjedovanja ili činjenja drugom dostupnim uređaja ili računalnih programa ili računalnih podataka koji su stvoreni ili prilagođeni za počinjenje kaznenih djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava. Kaznenim djelom zlouporaba naprava kriminaliziraju se određene pripremne radnje poduzete radi počinjenja nekih od računalnih kaznenih djela. Pojam „naprava“ prema obrazloženju uz Konvenciju odnosi se kako na hardver, tako i na softverska rješenja namijenjenog počinjenju nekog iz grupe kaznenih djela. Kao primjer softvera navode se virusi ili programi izrađeni ili prilagođeni za ostvarivanje neovlaštenog pristupa računalnom sustavu. Odredbe se odnose i na naprave koje se inače koriste u legalne svrhe kad ih počinitelj koristi s namjerom počinjenja nekog računalnog kaznenog djela.[63] U odnosu na Konvenciju opis je postavljen šire te obuhvaća i naprave koje se koriste za počinjenje kaznenih djela računalne prijevare i računalnog krivotvorenja.

5.2. RAČUNALNA KAZNENA DJELA

Za računalna kaznena djela je specifično da trebaju računalni sustav kao sredstvo počinjenja te da postoje i paralelna tradicionalna kaznena djela kojim se štite iste ili slične vrijednosti u materijalnom obliku od napada klasičnim sredstvima. Direktiva 2013/40/EU o napadima na informacijske sustave, ne propisuje računalna kaznena djela.[64]

[62] Kokot, Op.cit. (bilj.5)
[63] Ibid.
[64] Ibid.

Prijevare putem računala danas su jako popularne, jer se pomoću programskih alata za automatizaciju i skrivanje identiteta, omogućuju masovni napadi na način da žrtve pretrpe nizak financijski gubitak te da im se ne isplati prijavljivati i progoniti takve napadače, dok istodobno masovnost takvih napada osigurava profit napadačima. [65]

5.2.1 RAČUNALNO KRIVOTVORENJE (čl. 270. KZ)

Kazneno djelo računalnog krivotvorenja u hrvatskom kaznenom pravu izrađeno je po uzoru na članak 7. Konvencije, a opisano je u članku 270. kaznenog zakona.[66] U odnosu na ranije kaznene odredbe, ispušten je računalni program kao objekt napada te je dodan nov način počinjenja kroz formulaciju činjenja računalnih podataka nedostupnim.Po načinu izvršenja obuhvaća dvije vrste manipulacija. Prve su kod kojih se računalni sustav koristi za krivotvorenje tuđih postojećih dokumenata u digitalnom obliku, a druge su manipulacije kod kojih se kompjuter koriste da bi se kreirali takvi dokumenti, izvršilo krivotvorenje novca, vrijednosnih papira, isprava ili drugih dokumenata. U pravnom pogledu je relevantno i zakonski regulirano samo ono krivotvorenje koje se odnosi na službene dokumente, odnosno isprave koje se koriste u pravnom prometu.[67] Pravno dobro koje se štiti jest vjerodostojnost isprave u digitalnom obliku. Ono pokriva manipulaciju digitalnim dokumentima, odnosno podacima. Cilj kriminalizacije bilo je izraditi djelo koje će biti jednako krivotvorenju materijalnih dokumenata, a s ciljem popunjavanja pravnih praznina povezanih s tradicionalnim poimanjem krivotvorenja. Računalno krivotvorenje u osnovi stoga obuhvaća izradu ili izmjenu pohranjenih podataka tako da oni dobiju drugu vrijednost u pravnom prometu koji se temelji na vjerodostojnosti podataka. Tradicionalno poimanje krivotvorenja u pravilu podrazumijeva postojanje pisane isprave ili predmeta u materijalnom obliku i vizualnu prezentaciju, dok digitalni podaci zahtijevaju računalnu obradu i prezentaciju. Odredba o krivotvorenju jednako pokriva i javne i privatne isprave koje imaju vrijednost za pravne odnose. Prema Konvenciji, neovlašteni unos točnih ili netočnih podataka, predstavlja situaciju jednaku izradi lažne isprave. Naknadne promjene, brisanja ili činjenje podataka neuporabljivim odgovara krivotvorenju materijalne isprave. Za postojanje kaznenog djela ne

[65] Legislation https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx (27. svibnja 2022.)

[66] Računalno krivotvorenje, članak 270. KZ – Tko neovlašteno izradi, unese, izmjeni i izbriše ili učini neuporabljivim ili nedostupnim računalne podatke koji imaju vrijednost za pravne odnose, u namjeri da se oni uporabe kao vjerodostojni, ili tko ta uporabi ili nabavi radi uporabe kaznit će se kaznom zatvora do tri godine.

[67] Dragičević, Op.cit.(bilj.2), str.137.

traži se samo poduzimanje neke od spomenutih radnja na podacima, nego da te radnje rezultiraju nevjerodostojnim podacima.[68] Krivotvorenje postojećih dokumenata izvodi se ovlaštenim ili neovlaštenim pristupom računalnom sustavu, odnosno mediju na kojem su isprave pohranjene, nakon čega se krivotvorenje izvodi neposrednom izmjenom postojećeg dokumenta, kopiranjem već izmijenjenog dokumenta preko postojećeg ili prenošenjem malicioznog programa koji ima za svrhu da takve izmjene napravi.[69]

Ovo kazneno djelo posebno je postalo aktualno u vrijeme Covid krize, tako su prema priopćenju državnog odvjetništva u Zagrebu ispitani osumnjičenici zbog osnovane sumnje da su izradili neoriginalne EU covid potvrde o cijepljenju, u nakani da se okoriste, te tražili određeni novčani iznos za iste. Sumnja se da je osumnjičenica kao zaposlenica jedne zdravstvene ustanove, u kojoj je ovlaštena unositi podatke o cijepljenju osoba u za to predviđen informacijski sustav, za unaprijed dogovoren novčani iznos, u računalni sustav unijela neistinit podatak da je osoba cijepljena, iako je znala da nije.[70]

5.2.2 RAČUNALNA PRIJEVARA (čl. 271. KZ)

Kazneno djelo računalne prijevare u hrvatskom kaznenom pravu izrađeno je po uzoru na članak 8. Konvencije, a opisano je u članku 271. KZ-a.[71] Konvencija je računalnu prijevaru opisala u članku 8. Kako bi svi mogući oblici manipulacije bili obuhvaćeni, temeljnim oblicima unošenju, brisanju ili činjenju neuporabljivim računalnih podataka dodana je i generalna klauzula koja se odnosi na bilo kakvo ometanje funkcioniranja sustava. Manipulacije koje predstavljaju računalnu prijevaru kriminaliziraju se samo ako je drugome prouzročen gubitak imovine, a počinitelj postupa s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist. Pojam gubitak imovine u širem smislu obuhvaća novac i ekonomski vrijednu materijalnu i nematerijalnu imovinu. Računalna prijevara može se počiniti samo s namjerom

[68] Kokot, Op.cit.(bilj.5)
[69] Dragičević, Op.cit.(bilj.2), str.138.
[70] Općinsko državno odvjetništvo u Zagrebu. Ispitano dvoje osumnjičenika zbog krivotvorenja isprava i zlouporaba položaja i vlasti https://dorh.hr/hr/priopcenja/opcinsko-drzavno-odvjetnistvo-u-zagrebu-ispitano-dvoje-osumnjicenika-zbog-krivotvorenja (2. lipnja 2022.)
[71] Računalna prijevara, članak 271 KZ, Tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, izmijeni, izbriše, ošteti, učini neuporabljivim ili nedostupnim računalne podatke ili ometa rad računalnog sustava i na taj način prouzroči štetu drugome, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

Računalna prijevara obuhvaća različite vrste manipulacija na podacima, najčešće s namjerom da sebi ili drugome pribavi nezakonita imovinska ili druga korist. Ovakve zlouporabe danas predstavljaju najbrojniju vrstu računalnih zlouporaba kako po svom broju, tako i po oblicima kojim se izvršavaju. Postoje dvije vrste računalnih prijevara, a to su izravna i neizravna. Razlika je u objektu, odnosno pokušava li se prevariti računalo ili fizička osoba. Pod *izravnom računalnom prijevarom* smatra se obmanjivanje oštećenika koji je fizička osoba na način da se kao sredstvo obmanjivanja koristi računalni sustav. Radi se o kaznenom djelu prijevare koje je specifično po sredstvu koje se koristi kako bi se oštećenika dovelo u zabludu ili održavalo u zabludi. Jedan od čestih oblika postupanja je prijevara putem elektroničke pošte. Ovo kazneno djelo je u literaturi poznato kao „Nigerijska prijevara" odnosno „Scam 402" nakon što je po prvi put u svijetu normirano nigerijskim kaznenim zakonom. Nigerijska prijevara sastoji se u tome da počinitelj šalje e-mail oštećeniku u kojem mu lažno obećava određenu imovinsku korist., ako mu oštećenik da broj vlastitog bankovnog računa ili plati određenu svotu novca. Nakon što dobije tražene podatke, prekida svaku vezu s oštećenikom. Još jedan vrlo rasprostranjen oblik prijevare je i prijevarna kupnja ili prodaja putem interneta. Ovdje se može pojaviti problem dokazivanja namjere jer se naručena roba transportira poštom iz udaljenih dijelova svijeta pa je uvijek moguće da se izgubi ili ošteti na putu. Druga vrsta je *neizravna računalna prijevara* koja se sastoji u varanju samog računalnog sustava. Računalni sustav je objekt kaznenog djela, radi se o slučajevima u kojim počinitelj utječe na elektroničku obradu podataka kako bi sebi ili drugome pribavio protupravnu imovinsku korist. Zbog takvih manipulacija računalni sustav ne može prepoznati pristupa li mu ovlaštena ili neovlaštena osoba. Ovo kazneno djelo se značajno razlikuje od općeg kaznenog djela prijevare jer se ovdje oštećenik ne dovodi u zabludu niti se održava u zabludi. Dok prijevaru redovito karakterizira određeni doprinos žrtve uvjetovan njenom pohlepom ili naivnošću, ovdje ga nema.[72] Primjer neizravne prijevare je slučaj kada osoba s tuđom bankovnom karticom podigne određeni novčani iznos na bankomatu. Ovo se smatra varanjem računalnog sustava jer računalo smatra da mu pristupa ovlašteni korisnik. Računalo je u zabludi jer on putem četveroznamenkastog koda (PIN-a) provjerava pravo pristupa određenom bankovnom računu.[73] Kazneno djelo računalne prijevare kao posebno kazneno djelo neizostavan je dio suvremenog kaznenog zakonodavstva. Oni zakoni koji ne sadrže takvo djelo ostavljaju značajan kaznenopravni prostor nereguliran, s obzirom na to da se općim kaznenim djelom

[72] Nedić, Tomislav, Vuletić Igor, Računalna prijevara u hrvatskom kaznenom pravu, Zbornik pravnog fakulteta Sveučilišta u Rijeci, Vol.35, No.2, 2014., str .679-692.
[73] Protrka, Nikola, Računalna prijevara – analiza djelotvornosti otkrivačke djelatnosti, Policija i sigurnost, Vol.28., No. 3/20019, 2019., str. 270-283.

prijevare mogu pokriti tek izravne računalne prijevare.Glavna razlika između obične i računalne prijevare je u objektu napada. Kod obične prijevare objekt napada je osoba koja počinitelj dovodi u zabludu ili održava u zabludi, dok kod računalne prijevare objekt napada je računalni sustav ili su to računalni podaci. Ali cilj je isti, stjecanje protupravne imovinske koristi.[74]

5.3 KAZNENA DJELA U SVEZI SA SADRŽAJEM

Kaznena djela povezana sa sadržajem odnose se na objavljivanje ili distribuciju sadržaja koji se smatra nezakonitim, posebice koji se odnosi na dječju pornografiju, nacionalizam, mržnju prema strancima, kao i diskriminaciju i vrijeđanje u vjerskom smislu. Definicija toga što je nezakonit sadržaj ovisi o nacionalnim kulturološkim vrijednostima koje su implementirane u lokalni pravni sustav, te se može bitno razlikovati od države do države. Pravna borba protiv te kategorije kaznenih djela se svodi na nacionalni nivo. Kaznena djela dječje pornografije te rasne i druge diskriminacije propisana su Konvencijom o kibernetičkom kriminalu pa će shodno tome biti obrađena u ovom poglavlju. Za razliku od njih, kazneno djelo "Zloupotreba snimke spolno eksplicitnog sadržaja" nije predviđeno Konvencijom. U ovom poglavlju je obuhvaćeno budući da se radi o objavljivanju ili distribuciji sadržaja učinjenog posredstvo računalne tehnologije. Taj sadržaj nije nezakonit, ali je stečen zloupotrebom povjerenja i povredom privatnosti.

5.3.1 DJEČJA PORNOGRAFIJA (čl. 163. KZ)

Dječja pornografija na internetu spada u kategoriju štetnih kontakta gdje je dijete ciljano izabrano kao žrtva od odrasle osobe radi iskorištavanja djece za pornografiju, slanja zlonamjernih sadržaja, zloupotrebe lozinki i ostalih osobnih podataka, upoznavanja osobe koju su upoznali u virtualnom okruženju. Dječja pornografija u najširem obliku definira je kao zloupotreba djece u pornografske svrhe. Pravne definicije dječje pornografije naglašavaju opsceni ili seksualni sadržaj prikaza kroz opise kaznenih djela, no detalji se razlikuju ovisno o legislativi različitih zemalja. Prema Konvenciji o pravima djeteta dijete je svaka osoba do 18 godine starosti. Konvencija o kibernetičkom kriminalu sadrži izraz „maloljetnik" koja se također odnosi na sve osobe u dobi mlađoj od 18 godina te je istom predviđeno da država stranka može utvrditi i nižu dobnu granicu, ali ne može biti ispod 16 godina starosti. Konvencija u članku 9. definira dječju pornografiju kao pornografski materijal koji vizualno prikazuje maloljetnika koji sudjeluju u seksualno eksplicitnom ponašanju, osobu koja izgleda

[74] I Nedić, Vuletić, Op.cit. (bilj.72)

kao maloljetnik koji sudjeluju u seksualno eksplicitnom ponašanju ili stvarne slike navedenih radnji.[75] Naš KZ u skladu je s međunarodnim dokumentima, Konvencijom o kibernetičkom kriminalu, Konvencijom o zaštite djece od seksualnog iskorištavanja i seksualnog nasilja te Direktivom 2011/93/EU o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije. Prema članku 163. KZ "dječja pornografija je materijal koji vizualno ili na drugi način prikazuje pravo dijete ili realno prikazano nepostojeće dijete ili osobu koja izgleda kao dijete, u pravom ili simuliranom spolno eksplicitnom ponašanju ili koji prikazuje spolne organe djece u spolne svrhe." Člankom 163. inkriminira se iskorištavanje djece za pornografiju[76], dok članak 164. inkriminira iskorištavanje djece za pornografske predstave.[77] Članak 165. inkriminira činjenje pristupačnim djeci mlađoj od 15 godina, spise, slike, audiovizualne sadržaje ili druge predmete pornografskog sadržaja posredstvom računalnog sustava. Taj članak se može primijeniti na slučajeve izravnog nuđenja djeci pornografskog sadržaja, ali problem je kad sama djeca pretražuju Internet u potrazi za takvim sadržajem i ulaze na pornografske web stranice, lažno se predstavljajući punoljetnim.[78]

Prema istraživanju koje su poveli Brkić, Radat i Vejmelka, najčešći oblik počinjenja odnosi se na skidanje sadržaja s Interneta te spremanje na računalo dječje pornografije, zatim presnimavanje i distribucija, te lažno predstavljanje putem *društvene mreže Facebook* i traženje od djeteta da šalje svoje nage fotografije. U vezi s posljednjim navedenim oblikom počinjenja imamo presudu Županijskog suda u Osijeku, Poslovni broj 1 Kzd-4/2021-5 od 01.07.2021. kojim se optuženik proglašava krivim što je početkom mjeseca kolovoza 2019. zajedno sa drugom osobom, *putem društvene mreže „Facebook*" dogovorio dolazak u kuću šestogodišnje polusestre, s namjerom kako bi fotografirao njezine intimne dijelove tijela iako je znao da se radi o nezrelom djetetu izrazito niske životne dobi. Potom je dolaskom kuću u prijepodnevnim satima, iskoristivši trenutak kada u kući nije bilo roditelja, nakon što je druga osoba prethodno djetetu skinula gaćice i stavila povez na oči radi navodne igre "skrivača" te ju posjela na kauč i raširila joj noge, optuženik svojim mobitelom fotografirao spolovilo i

[75] Brkić, Goran, Radat, Katarina, Vejmelka Lucija, Dječja pornografija na internetu-obilježja osuđenih počinitelja, Pravni vjesnik, časopis za pravne i društvene znanosti Pravnog fakulteta Sveučilišta J.J. Strossmayera u Osijeku, Vol.33, No.2, 2017., str. 77-100.

[76] Iskorištavanje djece za pornografiju, članak 163. KZ, Tko dijete namamljuje, vrbuje ili potiče na sudjelovanje u snimanju dječje pornografije ili tko omogući ili organizira njezino snimanje, kaznit će se kaznom zatvora od 1 do 8 godina.

[77] Iskorištavanje djece za pornografske predstave, članak 164 KZ, Tko dijete namamljuje, vrbuje ili potiče na sudjelovanje u pornografskim predstavama, kaznit će se kaznom zatvora od 1 do 7 godina.

[78] Vojković, Štambuk-Sunjić, Op.cit. (bilj.31)

sačinio fotografsku snimku koju je istoga dana proslijedio putem društvene mreže dakle, čime je počinio kazneno djelo spolnog zlostavljanja i iskorištavanja djeteta - teško kazneno djelo spolnog zlostavljanja i iskorištavanja djeteta, opisano u čl. 166. st. 1. u vezi s čl. čl. 163. st. 2. KZ/11, a kažnjivo po čl. 166. st. 1. KZ/11. Optuženik se sam očitovao krivim, te je osuđen na kaznu zatvora u trajanju od tri godine. Uz kaznu su mu izrečene i sigurnosne mjere obveznog psihijatrijskog liječenja, zabrane pristupa internetu u trajanju od dvije godine te zaštitni nadzor po punom izvršenju kazne u trajanju od pet godina.[79] Za razliku od ovog slučaja gdje je optuženik dobio zatvorsku kaznu, prema prethodno navedenom istraživanju najveći broj osuđenika osuđen je na uvjetnu zatvorsku kaznu koja je potom zamijenjena radom za opće dobro. Prema tim podacima, suci su pri odmjeravanju kazne bili prilično blagi prema počiniteljima te su u najvećem broju predmeta, izrekli minimalnu zatvorsku kaznu.[80]

5.3.2 OSVETNIČKA PORNOGRAFIJA (čl. 144.a KZ)

Osvetnička pornografija je naziv za objavljivanje fotografija seksualno eksplicitnih sadržaja bez pristanka osobe koja se na njima nalazi. Objavljivanje intimnog sadržaja bez pristanka osobe, najčešće prethodi dobrovoljnom dijeljenju sadržaja između partnera dok su se nalazili u emocionalnoj vezi, ali isključivo s namjenom da takvi sadržaji budu privatni. Ovim oblikom nasilja najčešće se služe bivši partneri iz osvete zbog prekida veze. No nasilnik ne mora biti nužno i bivši partner, s obzirom da fotografije i snimke mogu nastati i bez znanja žrtve, snimanjem u intimnim situacijama, u vrijeme kad je žrtva bila pod utjecajem alkohola i droga, hakiranjem uređaja žrtve iz koje se mogu preuzeti foto i video materijali koji nisu bili namijenjeni za slanje.[81] Zakonom o izmjenama i dopunama Kaznenog zakona, koji je stupio na snagu u srpnju 2021. u hrvatsko zakonodavstvo uvedeno je kazneno djelo Zlouporaba snimke spolno eksplicitnog sadržaja. Definirano u glavi XIV. Kaznena djela protiv privatnosti, člankom 144.a. „tko zlouporabi odnos povjerenja i bez pristanka snimane osobe učini dostupnim trećoj osobi snimku spolno eksplicitnog sadržaja koja je snimljena uz pristanak te osobe za osobnu upotrebu i na taj način povrijedi njenu privatnost, kaznit će se kaznom zatvora do 1 godine. “ Djelo je propisano kao materijalno kazneno djelo kod kojeg treba utvrditi nastup posljedice koja se sastoji u povredi privatnosti. Ako takve posljedice nema, a počinitelj postupa s namjerom koja mora obuhvatiti činjenicu zlorabe odnosa povjerenja i pristanka snimane osobe, tada bi se radilo o pokušaju koji nije kažnjiv. Zaštita

[79] ŽS u Osijeku, Kzd 4/2021-5. od 1.7.2021. https://www.iusinfo.hr/sudska-praksa/ZSRH2021OsKzdB4A5 (29. svibnja 2022.)
[80] Brkić, Radat, Vejmelka, Op.cit. (bilj.75)
[81] Osvetnička pornografija https://babe.hr/osvetnicka-pornografija-2/ (29. svibnja 2022.)

povjerenja vidi se i u tome da se i kumulativno traži nepostojanje pristanka snimljenje osobe da učini dostupnim trećoj osobi snimku[82] Ako bi snimka postala dostupna većem broju ljudi, primjerice da je objavljena na Internetu, propisana kazna je tri godine zatvora.

Stavkom 2, članka 144.a. propisano je da će se kazniti tko uporabom računalnog sustava izradi novu ili preinači postojeću snimku spolno eksplicitnog sadržaja i tu snimku upotrijebio kao pravu te time povrijedio privatnost osobe na toj snimci. Radi se o „*deep faku*" odnosno sintetičkom medijskom obliku u kojem je osoba ili već otprije postojeća slika zamijenjena s tolikom točnošću da je ljudskom oku nemoguće vidjeti razliku. *Deep fakes* upotrebljava tehnike strojnog učenja i umjetne inteligencije za manipulaciju ili generiranje vizualnog i auditivnog sadržaja s visokim potencijalnom zavaravanja.[83]

„Uvođenjem tog kaznenog djela u hrvatski KZ, Republika Hrvatska pridružila se onim zemljama koje posjeduju posebno kazneno djelo koje regulira tu materiju i ne podvode ga pod druga, već postojeća kaznena djela dovoljno široko propisana da obuhvate i neke segmente „osvetničke pornografije." Neka od posebno reguliranih kaznenih djela u komparativnim zakonodavstvima ne traže da postoji odnos povjerenja. U Nizozemskoj se osvetnička pornografija goni kao kleveta, odnosno teško sramoćenja."[84]

5.3.3 RASNA I DRUGA DISKRIMINACIJA

Internet kao jednostavan medij za publiciranje raznih materijala, počeo se zlorabiti od strane pojedinaca i organizacija koje putem Interneta publiciraju društveno neprihvatljive stavove. Rasističke poruke na internetu, zločini iz mržnje i rasna diskriminacija zabrinjavajući su trendovi u svijetu, pa tako i u Europi. Takvo ponašanje je protuzakonito i potpuno suprotno vrijednostima na kojima je stvorena Europska Unija - vrijednostima jednakosti, ljudskih prava, slobode i dostojanstva. Predsjednica Europske komisije, Ursula von der Leyer, upozorila je da "Rasizam uvijek ne dospije na naslovnice, ali je tu - na našim ulicama, radnim mjestima, čak i u institucijama. On život čini borbom, izaziva očaj i frustraciju, a mlade ljude može obilježiti za cijeli život.[85]

---

[82] Nove izmjene kaznenog zakonodavstva https://www.iusinfo.hr/aktualno/u-sredistu/46843 (29. svibnja 2022.)
[83] Što je to „deep fake" https://znatko.com/7321/sto-je-to-deep-fake (29. svibnja 2022.)
[84] Roksandić, Sunčana, Šesta novela kaznenog zakona – uvođenje virtualnih valuta i „osvetničke pornografije" te dodatna zaštita odnosa povjerenja i ranjivih osoba, Hrvatski ljetopis za kaznene znanosti i praksu, vol 28 No.2, 2021, str. 437-472.
[85] Borba protiv rasizma traži jačanje i bolju implementaciju zakona https://www.ombudsman.hr/hr/borba-protiv-rasizma-trazi-jacanje-i-bolju-implementaciju-zakona/ (02. srpnja 2022.)

Okvirnom odlukom o suzbijanju rasizma i ksenofobije kaznenopravnim sredstvima[86], EU od država članica zahtijeva se da kriminaliziraju javno poticanje na nasilje ili mržnju na temelju boje kože, vjere, podrijetla te nacionalnog, rasnog ili etničkog podrijetla, uključujući djela koja su počinjena na internetu. Komisija je 2016. donijela kodeks postupanja za suzbijanje nezakonitog govora mržnje na internetu, uz dobrovoljnu obvezu platformi informacijske tehnologije da preispitaju i, prema potrebi, uklone sadržaje nezakonitoga govora mržnje. Društvene mreže koje su se pridružile tom kodeksu su Facebook, Youtube, Microsoft, Twitter, Snapchat i Tick Tock. Navede platforme će u roku od 24 sata procijeniti obavijesti korisnika, te ukloniti one poruke koje procjene nezakonitim. Europska komisija usvojila je taj dokument "radi sprječavanja i suzbijanja širenja nezakonitog govora mržnje na internetu."[87] Komisija će nastaviti surađivati s IT poduzećima i proširiti taj rad na druge platforme društvenih medija, uključujući one kojima se uglavnom koriste djeca i adolescenti, te će nastaviti promicati praktične korake za suzbijanje govora mržnje na internetu i promicanje prihvaćanja raznolikosti. Sljedeći korak bit će Akt o digitalnim uslugama, kojim bi se trebale povećati i uskladiti odgovornosti internetskih platformi i pružatelja informacijskih usluga te ojačati nadzor politika koje se odnose na sadržaj u EU-u. Sve je to Akcijskog plana EU za antirasizam za razdoblje od 2020.-2025.[88]

Ovo kazneno djelo, propisano je Dodatnim protokolom[89] uz Konvenciju. Svrha mu je omogućiti usklađivanje materijalnog kaznenog prava država stranaka u borbi protiv rasizma i ksenofobije, suzbijanje njihove promidžbe zlouporabom računalnih sustava, te omogućiti međunarodnu suradnju na ovom području. Prema članku 3. „svaka stranka će usvojiti zakonodavne i druge potrebne mjere kako bi se u skladu, s njezinim domaćim pravom, utvrdilo kao kazneno djelo, ako je počinjeno namjerno i neovlašteno, sljedeće ponašanje: distribuiranje ili omogućavanje dostupnim javnosti na neki drugi način, rasnog i ksenofobnog materijala[90], pomoću računalnog sustava."

---

[86] Okvirna odluka Vijeća 2008/913/PUP od 28. studenoga 2008. o suzbijanju određenih oblika i načina izražavanja rasizma i ksenofobije kaznenopravnim sredstvima

[87] Code of conduct on countering illegal hate speech online, file:///C:/Users/Swift3/Downloads/code_of_conduct_on_countering_illegal_hate_speech_online_en_C08AC7D9-984D-679D-CAEF129AD536E128_42985%20(2).pdf (02. srpnja .2022.)

[88] Komunikacija komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i odboru regija Unija ravnopravnosti: Akcijski plan EU-a za antirasizam za razdoblje od 2020.-2025., 18.9.2020.

[89] Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava, Narodne novine 4/2008.

[90] U svrhu Protokola, rasni i ksenofobni materijal označava svaki pisani materijal, svaku sliku ili bilo kakav drugi prikaz ideja ili teorija koje zagovaraju, potiču ili promiču mržnju, diskriminaciju ili nasilje prema pojedincu ili

U Hrvatskoj Kazneno djelo "rasne i druge diskriminacije" prvotno je bilo regulirano KZ iz 1997. Danas bi se rasna i druga diskriminacija počinjena putem interneta mogla okarakterizirati kao govor mržnje. Tako da bi odredbe koje propisuju ovo kazneno djelo trebalo potražiti u KZ u članku 325. "javno poticanje na nasilje i mržnju".[91] Govorom mržnje općenito smatraju se svi oblici usmenog ili pisanog javnog izražavanja koji šire, potiču, opravdavaju ili pozivaju na mržnju prema određenoj skupini ili njenim pripadnicima, a u cilju stvaranja netrpeljivosti, diskriminacije, razdora ili poticanja na nasilje. Kao primjer iz sudske prakse imamo presudu Općinskog suda u Novom Zagrebu, br. K-397/20-9 od 27. siječnja 2021. Putem svog profila na društvenoj mreži "facebook" optuženik je otišao na stranicu Z.P. i ostavio javni komentar vezan uz raniji događaj koji se odnosio na nasilje prema osobama homoseksualne orijentacije od strane drugih osoba. U nakani iskazivanja netrpeljivosti objavio je kako mu je žao što posljedice napada nisu bile veće i što nisu "fasovali" svi od reda. Utvrđeno je da je putem računalnog sustava i mreže javno poticao na nasilje i mržnju prema skupini ljudi zbog njihovog spolnog opredjeljenja te je osuđen na kaznu zatvora u trajanju 6 mjeseci uz uvjetnu osudu kojom se određuje da se kazna zatvora neće izvršiti ukoliko osuđenik u vremenu provjeravanja u trajanju od 1 godine ne počini novo kazneno djelo. Olakotne okolnosti su bile što se ispričao žrtvi zbog objavljenog komentara te izrazio kajanje zbog objave.[92]

5.4 POVREDA PRAVA AUTORA RAČUNALNOG PROGRAMA (čl. 285. KZ)

Ova grupa kaznenih djela povezana je s piratizacijom softvera i audiovizualnih djela na način da se kaznena djela iz tog područja mogu izvršiti isključivo uz pomoć računala. Neovlašteno korištenje i reproduciranje zaštićenih računalnih programa, softversko piratstvo, jedan je od najrasprostranjenijih oblika zloupotrebe na području informacijske tehnologije. Digitalni oblik u kojem se nalaze i mediji na kojima su pohranjeni, omogućava njihovo jeftino, jednostavno i brzo reproduciranje i razmjenjivanje što je doprinijelo gospodarskoj rasprostranjenosti ovog djela. Budući da se softversko piratstvo nije moglo podvesti pod

skupini pojedinaca, a temelje se na rasi, boji kože, podrijetlu ili nacionalnom ili etničkom podrijetlu te vjeri ako se ona koristi kao povod za bilo koje od spomenutog.

[91] Munivrana, Vajda, Maja, Marton, Šurina, Andrea, Gdje prestaju granice slobode izražavanja na internetu, a počinje govor mržnje? Analiza hrvatskog zakonodavstva i prakse u svjetlu europskih pravnih standarda, Hrvatski ljetopis za kaznene znanosti i praksu, Zagreb, vol. 23, broj 2/2016, str. 435-467.

[92] OS u Novom Zagrebu, br. K-397/20-9 od 27. siječnja 2021.
https://www.iusinfo.hr/document?sopi=DDHR20200202N4280 (2. srpnja .2022.)

inkriminaciju krađe[93], pravna zaštita se mogla pružiti jedino nekim od prava intelektualnog vlasništva, autorskim pravom ili pravom industrijskog vlasništva. Uvidjelo se da samoj prirodi računalnih programa najviše odgovara autorskopravna zaštita. S daljnjim razvojem u sve većem broju zemalja usvojeno je načelo da se pravna zaštita softvera ostvaruje autorskim pravom, odnosno copyrightom. Na međunarodnom planu, zaštita autorskog prava regulirana je još 1986. godine Bernskom konvencijom za zaštitu književnih i umjetničkih djela. U njoj se nije tražilo ispunjavanje bilo kakvih formalnosti za priznavanje autorskog prava, te je zbog toga veliki broj država nije prihvatio. Da bi se to ispravilo donesena je Svjetska(univerzalna) konvencija o autorskom pravu, koja propisuje minimum formalnih uvjeta koje neko djelo mora zadovoljiti da bi se zaštitila prava autora. Hrvatska je također potpisnica konvencije. Nakon što je prihvaćena autorskopravna zaštita računalnih programa, uslijedile su reforme u zakonodavstvu koje su pratile i preporuke nadnacionalnih organizacija kojima se zemljama članicama savjetuje da pravnu zaštitu softveru pruže autorskim pravom.[94]

Sam pojam računalnog programa u pravilu se ne definira propisom, kako u međunarodnim ugovorima, tako ni u Direktivi o računalnim programima, pa ni u nacionalnim zakonima, uključujući hrvatski Zakon o autorskim i srodnim pravima.[95] (u daljnjem tekstu ZAPSP) Razlog tome je činjenica da bilo kakva definicija računalnog programa razvojem informatičkih tehnologija bi mogla zastarjeti.[96] U europskom zakonodavstvu softver i računalni program su istoznačnice, te ga definiramo kao skup uputa koje su namijenjene čipovima i cjelokupnom računalu kako bi se normalno odradio određeni proces. Zaštitu prava računalnih programa uvrštavamo u autorsko, a dijelom i u intelektualno pravo. Računalni programi u ZAPSP-u su proglašeni autorskim djelom, te u skladu sa zakonom i praksom postaju zaštićeni kao „pisana djela svake vrste.“[97] Računalni programi se ne mogu zaštiti patentom budući da se u kontekstu patentne zaštite smatra da ne predstavljaju izum. Autorskopravna zaštita predviđena je i za baze podataka, ali zakonska zaštita koja je predviđena za baze podataka se ne odnosi na računalne programe koji su korišteni za izradu ili rad baze podataka.[98] Kupnjom softvera se ne postaje njegov vlasnik, nego se stječe pravo

[93] Računalni programi kao nematerijalni, ne mogu se podvesti pod pojam „stvari“ bez obzira na medij na kojem se pohranjeni.
[94] Dragičević, Op.cit.(bilj.2), str.107-8.
[95] NN 111/21
[96] Kunda Ivana, Raspolaganje autorskim pravom na računalnom programu – materijalnopravni i kolizijskopravni aspekti, Zbornik Pravnog fakulteta Rijeka (1991), v.31, br.1, 2010., str. 85-132.
[97] Manuilenko, Olena, Vukmir, Mladen, Računalni programi kao objekt zaštite prema Autorskom pravu i srodnim pravima, Zbornik Hrvatskog društva za autorsko pravo, Volumen 5, 2004., str. 160.
[98] Zlatović, Dragan, Pravo intelektualnog vlasništva u suvremenom digitalnom okruženju, Zagreb, 2009., str. 46.

njegove uporabe s obvezom poštivanja određenih ograničenja nametnutih od strane njegova vlasnika, a to je najčešće proizvođač. Detaljna pravila o njegovoj uporabi objašnjena su u popratnoj dokumentaciji i njih se kupac mora pridržavati. Ukoliko se postupa protivno tome dolazi do povrede dakle postupa se protupravno što dovodi do prekršajne i kaznene odgovornosti. Danas postoji pet vrsta softverskog piratstva: piratstvo od strane krajnjih korisnika, prekomjerna uporaba klijent servera, Internet piratizacija, krivotvorenje softvera te piratizacija audiovizualnih djela.[99] Zakon o autorskom pravu uređuje prekršajna prava autora, te građanskopravna, a KZ sadrži odredbe o kaznenopravnoj odgovornosti. Kaznena djela protiv autorskog i srodnih prava uređena su u glavi dvadesetsedmoj „Kaznena djela protiv intelektualnog vlasništva“ kojim je propisan širok spektar kaznenih djela neovlaštenog korištenja autorskih i srodnih prava. Tako je člankom 285. definirana nedozvoljena upotreba autorskog djela ili izvedbe umjetnika izvođača „Tko protivno propisima kojima se uređuje autorsko i srodna prava reproducira, preradi, distribuira, skladišti ili poduzima druge radnje radi distribucije ili priopći javnosti na bilo koji drugi način tuđe autorsko djelo ili dopusti da se to učini i na taj način pribavi imovinsku korist ili prouzroči štetu, kaznit će se kaznom zatvora do 3 godine.“ Postavlja se pitanje postojanja kaznene odgovornost u slučaju kršenja navedenih normi iz KZ, dok ujedno postoji i građanskopravna odgovornost, iz čega se može zaključiti da ne postoji kaznenopravna odgovornost dok su subjekti u ugovornom odnosu i dok se njihovi sporovi mogu rješavati u građanskoj parnici.[100]

5.5 CYBER TERORIZAM (čl.97. KZ)

Prema definiciji Instituta za mir Sjedinjenih Američkih država, cyber terorizam je „konvergencija internetskog prostora i terorizma, te se odnosi na nezakonite napade i prijetnje napadima na računala, mreže i njima pohranjene podatke zbog zastrašivanja vlade ili njezinog naroda, a u svrhu postizanja političkih ili ideoloških ciljeva.“ Teroristi se internetom ponajprije služe u svrhu širenja terorističkih ideologija i poticanja na počinjenje terorističkog akta te kao platformom za obučavanje i novačenje terorista. Internetom se služe u pripremi i u tijeku terorističkih napada kada im on služi kao komunikacijska infrastruktura.[101] Kao primjer imamo slučaj iz 1997. kad je teroristička skupina *Internet Black Tigers*, nasilne nacionalističke skupine iz Šri Lanke, posvećene stvaranju nezavisne države etničkih Tamila, napala e-mail sustave nekoliko veleposlanstva Šri Lanke po svijetu. Budući da su slali oko

[99] Bača, Op.cit.(bilj.1), str. 53-54.
[100] Pravna zaštita autorskog prava https://www.iusinfo.hr/aktualno/u-sredistu/19603 (30. svibnja 2022.)
[101] Antoliš, Krunoslav, Internetska forenzika i cyber terorizam, Policija i sigurnost, Vol.19, No.1, 2010., str. 121-128.

osamsto e-mailova na dan, uspjeli su onesposobiti mreže veleposlanstva na oko dva tjedna. Skupina je izjavila kako ima za cilj suprotstaviti se promidžbi vlade Šri Lanke. Mnogi stručnjaci ovaj slučaj smatraju značajnim za razvoj cyber terorizma, a obavještajne zajednice ga smatraju prvim napadom na mreže jedne države.[102]

U ovom području postoji problem zakonske regulative koja je nedorečena u sadržaju te međunarodno gledano neprihvatljiva. Konvencija o kibernetičkom kriminalu i Konvencija Vijeća Europe o sprječavanju terorizma daju najobuhvatniji prostor za učinkovitu borbu protiv terorističke zlouporabe interneta. Po pitanju nacionalne sigurnosti, zemlje se moraju samostalno nositi s problemima ugroza koje dolaze s interneta jer primjerice politika NATO saveza je prilično eksplicitna i kaže kako je briga o informacijskoj sigurnosti nacionalno pitanje, a ne pitanje saveza. Tako da u slučaju da dođe do cyber napada, ne postoji mogućnost aktiviranja članaka ugovora NATO saveza, po načelu ako je napadnuta jedna članica, da su ostale dužne pružati pomoć.[103] Na razini EU donesena je Uredba 2021/784 o borbi protiv širenja terorističkog sadržaja na internetu. Uredbom se postavljaju pravila na razini cijele EU za borbu protiv zlouporabe usluga *hostinga* za javno širenje terorističkog sadržaja na internetu. U njoj je navedeno da „prisutnost terorističkog sadržaja na internetu dokazano potiče radikalizaciju pojedinaca, što može rezultirati terorističkim djelima, te stoga imati ozbiljne negativne posljedice za korisnike, građane i društvo u cjelini, kao i na pružatelje internetskih usluga na čijim se poslužiteljima nalazi takav sadržaj jer se time narušava povjerenje njihovih korisnika i nanosi šteta njihovim poslovnim modelima.“ Njom se postavljaju obveze koje će poštovati davatelji usluga kako bi se uhvatili u koštac s javnim širenjem terorističkog sadržaja putem svojih usluga i osigurali, prema potrebi da se takav sadržaj ukloni ili da mu se onemogući pristup.[104] Hrvatski zakonski okvir koji osigurava zaštitu od terorizma i ugroza informacijskog sustava, uz Konvenciju obuhvaća Zakon o informacijskoj sigurnosti[105] i Kazneni zakon. U članku 97. Kaznenog zakona definiran je terorizam, a ostalim člancima definirana su kaznena djela koja se izravno vežu uz terorizam, financiranje terorizma u članku 98, javno poticanje na terorizam u članku 99. te novačenje za terorizam u članku 100, obuka za terorizam u članku 101, te člankom 102. kojim se inkriminira onaj tko vodi ili organizira zločinačko udruženje kojem je cilj počinjenje prethodno navedenih kaznenih djela. Izmjenama i dopunama KZ 2021. proširenо je biće

[102] Cyberterrorisam after Stuxnet https://www.jstor.org/stable/resrep11324?seq=1 (2.lipnja 2022.)
[103] Antoliš, Op.cit.(bilj.101)
[104] Uredba 2021/784 Europskog parlamenta i Vijeća od 29. travnja 2021. o borbi protiv širenja terorističkog sadržaja na internetu, Službeni list Europske Unije, 29.4.2021.
[105] NN 79/07

kaznenog djela terorizma kako bi se obuhvatila ponašanja inkriminirana Direktivom EU 2017/541 o suzbijanju terorizma. Tako je kaznenim djelom terorizma obuhvaćeno i „ometanje rada računalnog sustava koje nije počinjeno protiv računalnog sustava kritične infrastrukture, a koje uzrokuje znatnu štetu ili kojim je pogođen znatan broj računalnih sustava uporabom naprava namijenjenih ili prilagođenih u tu svrhu te oštećenje računalnih podataka kada je počinjeno u odnosu na računalni sustav kritične infrastrukture.“[106] Uz tako manjkav zakonodavni okvir te rapidno širenje, cyber terorizam postaje jedan od većih problema današnjice. Budući da teroristi pored klasičnih oružja, na raspolaganju imaju oružja kao što su masovni mediji i tehnologija, oni element straha i panika mogu najbolje i najbrže plasirati kroz masovne medije uz primjenu razvijenih tehnoloških sredstava. Prema tome opasnost od online terorizma postala je naša stvarnost.[107]

6. ZAKLJUČAK

U zadnjih dvadeset godina, Internet je uvelike promijenio naš život, kulturu i društvo. Uz sve nove beneficije i mogućnosti koje nam je pruža, jednako je u naš život unio i novu vrstu kriminala, kibernetički kriminal. Brojnim oblicima zloupotrebe izložen je svatko od nas bio pojedinac, skupina, udruženje ili država. Radi se o rapidno rastućoj vrsti kriminala koja će u budućnosti nastaviti ispoljavati nove oblike kažnjivog ponašanja. Budući da nije moguće ostvariti apsolutnu sigurnost računalnih i drugih informacijskih sustava, bez obzira na poduzete fizičke, tehničke i druge mjere, nužno je uz postojeće mjere, metode, sredstva zaštite, osigurati efikasnu pravnu zaštitu koja će provoditi u suradnji s nadležnim organizacijama i ustanovama drugih zemalja.[108] Jedan od većih problema je što ni danas, ne postoji neka općeprihvaćena definicija, kao ni točna klasifikacija oblika koje može podvesti pod njega. Shodno tome svaka zemlja može samostalno kriminalizirati njegove pojavne oblike, čime mnoga kriminalna ponašanja mogu ostati izvan okvira pravne regulacije. Pozornost treba posvetiti generalnoj prevenciji odnosno odvraćanju od takvog činjenja, ali isto tako propisivanju novih kaznenih djela i sankcija za počinitelje. Hrvatski KZ tako je u srpnju 2021. uveo novo kazneno djelo „zlouporaba snimke spolno eksplicitnog sadržaja“ čime pokazuje da prati neka razvijenija zakonodavstva. No prema Kokotu, većina kaznenih djela kibernetičkog kriminala je postavljena šire od međunarodnih izvora, dok su pojedina kaznena

[106] Roksandić, Op.cit.(bilj.84)
[107] Babić, Vladica, Novi oblici djelovanja terorista (Cyber terorizam), Zbornik radova IV. Međunarodno znanstvene-stručne konferencije „Istraživački dani visoke policijske škole u Zagrebu“, 2015., str. 11-26.
[108] Hamidović, Amra, Hamidović Haris, Zajmović Mahir, Okvir za rješavanje problema cyber kriminala, Infoteh-Jahorina Vol.15, March 2016., str. 557-562.

djela nedorađena. Računalni podaci, programi, mreže kao temeljni podaci su različito prevedeni, protumačeni i kroz zakonski tekst različito postavljeni.[109] Također danas imamo i porast cyber terorizma, koji je možda čak i najmanjkavije zakonski uređen od svih navedenih kaznenih djela. Terorističke skupine sve više koriste Internet za širenje svoje propagande, regrutiranje novih članova i prikupljanje sredstava.[110] KZ RH sadrži generalne odredbe o terorizmu, a jedina odredba koja se odnosi na cyber terorizam je navedena u čl. 97. st.1. t.10., a njime je opet obuhvaćeno samo ometanje rada računalnog sustava, te oštećenje računalnih podataka kada je počinjeno u odnosu na računalni sustav kritičke infrastrukture. Kibernetički kriminal je globalni fenomen, tako da je za borbu i prevenciju potrebna međunarodna suradnja s obzirom da su počinitelj i žrtva nerijetko iz različitih država. Stoga smatram da je potreban širi pristup i suradnja na ovom području, kao i stalno praćenje situacije, kako bi se novi pojavni oblici adekvatno regulirali. Konvencija o kibernetičkom kriminalu zajedno sa Direktivom 2013/40/EU za sada postavlja zadovoljavajuće okvire za kriminalizaciju kažnjivih ponašanja, ali s ovakvim rastom i tehnološkim napretkom uskoro neće biti dovoljna.

[109] Kokot, Op.cit. (bilj.5)
[110] Babić, Op.cit. (bilj. 107)

7. LITERATURA

Akademski članci i knjige:

1. Antoliš Krunoslav, Internetska forenzika i cyber terorizam, Policija i sigurnost, Vol.19, No.1, 2010.
2. Babić Vladica, Kompjuterski kriminal: metodologija kriminalističkih istraživanja, razjašnjavanja i suzbijanja kompjuterskog kriminala, Rabic Sarajevo, 2009.
3. Babić Vladica, Novi oblici djelovanja terorista (Cyber terorizam), Zbornik radova IV. Međunarodno znanstvene-stručne konferencije „Istraživački dani visoke policijske škole u Zagrebu“, 2015.
4. Bača Miroslav, Uvod u računalnu sigurnost Zagreb, Narodne novine, 2004.
3. Brkić Goran, Radat Katarina, Vejmelka Lucija, Dječja pornografija na internetu-obilježja osuđenih počinitelja, Pravni vjesnik, časopis za pravne i društvene znanosti Pravnog fakulteta Sveučilišta J.J. Strossmayera u Osijeku, Vol.33, No.2, 2017.
4. Dragičević Dražen, Kompjutorski kriminalitet i informacijski sustavi Zagreb, Informatorov biro sustav, 2004.
5. Hamidović Amra, Hamidović Haris, Zajmović Mahir, Okvir za rješavanje problema cyber kriminala, Infoteh-Jahorina Vol.15, 2016.
6. Horvatić Željko, Osnove kriminologije, Ministarstvo unutarnjih poslova Republike Hrvatske, Zagreb, 1988.
7. Kokot Ivica, Kaznenopravna zaštita računalnih sustava, programa i podataka, Zagrebačka pravna revija, Vol.3, No.3, 2014.
8. Kunda Ivana, Raspolaganje autorskim pravom na računalnom programu – materijalnopravni i kolizijskopravni aspekti, Zbornik Pravnog fakulteta Rijeka (1991), v.31, br.1, 2010.
9. Manuilenko Olena, Vukmir Mladen, Računalni programi kao objekt zaštite prema Autorskom pravu i srodnim pravima, Zbornik Hrvatskog društva za autorsko pravo, Volumen 5, 2004.
10. Munivrana Vajda Maja, Marton Šurina Andrea, Gdje prestaju granice slobode izražavanja, a počinje govor mržnje? Analiza hrvatskog zakonodavstva i prakse u svjetlu europskih pravnih standarda, Hrvatski ljetopis za kaznene znanosti praksu, Zagreb, vol. 23, broj 2/2016.

11. Nedić Tomislav, Vuletić Igor, Računalna prijevara u hrvatskom kaznenom pravu, Zbornik pravnog fakulteta Sveučilišta u Rijeci, Vol.35, No.2, 2014.
12. Protrka Nikola, Računalna prijevara – analiza djelotvornosti otkrivačke djelatnosti, Policija i sigurnost, Vol.28., No. 3/20019, 2019.
13. Pavlović Šime, Kompjutorska kaznena djela u Kaznenom zakoniku, Hrvatski ljetopis za kazneno pravo i praksu, Zagreb, vol. 10, broj 2/2003.
14. Roksandić Sunčana, Šesta novela kaznenog zakona – uvođenje virtualnih valuta i „osvetničke pornografije“ te dodatna zaštita odnosa povjerenja i ranjivih osoba, Hrvatski ljetopis za kaznene znanosti i praksu, vol 28 No.2, 2021.
15. Sieber Ulrich, Computer Crime and Criminal Information Law – New Trends in the International Risk and Information Society, Computer und Recht, 1995.
16. Šimundić Slavko, Računalni kriminalitet Split, Pravni fakultet Sveučilišta, 2009.
17. Šimundić Slavko, Manipulacija računalom s ciljem ostvarivanja vlastite koristi Zbornik radova Pravnog fakulteta u Splitu, 2001.
18. Šimović Vladimir, Mogućnosti tehnološke prevencije kompjutorskog kriminaliteta u svezi s elektroničkim novčanim transakcijama, Zbornik radova Pravnog fakulteta u Splitu, 1999.
19. Škrtić Dražen, Kaznena djela računalnog kriminaliteta u novom kaznenom zakonu Republike Hrvatske, Slovenski dnevi varstvoslovja, Zbornik prispevkov, Fakulteta za varnostne vede, Ljubljana, 2012.
20. Vojković Goran, Štambuk-Sunjić Marija, Konvencija o kibernetičkom kriminalu i kazneni zakon Republike Hrvatske, Zbornik radova Pravnog fakulteta u Splitu, svezak 43, br. 1, 2006.
21. Zlatović Dragan, Pravo intelektualnog vlasništva u suvremenom digitalnom okruženju, Zagreb, 2009.

Pravni izvori:

1. Direktiva 2018/1972/EU Europskog parlamenta i Vijeća od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija, Službeni list Europske Unije, 17.12.2018.
2. Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, Službeni list Europske Unije, 12.8.2013.

3. Direktiva 2017/541/EU Europskog parlamenta i Vijeća od 15. ožujka 2017. o suzbijanju terorizma i zamjeni Okvirne odluke Vijeća 2002/475/PUP i o izmjeni odluke Vijeća 2005/671/PUP, Službeni list Europske Unije, 31.3.2017.
4. Kazneni zakon, NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21
5. Kodeks postupanja za borbu protiv nezakonitog govora mržnje na internetu, 2016.
6. Komunikacija komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i odboru regija Unija ravnopravnosti: Akcijski plan EU-a za antirasizam za razdoblje od 2020.-2025.
7. Konvencija Vijeća Europe o kibernetičkom kriminalu, 2001.
8. Odluka o pokretanju postupka za sklapanje Drugog dodatnog protokola uz Konvenciju o kibernetičkom kriminalu o pojačanoj suradnji i otkrivanju elektroničkih dokaza, Vlada republike Hrvatske, 12. svibnja 2022.
9. Okvirna odluka Vijeća 2008/913/PUP od 28. studenoga 2008. o suzbijanju određenih oblika i načina izražavanja rasizma i ksenofobije kaznenopravnim sredstvima, Službeni list Europske Unije, 6.12.2008.
10. Uredba 2021/784 Europskog parlamenta i Vijeća od 29. travnja 2021. o borbi protiv širenja terorističkog sadržaja na internetu, Službeni list Europske Unije, 29.4.2021.
11. Uredba o preuzimanju Direktive 2013/40/EU o napadima na informacijske sustave te Direktive 2014/62/EU o kaznenopravnoj zaštiti eura i drugih valuta od krivotvorenja, NN 102/2015.
12. Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava, NN 4/2008.
13. Zakon o autorskim i drugim srodnim pravima, NN 111/21
14. Zakon o informacijskoj sigurnosti, NN 79/07
15. Zakon o izmjenama i dopunama Kaznenog zakona, NN 84/2021.
16. Zakon o kaznenom postupku, NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19, 126/19
17. Zakon o suzbijanju diskriminacije, NN 85/08, 112/12

Sudska praksa:

1. OS u Novom Zagrebu, K-397/20-9 od 27.1.2021.
2. ŽS u Osijeku, Kzd 4/2021-5. od 1.7.2021.

Mrežne stranice:

1. Borba protiv rasizma traži jačanje i bolju implementaciju zakona https://www.ombudsman.hr/hr/borba-protiv-rasizma-trazi-jacanje-i-bolju-implementaciju-zakona/
2. Cyber crime legislation https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/Tafazzoli-cybercrime%20legislations.pdf
3. Cyberterrorisam after Stuxnet https://www.jstor.org/stable/resrep11324?seq=1
4. Covid i kriminalitet u 2020. Komentar pokazatelja sigurnosti u Republici Hrvatskoj https://mup.gov.hr/UserDocsImages/2021/04/Covid%20i%20kriminalitet%20u%202020%20-%20Komentar%20pokazatelja%20sigurnosti%20u%20Republici%20Hrvatskoj.pd
5. Legislation https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx
6. Nove izmjene kaznenog zakonodavstva https://www.iusinfo.hr/aktualno/u-sredistu/46843
7. Općinsko državno odvjetništvo u Zagrebu. Ispitano dvoje osumnjičenika zbog krivotvorenja isprava i zlouporaba položaja i vlasti https://dorh.hr/hr/priopcenja/opcinsko-drzavno-odvjetnistvo-u-zagrebu-ispitano-dvoje-osumnjicenika-zbog-krivotvorenja
8. Osvetnička pornografija https://babe.hr/osvetnicka-pornografija-2/
9. Pravna zaštita autorskog prava https://www.iusinfo.hr/aktualno/u-sredistu/19603
10. Recommendation No. R(89)9 of the Committee of ministers to member states on computer-related crime https://rm.coe.int/09000016804f1094
11. Sankcioniranje cyber nasilja prema novom Kaznenom zakonu https://www.iusinfo.hr/aktualno/u-sredistu/13063
12. Što je to „deep fake“ https://znatko.com/7321/sto-je-to-deep-fake
13. Tijekom pandemije značajno porasle štete prouzrokovane kibernetičkim kriminalom https://faktograf.hr/2022/02/23/tijekom-pandemije-znacajno-porasle-stete-prouzrocene-kibernetickim-kriminalom/