Kaznenopravna zaštita od kibernetičkog kriminala i uloga davatelja telekom usluga

Mikulin, Robert

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Robert Mikulin

KAZNENOPRAVNA ZAŠTITA OD KIBERNETIČKOG KRIMINALA I ULOGA DAVATELJA TELEKOM USLUGA

DIPLOMSKI RAD

Zagreb, 2019.

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 29. ožujka 2019.

Zavod: **Zavod za informacijsko komunikacijski promet**

Predmet: **Telekomunikacijska legislativa i standardizacija**

DIPLOMSKI ZADATAK br. 5141

Pristupnik: **Robert Mikulin (0135244894)**

Studij: Promet

Smjer: Informacijsko-komunikacijski promet

Zadatak: **Kaznenopravna zaštita od kibernetičkog kriminala i uloga davatelja telekom usluga**

Opis zadatka:

Borba protiv cyber-kriminala uvelike se temelji na suradnji davatelja telekomunikacijskih usluga s nadležnim tijelima. Davatelj usluga je upravo onaj tko posjeduje informacije o najvažnijoj poveznici - tko stoji iza određene IP adrese na Internetu, pa i gdje se ta osoba fizički nalazi. Takvi podaci su iznimno važni u pronalaženju počinitelja cyber-kaznenih djela, no s druge strane davatelj usluga mora osigurati i zaštitu privatnosti korisnika, kako ne bi došlo do zloporabe podataka. U radu je potrebno razjasniti taj odnos, te mjere koje se moraju poduzeti kako bi s jedne strane podaci bili sačuvani, ali ujedno i sačuvana privatnost korisnika od zlonamjernih i nezakonitih prikupljanja i obrade osobnih podataka.

Mentor:

doc. dr. sc. Goran Vojković

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

KAZNENOPRAVNA ZAŠTITA OD KIBERNETIČKOG KRIMINALA I ULOGA DAVATELJA TELEKOM USLUGA

CRIMINAL AND LEGAL PROTECTION FROM CYBERCRIME AND ROLE OF TELECOM SERVICES PROVIDERS

Mentor: izv. prof. dr. sc. Goran Vojković

Student: Robert Mikulin
JMBAG: 0135244894

Zagreb, rujan 2019.

KAZNENOPRAVNA ZAŠTITA OD KIBERNETIČKOG KRIMINALA I ULOGA DAVATELJA TELEKOM USLUGA

SAŽETAK

Razvojem računalne tehnologije, uz tradicionalne vrste kriminalnih radnji, pojavio se i novi oblik kriminaliteta koji uključuje uporabu računalnih tehnologija. Ta nova vrsta kriminala nazvana je "kibernetički kriminal", i obzirom na karakter tih radnji, došlo je do potrebe potpuno novog pristupa u borbi sa tom vrstom kriminala. Osnovane su razne globalne, regijske i nacionalne institucije čiji je zadatak donesti nove preporuke i odredbe koje bi se trebale implementirati u nacionalne kaznenopravne okvire. Pretpostavka za uspjeh protiv ovakve vrste kriminala je i globalna suradnja svih zemalja, pa će se u ovome radu analizirati uspješnost i izazovi pravne borbe koji se pojavljuju na raznim nacionalnim, ili pak međunarodnim nivoima. Također, poseban osvrt napraviti će se na utjecaj kibernetičkih prijetnji na davatelje telekom usluga i internetske platforme.

KLJUČNE RIJEČI: kibernetički kriminal; kaznenopravni okvir; davatelj telekom usluga

SUMMARY

With the development of computer technology, along with the traditional types of criminal activities, a new form of criminality has emerged that involves the use of computer technologies. This new kind of crime was called "cybercrime", and given the character of these actions, there was a need for a completely new approach to fighting this type of crime. Various global, regional and national institutions have been set up, whose task is to make new recommendations and directives that should be implemented in national criminal justice frameworks. The prerequisite for success against this kind of crime is the global co-operation of all countries, so in this paper there will be analyzed the success and challenges of legal struggle that occur at various national or international levels. Also, special attention will be given to the impact of cyber threats on providers of telecom services and the Internet platforms.

KEYWORDS: cybercrime; legal justice framework; telecom service provider

SADRŽAJ

1. Uvod

Razvojem informacijskih i komunikacijskih računalnih tehnologija, te pojavom nove vrste kriminala nazvane kibernetički kriminal, postojeći pravni okviri više nisu zadovoljavali, odnosno nisu omogućavali kvalitetnu istražnu metodologiju koju je ta vrsta kriminala zahtijevala.

Danas svjedočimo 4. industrijskoj revoluciji koja podrazumijeva automatizaciju i izmjenu podataka između gotovo svih vrsta "živih" uređaja, i uz upotrebu 5G mreža iznimno velikih kapaciteta, povezanost svega sa svime – *Internet of things* i računalne oblake, a svaki aspekt upotrebe tehnologije i uređaja dobiva naziv "pametan". Takav neviđen tehnološki skok koji mijenja apsolutno svaki aspekt ljudskog života na način da je sve povezano i lako dostupno, nosi sa sobom i jedan od najvećih izazova u ljudskoj povijesti – kako takav tehnološki sustav na kojem počiva ljudska civilizacija zadržati sigurnim.

Obzirom na međunarodni karakter te vrste kriminala, ukazala se nužnost za donošenjem novih zakona i definicija, kako na nacionalnim nivoima, tako i na međunarodnom planu. Globalna suradnja pokazati će se kao ključan faktor u ovoj borbi, što je direktno uticalo na osnivanje niza novih institucija, nacionalnih i međunarodnih, kako bi se taj pravni okvir i ta međunarodna suradnja efikasno provodila. U sklopu navedene teme, opisalo bi se koji su to kaznenopravni okviri nastali kao odgovor na kibernetički kriminal, kako na međunarodnom planu, tako i u Republici Hrvatskoj.

Rad će bit podijeljen na slijedeća poglavlja:

1. Uvod
2. Definicija, razvoj i vrste kibernetičkog kriminala
3. Odgovor međunarodne zajednice na kibernetički kriminal
4. Kaznenopravni okvir Republike Hrvatske obzirom na kibernetičke prijetnje
5. Utjecaj kibernetičkog kriminala na davatelje telekom usluga
6. Pravo nadzora nasuprot prava privatnosti i slobode govora
7. Zaključak

U poglavlju 2., definirati ćemo što sve podrazumijeva kibernetički kriminal, ima li taj pojam jednako značenje globalno ili postoje razlike u interpretaciji istoga. Vidjeti će se kako se taj oblik kriminala razvijao od svojih začetaka pojavom računalne

tehnologije, pa sve do danas, kada je taj vid kriminala postao jedan od najzastupljenijih oblika kriminala.

Kroz poglavlje 3., objasniti će se na koji je način odgovorila međunarodna zajednica na taj vid kriminala, posebno kako je reagirala Europska Unija i kako je to utjecalo na Republiku Hrvatsku i njen kaznenopravni okvir.

U nastavku, poglavlje 4. obrađuje zakone i institucije Republike Hrvatske koje se bave ovom tematikom, a nastale su direktno usklađivanjem kaznenopravnog okvira sa Europskom Unijom i njihovim Direktivama i Preporukama. Također, dati će se statistički uvid u prisutnost ove vrste kriminala u Republici Hrvatskoj u prošle dvije godine.

Poglavlje 5. dati će odgovore na pitanja koja je uloga i koje su obveze mrežnih operatera i davatelja telekom usluga u sprječavanju kibernetičkog kriminala. U radu bi bile opisane generalne smjernice za sigurnosnu zaštitu kritične infrastrukture, najčešće implementirani mehanizmi, regulativa i pravni okvir koji obavezuje davatelje telekom usluga, te posebno analiza problema sa kojima se suočavaju davatelji telekom usluga u provođenju smjernica Konvencije o kibernetičkom kriminalu.

Pitanje koje se uvijek provlači u borbi protiv te vrste kriminala je i gdje je granica narušavanja privatnosti prilikom nadzora u preveniranju te vrste kriminala. Sveopći nadzor i monitoriranje aktivnosti privatnih i pravnih osoba na javnim mrežama, nerijetko je u sukobu sa zakonima koji štite privatnost, razne osobne podatke ili slobode govora i izražavanja mišljenja. U poglavlju 6., opisano bi bilo kakvih promjena ima na tom polju, odnosno što je donio novi Zakon o provedbi Opće uredbe o zaštiti podataka.

2. Definicija, razvoj i vrste kibernetičkog kriminala

Od pojave prvih računala, postojali su i ljudi koji su pokušavali pribaviti ilegalnu korist pomoću tih računala, ili ukrasti informacije čuvane na računalnim sustavima. Naravno, razvojem informatičkih sustava, evolucijom računala i računalnih mreža, te pojavom Interneta – razvio se i novi aspekt kriminala koji je koristio novonastale resurse i infrastrukture za počinjenje postojećih nezakonitih radnji, ali i otvorio mogućnosti nastanku nekih sasvim novih kriminalnih radnji kojima je tehnologija otvorila put. Kako je preduvjet nastanka kibernetičkog kriminala razvoj komunikacijske i računalne infrastrukture, prvi počinitelji i prve žrtve su bile u Sjedinjenim Američkim Državama, no eksponencijalni rast informacijsko-komunikacijskih resursa u cijelom svijetu uskoro je polučio time da niti jedan kutak u svijetu nije ostao nedotaknut od strane kibernetičkog kriminala. Danas, kriminalce koji se upuštaju u računalni kriminal, ne pokreće ego ili stručnost. Umjesto toga, žele koristiti svoje znanje kako bi na brz način stekli određene materijalne koristi. Kibernetički kriminal danas je postao stvarna prijetnja i sasvim je različit od klasičnih kaznenih djela. Za razliku od ovih zločina, kibernetički kriminal ne zahtijeva fizičku prisutnost kriminalaca. Zločini se mogu počiniti s udaljenog mjesta i kriminalci ne moraju brinuti o institucijama za provođenje zakona u zemlji u kojoj čine zločine. Isti sustavi koji su ljudima olakšali provođenje e-trgovine i mrežnih transakcija sada se iskorištavaju od strane kibernetičkih kriminalaca. Na početku, izrazito je bitno da se jednoznačno definiraju pojmovi "računalni kriminal" i "kibernetički kriminal", tj. pobliže odredi u kojem su odnosu ta dva termina.

2.1 Definicija pojmova

Zadnjih nekoliko desetljeća usvojeni su razni pristupi koji se bave tematikom računalnog i kibernetičkog kriminala i pokušavaju dati preciznije definicije ta dva pojma.

Odmah na prvu, pojam "kibernetički kriminal" je uži od pojma "računalnog kriminala", jer mora uključivati korištenje računalne mreže, lokalne ili globalne. Pojam "računalni kriminal" odnosi se na sve kriminalne radnje u kojima je korišteno računalo i kao samostalan uređaj, bez korištenja računalne mreže. Za vrijeme desetog kongresa Ujedinjenih naroda (UN) na temu "Sprječavanje kriminala i postupanje sa počiniteljima", na tematskim radionicama iskristalizirale su se dvije definicije [1]:

- kibernetički kriminal u užem smislu (ovdje specificiran i kao računalni kriminal), obuhvaća svako nezakonito ponašanje putem elektroničkih operacija kojima je cilj ugroziti sigurnost računalnih sustava ili sigurnost podataka koje ti sustavi obrađuju
- kibernetički kriminal u širem smislu (ovdje specificirano kao kaznena djela koja su povezana sa računalom) obuhvaća svako nezakonito ponašanje u koje je uključeno korištenje računala ili mreže, bilo da je cilj ugroziti sigurnost računalnih sustava ili je cilj ilegalno posjedovanje i distribucija informacija i sadržaja

Jedna zajednička definicija opisuje kibernetički kriminal kao svaku aktivnost u koju je involvirano računalo ili računalna mreža kao sredstvo, cilj ili mjesto kriminalne aktivnosti. Ovakva široka definicija stvara dosta poteškoća, jer bi onda to uključivalo i tradicionalne kriminalne radnje poput ubojstva, otmica i sl.

Neke druge šire definicije pokušavaju precizirati ciljeve i namjere i točnije definirati kibernetički kriminal, kao npr. [1], [2]:

- kibernetički kriminal su kaznena dijela koja se odnose na kibernetičke sisteme
- kibernetički kriminal su računalno posredovane aktivnosti koje su ili nezakonite ili se smatraju nedopuštenim od strane određenih interesnih skupina, i koje se mogu provoditi putem globalnih računalnih mreža

Ovakve definicije isključuju klasična kaznena dijela u kojima se pojavljuje računalo kao sredstvo počinjenja kaznenog djela ili kao dio dokaza, ali isto tako nose rizik da isključe neka kaznena djela koja se smatraju kibernetičkim kriminalom u nekim međunarodnim sporazumima, poput npr. Konvencije Vijeća Europe o kibernetičkom kriminalu. Na primjer, osoba koja pomoću zlonamjernih računalnih programa na USB prenosnom uređaju obriše podatke na nekom računalnom sustavu, to djelo ne bi bilo okvalificirano kao kibernetički kriminal prema tim definicijama, jer nije počinjeno korištenjem računalnih mreža.

Različiti pristupi, kao i povezani problemi, pokazuju da postoje znatne teškoće u definiranju pojmova "računalni kriminal" i kibernetički kriminal", obzirom da se odnose na opisivanje niza kaznenih djela, kako tradicionalna računalna kaznena dijela, tako i na mrežna. Budući da se ta kaznena dijela razlikuju na mnogo načina, ne postoji jedinstveni kriterij koji bi uključivao sve radnje spomenute u različitim međunarodnim

pravnim okvirima. Činjenica da ne postoji jedinstvena definicija kibernetičkog kriminala ne mora biti važna, sve dok se taj pojam ne koristi kao pravni termin. Umjesto definicije, možemo se služiti tipološkim pristupom, kao što je npr. definirano u spomenutoj Konvenciji Vijeća Europe o kibernetičkom kriminalu, koja razlikuje četiri različita tipa kaznenih djela kibernetičkog kriminala [1], [2]:

- kaznena dijela protiv povjerljivosti, cjelovitosti i dostupnosti računalnih podataka i sustava
- kaznena dijela povezana sa sadržajem
- kaznena dijela povezana sa autorskim pravima
- kaznena djela povezana sa računalom

Ova tipologija nije u potpunosti dosljedna, jer se ne temelji na istom kriteriju za razlikovanje kategorija. Prve tri navedene kategorije odnose se na objekt pravne zaštite (podaci, sadržaj, autorska prava), a četvrta kategorija bavi se načinom koji se koristi za počinjenje kaznenog djela. Ova nedosljednost dovodi do preklapanja među kategorijama, odnosno neka kaznena dijela mogu spadati u više kategorija istovremeno. U svakom slučaju, ovakva tipologija može biti dobar temelj za daljnje rasprave na temu kibernetičkog kriminala.

2.2 Razvoj kibernetičkog i računalnog kriminala

Kriminalna zlouporaba informacijske tehnologije, i nužnost pravnog okvira na tu temu, su predmet raznih rasprava tijekom posljednjih šezdesetak godina, od kada je počeo ubrzani tehnološki razvoj. Jedan od razloga neprestanih rasprava, je brzina tehnološkog razvoja, kao i promjenjivost metoda počinjenja kaznenih djela.

2.2.1 Šezdesete godine prošlog stoljeća

Negdje šezdesetih godina prošlog stoljeća, pojavom tranzistorskih računala koja su bila manja i jeftinija od dotadašnjih računala baziranih na vakuumskim cijevima, došlo je do rasta korištenja računalne tehnologije i njene primjene. U tim ranim fazama, kaznena dijela su se većinom odnosila na fizičko uništavanje računalnih sustava ili spremljenih podataka [1], [3].

2.2.2 Sedamdesete godine prošlog stoljeća

Tokom sedamdesetih godina dolazi do značajnijeg povećanja primjene računalnih sustava, mahom *mainframe* sustava kojih je npr. samo u Sjedinjenim Američkim Državama (USA) bilo oko 100 000 na kraju dekade. Padom cijena, ta tehnologija je nalazila sve veću primjenu u vladinoj administraciji, kao i u poslovnim okruženjima. Uz postojeći oblik kaznenog dijela fizičkog uništenja računalnih sustava koji je dominirao šezdesetim godinama, razvili su se i novi oblici računalnog kriminala, poput ilegalnog korištenja računalnih sustava i manipulacije elektroničkim podacima. Isto tako, pomak sa ručnih na računalne transakcije doveo je do prevara počinjenih pomoću računala, koje su uzrokovale multimilijunsku štetu. Sve to potaklo je diskusiju o pravnom odgovoru na takva kaznena dijela, obzirom da je postojeći pravni okvir imao dosta poteškoća sa tim novim oblicima kaznenih djela [1], [3].

2.2.3 Osamdesete godine prošlog stoljeća

Već u idućoj dekadi, osamdesetih godina, korištenje osobnih računala postaje sve popularnije. Samim time, narastao je i broj potencijalnih ciljeva kaznenih dijela. Također, širenjem navedene tehnologije, povećao se i interes i potreba za raznim računalnim programima, što je dovelo do prve pojave piratskih programa i krađa patenata i autorskih prava. Pojava računalnih mreža omogućila je počinjenje zločina bez prisutnosti na mjestu zločina, kao npr. širenje malicioznih programa i virusa. Obzirom na promjenu okoline počinjenja kaznenih djela, države su počele prilagođavati svoje pravne okvire novonastaloj situaciji, a po prvi puta uplele su se i međunarodne organizacije u taj proces. Organizacija za ekonomsku suradnju i razvoj (OECD) i Vijeće Europe uspostavile su radne skupine koje su trebale analizirati novonastali fenomen i procijeniti mogućnosti za pravni odgovor [1], [3].

2.2.4 Devedesete godine prošlog stoljeća

Pojavom grafičkih sučelja i globalne Internet mreže došlo je do novih izazova. Informacije koje su u nekoj državi bile legalne, postale su dostupne putem Interneta i u državama u kojima su ilegalne. Računalni kriminal je odjednom postao transnacionalna pojava sa izrazito brzom izmjenom informacija. Npr. dječja pornografija koja se razmjenjivala fizički u obliku slika, video vrpci, sada se razmjenjivala elektronski. Rezultat je bio veći angažman međunarodne zajednice na

temu suzbijanja kibernetičkog kriminala koji je poprimio oblik međunarodnog kriminala. Rezolucija 45/121 opće skupšine UN-a usvojena 1990. godine, jedan je primjer tog angažmana [1], [3].

2.2.5 Dvadeset prvo stoljeće

Dvadeset prvo stoljeće je donijelo nikad brži razvoj informatičke i komunikacijske tehnologije, a sa njime i sasvim nove izazove u borbi protiv kibernetičkog kriminala. Nove sofisticirane metode napada poput *phishing* i *botnet* napada, nove tehnologije koje otežavaju istragu (*Voice over IP* - VoIP komunikacija, računalstvo u oblaku, *Internet of Things*), automatizirani napadi koji eksponencijalno povećavaju broj kaznenih dijela – rezultat toga je da je na nacionalnim i međunarodnim scenama kibernetički kriminal i pravni odgovor na njega dobio vrhunski prioritet [1], [3].

2.3 Vrste kibernetičkog kriminala

Kako je već spomenuto, vrsta kibernetičkog kriminala ima mnogo i gotovo svaki dan svjedočimo pojavi neke nove vrste napada, i taj trend raste eksponencijalno zajedno sa potencijalnim metama, tj. poslovnim i privatnim računalima, te podatkovnim centrima.

Najčešća podjela kibernetičkog kriminala podrazumijeva slijedeće četiri kategorije [1], [2]:

- kaznena djela protiv povjerljivosti, cjelovitosti i dostupnosti računalnih podataka i sustava
- kaznena djela povezana sa sadržajem
- kaznena djela povezana sa autorskim pravima
- kaznena djela povezana sa računalom

U nastavku, dati će se pregled najčešćih kaznenih djela vezanih uz pojedinu kategoriju.

2.3.1 Kaznena djela protiv povjerljivosti, cjelovitosti i dostupnosti računalnih podataka i sustava

Sva kaznena djela u ovoj kategoriji usmjerena su protiv barem jednog od tri pravna načela povjerljivosti, integriteta i dostupnosti. Kompjuterizacija tih kaznenih

djela zahtjeva i poboljšani pravni okvir koji može pružiti adekvatnu zaštitu baziranu na tim novim principima.

Najčešća kaznena djela povezana sa ovom kategorijom odnose se na nezakonit pristup računalnom sustavu pod nazivom *hacking* , što je ujedno i jedno od najstarijih računalnih kaznenih djela. Pojavom Interneta, ova vrsta napada postaje masovan fenomen. Većinom se svodi na razne metode kojima se pokušava otkriti lozinka korisnika, i na taj način ostvariti pristup njihovim računalima. Motivi za ovakve napade variraju – od samodokazivanja unutar hakerskih zajednica, preko politički motiviranih, pa sve do napada sa ciljem ostvarivanja financijske koristi.

Tri su faktora koja omogućavaju takav rast ove vrste napada: neadekvatna zaštita računala, automatizacija napada i veliki porast količine osobnih računala kao potencijalnih ciljeva.

Krađa informacija sa korporativnih računalnih sustava ili elektronička špijunaža je također vrlo čest oblik kriminala. Metode i tehnike napada podrazumijevaju otkrivanje nezaštićenih portova, ili rupa u mjerama zaštite, i u najnovije vrijeme – socijalni inženjering. Ovaj posljednji tip napada je izuzetno plodan, obzirom da je operater računala odnosno ljudski faktor najčešće i najslabija karika unutar zaštitne politike. Jedna od najpoznatijih tehnika unutar socijalnog inženjeringa je svakako *phishing* – pokušaji da se prevarom ili krivim predstavljanjem izvuku osjetljive informacije od pojedinaca.

Još jedan od vrlo čestih napada, poznat je kao "presretanje" podataka, a korištenjem različite komunikacijske infrastrukture, bilo bežične ili žične, kao i bilo kojeg Internet servisa (*e-mail*, *chat*,VoIP....).

Razne vrste zlonamjernih programa, npr. poput "virusa" i "crva" napadaju integritet i dostupnost podataka na način da ih unište, obrišu ili kriptiraju i onemoguće korištenje istih, te na taj način mogu prouzročiti velike financijske štete. Nekada se računalo moglo zaraziti preko prenosnih medija, danas se to najčešće i najlakše dogodi preko interneta koristeći razne Internet servise.

Uz navedene vrste napada, raširen je i *Denial of Service* (DoS) ili "uskraćivanje usluge" tip napada. Takav napad podrazumijeva da meta ne može koristiti svoje računalne resurse i servise, a obično se izvodi preopterećivanjem i zagušenjem mrežnog prometa ciljanog računalnog sustava [1].

2.3.2 Kaznena djela povezana 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 i mržnju prema strancima, kao i diskriminaciju i vrijeđanje u vjerskom smislu. U ovom slučaju, definicija toga što je nezakonit sadržaj, uvelike ovisi o nacionalnim kulturološkim vrijednostima koji su implementirani u lokalni pravni sustav, i može se bitno razlikovati od države do države. Upravo zbog toga, pravna borba protiv te kategorije kaznenih djela svodi se na nacionalni nivo, najčešće filtere koji pronalaze uvredljiv ili nedopušten sadržaj te ga blokiraju na internetu za korisnike unutar svoje države.

Erotski ili pornografski materijal, koji ne uključuje dječju pornografiju, jedan je od najprisutnijih sadržaja na Internetu. Odnos prema takvom sadržaju opet se razlikuje od države do države, pa tako negdje može biti potpuno dozvoljen za punoljetne osobe, a negdje potpuno zabranjen. Pravno gonjenje i zabrana takvih sadržaja je također poprilično onemogućena, obzirom da se često takav sadržaj nalazi na serverima u drugim zemljama koje imaju potpuno drugačiji pravni okvir. Na kraju, ponovo najefektnija metoda je filtriranje web sadržaja i provjera punoljetnosti prilikom pristupa takvom sadržaju, mada sama provjera je deklarativnog karaktera i ne sprječava lažno predstavljanje i pristup toj vrsti sadržaja.

Borba protiv snimanja i distribucije dječje pornografije postala je bitno složenija. U prošlosti, takav materijal je bilo i teško snimiti, i teško umnažati i distribuirati bez gubitka kvalitete. Traganje za takvim kriminalnim djelima je bilo lakše, jer se znalo tko ima mogućnosti i opremu za snimati takav materijal. Pojavom kamera za osobnu upotrebu, npr. kakve danas imamo u svakom mobilnom uređaju, takav materijal je u mogućnosti snimiti bilo tko, a prelazak sa analogne na digitalnu tehnologiju omogućio je distribuciju materijala bez gubitka kvalitete. Tehnički slabije obrazovanim skupinama, Internet pruža privid anonimnosti prilikom pregledavanja ili distribuiranja takvog materijala, tako da se količina istog rapidno povećala. Naravno, obzirom na veliku financijsku korist koju distributeri takvog materijala stječu, trgovanje takvim materijalima većinom se odvija unutar zatvorenih grupa ili foruma, kojima nema pristup bilo tko, pa je i na taj način otežan pravni progon. Enkripcija i virtualne valute su dvije tehnologije koje u najvećoj mjeri otežavaju otkrivanje ovakvih kaznenih djela.

Većina političkih i drugih ekstremista koristi masovnu komunikaciju, kao npr. što je Internet, za širenje svoje propagande. Postoje brojni *web* sadržaji govora mržnje, rasističke tematike ili veličanja nasilja i netolerancije bilo koje vrste. Na takvim *web* mjestima prodaje se i roba sa obilježjima takvih skupina, npr. roba sa nacističkim simbolima. I ovdje postoji razlika u zakonodavstvu pojedinih država, gdje je takav istup u nekima nezakonit, a u nekima je zaštićen slobodom govora, što je ujedno i jedan od najvećih prijepora međunarodnoj suradnji u borbi protiv kibernetičkog kriminala. Slična je situacija i sa objavljivanjem potencijalno uvredljivog sadržaja baziranog na vjerskoj osnovi.

Ilegalno kockanje, klađenje i *on-line* igre, osim što izbjegavaju poreze, ili su u nekim zemljama zabranjeni, često su i paravan za pranje novca i financiranje terorizma. Mnoge zemlje, uključujući i Republiku Hrvatsku, počele su blokirati IP adrese za primanje uplata takvih nelegalnih kladionica, prvenstveno zbog neplaćanja poreza na dobitak u tim zemljama.

Kleveta ili objavljivanje lažnih informacija, također su kazneno djelo. Prestupnicima ove vrste takve radnje su omogućene već samim time što većina foruma i pružatelja servisnih usluga ne zahtjeva točnu identifikaciju osobe koja ostavlja komentar. Ovaj vid kaznenog djela, iako na prvu ne izgleda strašan, može imati dalekosežne posljedice po žrtvu takvog djela.

Spam je naziv za masovno slanje neželjenih poruka, koje najčešće sadrže promotivne objave, a nerijetko i zlonamjerne programe. Postoje filteri koji blokiraju ovakve vrste poruka prema ključnim riječima ili crnim listama pošiljaoca, i premda su svakim danom sve napredniji, ipak 90% svih poruka je *spam* [1].

2.3.3 Kaznena djela povezana sa autorskim pravima

Digitalizacija je omogućila mnoge dodatne funkcionalnosti i servise filmovima, muzici i ostalim tipovima digitalnih materijala u zabavnoj industriji, ali istovremeno otvorila vrata novim kaznenim djelima povezanim sa kopiranjem i ilegalnom distribucijom takvog sadržaja. Naime, osnova ilegalne trgovine takvim materijalima je kopiranje bez gubitka kvalitete reprodukcije, a *peer-to-peer* (P2P) mrežna tehnologija omogućila je i vrlo lako distribuiranje milijunima korisnika preko Interneta. Decentralizirana koncepcija čuvanja i dijeljenja takvoga sadržaja, jedan je od glavnih problema u sprječavanju takvih kaznenih djela. Iako je moguće pronaći korisnike koji skidaju takav sadržaj sa Interneta pomoću njihove IP adrese, sve je popularniji

koncept korištenja *virtual private network* (VPN) konekcija koje daju anonimnost takvim korisnicima, te na taj način dodatno otežava i onemogućuje istrage o takvim kaznenim djelima. Iako se pokušavaju implementirati svakojaka tehnološka rješenja koja onemogućavaju kopiranje i neovlašteno umnažanje, poput npr. *content scrambling systems* (CSS) tehnologije na DVD-ima, skoro svaka takva zaštita je probijena i pomoću određenih programskih rješenja može se zaobići.

Poseban oblik kaznenog djela povezanog sa autorskim pravima, je onaj koji se odnosi na prevare vezane uz globalne trgovinske marke. Često se na Internetu pojavljuje sadržaj koji se referencira na pojedine trgovinske marke na način da zbunjuje korisnike i navodi ih na pogrešne zaključke, te se na taj način reklamira nešto drugo od interesa počinitelja kaznenog djela. Također, česta je pojava i da se registriraju domene na Internetu koje su iste ili slične određenim trgovinskim markama, i zatim se pokušaju prodati toj marki za velik novac, ili prodaju sami neke proizvode krivo navodeći kupce [1].

2.3.4 Kaznena djela povezana sa računalom

Kaznena djela povezana sa upotrebom računala su jedna od najčešćih i najbrojnijih kaznenih djela. U tu kategoriju ulaze prijevare pomoću računala, krivotvorenje sadržaja, krađa identiteta, kao i zlouporaba uređaja.

Prijevare pomoću računala danas su jako popularne, jer se pomoću programskih alata za automatizaciju i sakrivanje identiteta, omogućuju masovni napadi na način da žrtve takvih napada pretrpe nizak financijski gubitak i da im se ne isplati prijavljivati i progoniti takve napadače, dok istovremeno masovnost takvih napada osigurava veliki profit tom istom napadaču. Vrlo česta je i npr. prijevara pomoću aukcijskih platformi kao što je eBay, koje su danas izuzetno popularne. Prijevara se uglavnom sastoji od traženja plaćanja unaprijed za robu koja ne postoji, ili traženja isporuke robe a sa namjerom da se za nju ne plati. Toj vrsti prijevara pokušava se doskočiti sistemom recenzija pojedinih ponuđača na tim platformama, kako bi sudionici prijašnjih transakcija dali potreban kredibilitet određenom ponuđaču.

Krivotvorenje pomoću računala, odnosi se većinom na nedozvoljenu manipulaciju digitalnim sadržajem, poput slika, dokumenata i sl. Primjer toga su npr. dokumenti koji su dokaz na sudu u nekom procesu, a koji mogu biti krivotvoreni ili njihov sadržaj promijenjen.

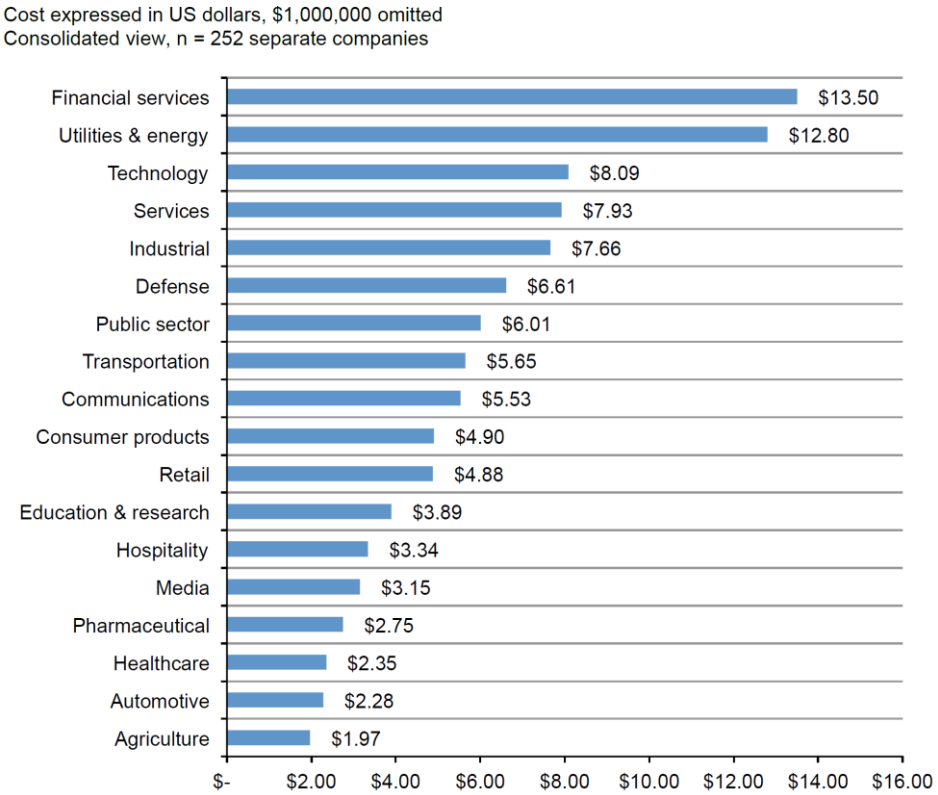
Kriv otvorenje *e-mail* adrese je najčešći oblik *phishing*-a, kojim se pokušava doći do osjetljivih podataka žrtve i pomoću njih onda ostvariti druga kaznena djela. Krivotvorene *e-mail* adrese obično izgledaju kao da su poslane od strane legalnih najčešće financijskih institucija, a u njima se traže određene akcije koje mogu oštetiti potencijalne žrtve takvih korisnika, kojima je jako teško razlučiti da je u pitanju krivotvorina. Takvi napadi, iz dana u dan sve su profinjeniji, i sve ih je teže identificirati kao krivotvorinu na vrijeme.

Krađa identiteta je vrlo široko područje, i obično se događa u tri faze. U prvoj fazi, napadač dolazi do informacija vezanih uz identitet neke osobe, npr. pomoću zlonamjernih programa ili pomoću *phishing*-a. Druga faza podrazumijeva neku interakciju vezanu uz nezakonito stečene osobne podatke, npr. prodaju tih podataka zainteresiranoj strani. I treća faza, naravno, podrazumijeva korištenje tih osobnih podataka za daljnje počinjenje kriminalnih djela.

Zlouporaba uređaja danas je omogućena velikim brojem programskih alata stvorenih upravo za tu namjenu. Automatizacija doprinosi masovnosti napada, simplifikacija samog procesa napada korištenjem specijaliziranih alata doprinosi povećanju broja prekršitelja, jer to više ne mora biti vrlo vješta osoba, nego i prosječan korisnik računala. Različitim pravnim okvirima pokušava se progoniti proizvođače takvih programskih alata, kao i posjedovanje ili prodaju istih [1].

2.4 Trendovi u kibernetičkom kriminalu

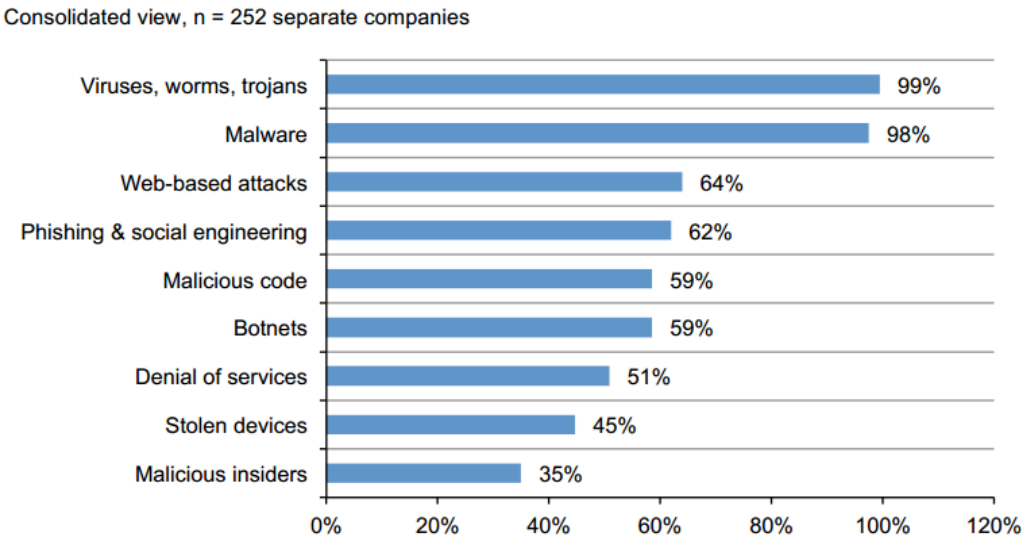
Statistika u nastavku pokazuje generalno stanje sigurnosti na svjetskoj razini i trendove u kibernetičkom kriminalu. Analizirati će se rezultati istraživanja Ponemon Institute-a financiranog od strane Hewlett Packard-a na 252 reprezentativne organizacije unutar sedam zemalja [4].



Slika 1. Prosječni godišnji trošak kibernetičkog kriminala po industrijama [4]

Iz Slike 1., jasno je vidljivo i očekivano da najviše štete u financijskom smislu trpe dva sektora u kojima su involvirana velika kapitalna sredstva, dakle energetski sektor koji je poslije financijskog sektora najteže pogođen ovom vrstom kriminala. Ne mnogo iza njih po pretrpljenim štetama, nalaze se tvrtke u tehnološkom, industrijskom i uslužnom sektoru.

Najzastupljenije vrste napada su virusi, crvi, *malware*-i i *trojan*-i, od kojih napada se ujedno i najjednostavnije obraniti, odnosno tehničkim kontrolama te adekvatnim operativnim djelovanjima taj rizik se može uvelike umanjiti. Iako zastupljeni sa manjim postotkom u ukupnom broju napada, napadi u smislu blokiranja usluge, unutrašnjih napadača, napada na *web* i sl. mogu izazvati golemu štetu napadnutim kompanijama, a ujedno je i teže i skuplje obraniti se od takve vrste napada. Navedeno je vidljivo iz Slike 2. u nastavku.



Slika 2. Udio napada prema vrsti [4]

Neke procjene govore da će šteta od kibernetičkog kriminala doseći 6 bilijuna USD do 2021. godine. Budući da se vrste kibernetičkih napada neprestano mjenjaju, evoluiraju zajedno sa tehnologijom i postaju sve teže prepoznatljive, potrebno je razumjeti koje zaštitne mjere su učinkovite i koja vrsta edukacije je potrebna u tu svrhu. European Network and Information Security Agency (ENISA) Threat Landscape Report 2018 pokazuje da je najčešća vrsta napada na organizacije još uvijek krađa ili gubitak informacija, sa 137,5 milijuna novih tipova zlonamjernog *software*-a u 2018. godini, od kojih je 93% polimorfnog tipa, što znači da stalno mjenja kod kako bi onemogućio ili otežao otkrivanje ili sprječavanje istog. Prema Imperva Cyberthreat Defence Report 2019, oko 78% anketiranih organizacija u 2018. godini bilo je pogođeno uspješnim kibernetičkim napadom. Zanimljiv je i podatak da u Ujedinjenom kraljevstvu (UK) 50% ukupnog broja kriminalnih djela otpada na kibernetički kriminal. Istraživanja Maryland univerziteta pokazuju da se danas kibernetički napad događa svakih 39 sekundi [5].

Globalna statistika pokazuje eksponencijalan rast kibernetičko kriminalnih aktivnosti, što u borbi protiv te vrste kriminala stvara veliki pritisak na povećanje resursa koji se bave digitalnom forenzikom i surađuju sa tijelima kaznenog progona, te konstantnu edukaciju i povećanje zaštitnih mjera digitalnih sustava – u organizacijama ali i privatnih računala i pametnih uređaja, kao i na intenzivnu međunarodnu suradnju u preveniranju ove vrste kriminala.

3. Međunarodni odgovor na kibernetički kriminal

Analiza globalne situacije u borbi protiv kibernetičkog kriminala pokazuje sporost implementacije zakonskih mehanizama u nacionalne pravne sustave, a nasuprot brzorastućem trendu kriminalnog ponašanja povezanog sa kibernetičkim kriminalom.

Identificirane su brojne prepreke koje neposredno utiču na neodgovarajući odgovor na sigurnosne prijetnje te vrste. Najveće od njih su nedostatak globalne konvencije i globalnog pravnog okvira, kao i određivanje granice između efikasnog nadzora u svrhu prevencije od kibernetičkog kriminala, i narušavanja osobnih prava fizičkih i pravnih osoba, te zakona o zaštiti osobnih podataka.

Međunarodna suradnja na polju kibernetičke prijetnje nužno se javlja u vidu specijaliziranih organizacija, često regionalnog ili višenacionalnog karaktera, kao i globalnih organizacija.

3.1 Međunarodne inicijative u borbi protiv kibernetičkog kriminala

U svom radnom dokumentu, Tajništvo Ureda UN-a za droge i kriminal (UNODC) primjećuje da zbog transnacionalne prirode kibernetičkog kriminala pitanja nacionalnog suvereniteta mogu ometati kaznene istrage u nedostatku aktivne suradnje između tijela za provedbu zakona nadležnih sudbenih tijela. Brzina kojom kibernetički kriminalci mogu nanijeti štetu i krenuti na izbjegavanje otkrivanja također dovode do agresivnih agencija pod velikim vremenskim pritiscima, što sve više zahtijeva potrebu međunarodne suradnje. UNODC identificira zakonodavnu konvergenciju kao ključnu za učinkovitu suradnju. Divergencija u zakonodavstvu može potkopati učinkovitu provedbu. Države gdje određena jurisdikcija nedostaje ili se sveobuhvatno zakonodavstvo o kibernetičkom kriminalu slabo provodi, najčešća su sigurna utočišta za računalne kriminalce. Ovakvu vrstu razilaženja može se riješiti samo usuglašenim naporima za usklađivanje pravnih standarda i unaprjeđivanjem suradnje između jurisdikcija [3], [6], [7].

3.1.1 Međunarodna kriminalističko-policijska organizacija

International Criminal Police Organization (INTERPOL) je međunarodna kriminalističko-policijska organizacija koja obuhvaća najveći broj država, njih 184. Njihova uloga u sprječavanju kibernetičkog kriminala svodi se na koordinaciju

nacionalnih institucija kaznenog progona, kao i usklađivanje pravnih okvira pojedinih država, a u svrhu povećanja resursa i efikasnije borbe protiv ove vrste kriminala. Interpol također daj smjernice za daljnje unaprjeđivanje nacionalnih pravosudnih sustava, te služi i kao centralizirana baza podataka za tu vrstu kriminaliteta.

3.1.2 Azijsko pacifička ekonomska suradnja

U Azijskoj regiji, organizacija Azijsko pacifička ekonomska suradnja (APEC) je organizacija koja je okupila 21 članicu sa ciljem rješavanja problema vezanih uz računalni kriminalitet. Šesti sastanak APEC-ovih čelnika urodio je donošenjem Deklaracije kojom se upućuje telekomunikacijsku i informacijsku industriju na proučavanje i primjenu smjernica iz EU Konvencije o kibernetičkom kriminalu, te na usklađivanje postojećih pravnih okvira vezano uz računalni kriminalitet.

3.1.3 Commonwealth

Tajništvo Commonwealth-a (zajednice država koje su nekada tvorile Britansko Carstvo), svojim 53-ima članicama predstavilo je Model zakona o računalnom i informatičkom kriminalitetu. To se dogodilo u listopadu 2002. godine, i kao osnova također je uzeta EU Konvencija o kibernetičkom kriminalu. Iako se države članice ohrabruju i usmjeravaju prema tome da potpišu i ratificiraju Konvenciju o kibernetičkom kriminalu, mnoge od njih nisu još uvijek prilagodile svoj pravni okvir računalnom kriminalitetu, ili se razlikuje od onoga koji prakticiraju članice EU Konvencije o kibernetičkom kriminalu.

3.1.4 Ujedinjeni narodi

Na globalnoj međunarodnoj sceni, Ujedinjeni narodi (UN) su vodeća organizacija koja potiče i inicira rasprave i rješavanje problema ove vrste kriminala na globalnom nivou. UN je donio brojne rezolucije, u kojima se sugerira osnivanje specijaliziranih skupina stručnjaka za dublje analize vezane uz mogućnosti zlouporabe računalne tehnologije. Također, daju se preporuke za borbu protiv računalnog kriminaliteta u vidu sinkronizacije pravnih okvira, sa ciljem uklanjanja sigurnih utočišta za takve kriminalce, kao i što boljeg osiguranja integriteta podataka i kaznenog progona ako dođe do ugroze istog.

Osim navedenih organizacija, svoj doprinos daju i organizacije poput Organizacije američkih država, Europske Unije i Skupine G8.

Konvencija o kibernetičkom kriminalu Vijeća Europe postala je centralna smjernica u sinkronizaciji međunarodnog i nacionalnog pravnog okvira, koju prihvaća sve veći broj država.

3.2 Odgovor EU i Vijeća Europe na kibernetičke prijetnje

Obzirom na međunarodnu otvorenost interneta, kibernetički kriminal je u značajnoj mjeri transnacionalni fenomen. Učinitelj i žrtva često će se nalaziti u različitim jurisdikcijama, što predstavlja akutne poteškoće agencijama za provođenje zakona u istrazi i procesuiranju zločina te vrste. Unatoč jasnoj potrebi za međunarodnom suradnjom na području kibernetičkog kriminala, još uvijek nema istinski globalnog multilateralnog ugovora (konvencije) koji se bavi tim pitanjem [3], [6], [7].

Trenutno je vodeća međunarodna konvencija o kibernetičkom kriminalu Konvencija Vijeća Europe o kibernetičkom kriminalu, koja je potpisana u Budimpešti 2001., a stupila je na snagu 2004. godine. U prosincu 2009. godine, Konvenciju o kibernetičkom kriminalu potpisalo je četrdeset i šest država, a ratificiralo ih je dvadeset i šest (tj. odobrilo u skladu s domaćim ustavnim zahtjevima). Konvencija je podijeljena u tri osnovna pilara: prvi pilar definira vrste kaznenih djela, drugi pilar se bavi odredbama koje su države obvezne implementirati u svoj pravni okvir, i treći pilar koji se bavi mehanizmima međunarodne suradnje. Ova Konvencija dopunjena je Dodatnim protokolom o kaznenim djelima rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava. Dodatni protokol otvoren je za potpis 2003. godine kada ga je potpisala i Republika Hrvatska, a stupio je na snagu u ožujku 2006. godine [3], [6].

Iako je Konvencija o kibernetičkom kriminalu izrađena u okviru Vijeća Europe, ona je otvorena za sudjelovanje nečlanova. Četvero nečlanica sudjelovalo je u pregovorima o sporazumu i potpisalo ga (Sjedinjene Države, Kanada, Japan i Južna Afrika), a jedan nečlan ga je ratificirao (Sjedinjene Države). Konvencija, dakle, nije strogo regionalni sporazum. Ipak, činjenica da ga je ratificirala samo jedna neeuropska država upućuje na to da se trenutna situacija ne može opisati kao globalna konvencija. Navedena Konvencija navodi niz zločina koje potpisnici trebaju klasificirati u domaćem zakonu, uključujući hakiranje, kaznena djela protiv dječje pornografije i određena kaznena djela povezana s kršenjem intelektualnog vlasništva. Također se navodi niz

postupovnih mehanizama koje potpisnici moraju uspostaviti, uključujući dodjeljivanje ovlasti tijelima nadležnim za provođenje zakona u svrhu prisile pružatelja telekom usluga da prate aktivnosti osoba na mreži [6].

Konvencija Vijeća Europe o kibernetičkom kriminalu ima najširu pokrivenost u usporedbi sa bilo kojim međunarodnim sporazumom koji se bavi kibernetičkim kriminalom (procjenjuje se da pokriva jednu trećinu korisnika Interneta). Kao što smo vidjeli, potpis je otvoren zemljama koje nisu članice Vijeća Europe, a već su ga potpisale i četiri ne-europske zemlje. Glavna pitanja su može li postojeća Konvencija o kibernetičkom kriminalu pružiti globalni standard, i ako je tako, treba li se svaka sljedeća konferencija usredotočiti na stvaranje zamaha za širi potpis i ratifikaciju postojeće Konvencije Vijeća Europe.

Primjećuje se da Konvencija o kibernetičkom kriminalu pruža jasno i sveobuhvatno rješenje i dobiva snažnu potporu ekonomske suradnje Azije i Pacifika, Europske unije , Interpola i Organizacija američkih država. Jedan od nedostataka pokretanja pregovora o novoj, globalnoj konvenciji je da bi to moglo imati učinak obustavljanja provedbe zakonodavne reforme koja je već u tijeku na nacionalnim nivoima [6], [7].

Međunarodna telekomunikacijska unija (ITU), specijalizirana agencija UN-a, smatra se kritičnim faktorom za usvajanje prijedloga Konvencije o kibernetičkom kriminalu kao globalnog standarda. Konvencija je uglavnom izradila smjernice za europske države, a sada je i donekle zastarjela. Rusija, koja je članica Vijeća Europe, ali nije potpisala Konvenciju, navodno podupire stavove ITU-a. Brazil je razmatrao potpisivanje Konvencije, no odbio je to učiniti, izražavajući svoje rezerve oko određenih aspekata Konvencije, uključujući odredbe koje se odnose na kriminalizaciju kršenja intelektualnog vlasništva.

Ove rezerve o Konvenciji o kibernetičkom kriminalu sugeriraju da bi pregovori o novoj Konvenciji u UN-u mogli biti teški: globalno, jasno se razlikuju stavovi glede odgovarajućih globalnih standarda. Nadalje, obveze postupanja i suradnje na temelju Konvencije mogu biti teške posmatrajući svjetsku razinu. Pitanja koje ove obveze mogu globalno potaknuti su ilustrirane domaćim kritikama usmjerenim na vladu Sjedinjenih Država kada je usvojila Konvenciju. Na primjer, navodilo se da bi Konvencija mogla imati učinak da Sjedinjene Države zahtijevaju provođenje stranih zakona koji ograničavaju slobodu govora ili prate komunikacije političkih disidenata u ime stranih vlada. Od ključnih sudionika poput Ruske Federacije ili Narodne Republike

Kine, za koje se sumnja da sponzoriraju razne oblike kibernetičkih napada u političke svrhe, teško je očekivati da će se složiti s visokim standardima međunarodne suradnje u istragama i kaznenim postupcima u borbi protiv kibernetičkog kriminala. UN ima dugu povijest podjele između razvijenih i zemalja u razvoju, a brazilske rezerve u vezi s prekršajem intelektualnog vlasništva ukazuju na to da bi ove podjele mogle i dalje imati veliku i presudnu ulog u pregovorima o kibernetičkom kriminalu [7].

Kibernetički kriminal ne samo da utječe na razvijena gospodarstva: sada ima više korisnika Interneta u zemljama u razvoju nego u razvijenim zemljama, a jedna studija sugerira da gospodarstva u nastajanju mogu biti posebno izložena riziku od kibernetičkog kriminala. Jasno je da će učinkovito suzbijanje kibernetičkog kriminala zahtijevati globalnu suradnju, koja uključuje mnogo širu skupinu zemalja od trenutnih potpisnika Konvencije Vijeća Europe o kibernetičkom kriminalu. S obzirom da se postojeća Konvencija pokazala razumno učinkovita i da su potpisnici stekli vrijedno iskustvo u provedbi, čini se da je ne bi trebalo ignorirati. Ipak, nastojanje da Konvencija Vijeća Europe postane globalni standard u svom sadašnjem obliku vjerojatno neće biti lako provedivo [3], [6], [7].

4. Kaznenopravni okvir RH obzirom na kibernetičke prijetnje

U pravni sustav Republike Hrvatske, pogotovo u sklopu usklađenja sa direktivama i odredbama EU, implementiran je niz zakona i temeljnih akata koji se bave informacijskom sigurnošću i zaštitom osobnih podataka u svrhu prevencije od kibernetičkog kriminala. Potpora tim zakonskim okvirima pruža se kroz niz institucija nadležnih za upravljanje informacijskom sigurnošću, suradnju na nacionalnom nivou sa drugim tijelima i institucijama, kao i suradnju na međunarodnom planu.

4.1 Povezanost sa Konvencijom Vijeća Europe

Republika Hrvatska potpisnik je Konvencije Vijeća Europe o kibernetičkom kriminalu, te je u srpnju 2002. godine donesen Zakon o potvrđivanju Konvencije Vijeća Europe o kibernetičkom kriminalu.

Također, Republika Hrvatska 26. ožujka 2003. potpisuje i Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava. Slijedom preuzetih obveza iz Konvencije i Dodatnog protokola, izmjene Kaznenog zakona implementirane su već 2004., kada Konvencija stupa na snagu, iako Dodatni protokol stupa na snagu tek 2008.

Daljnje usklađivanje hrvatskog zakonodavstva sa Europskom unijom nastavlja se izmjenama i dopunama Kaznenog zakona u 2015. godini, sukladno Direktivi 2013/40/EU Europskog parlamenta i Vijeća Europe o napadima na informacijske sustave, iz 2013. godine. Iste godine, u zakonodavstvo implementirana je i Direktiva 2011/93/EU Europskog parlamenta i Vijeća Europe o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije.

4.2 Nacionalna strategija kibernetičke sigurnosti

Nacionalna strategija kibernetičke sigurnosti [8] donesena je 7. listopada 2015. godine, a nastala je kao nužan produkt sudjelovanja u međunarodnoj zajednici u borbi protiv kibernetičkih prijetnji i prepoznavanja važnosti sigurnosti kibernetičkog prostora kao zajedničke odgovornosti svih segmenata društva. Pojam "kibernetički" uveden je u pravni poredak Republike Hrvatske ratifikacijom Budimpeštanske konvencije o kibernetičkom kriminalu 2002. godine. Svrha strategije je sustavno i koordinirano provođenje aktivnosti potrebnih za podizanje sposobnosti Republike Hrvatske u

području kibernetičke sigurnosti, odnosno provedba zakonskih i pravnih okvira i poštivanje temeljnih ljudskih prava u sklopu te borbe.

U svrhu borbe protiv kibernetičkog kriminala, a temeljeno na Nacionalnoj strategiji kibernetičke sigurnosti, vlada RH utemeljila je u lipnju 2016. dvije nove institucije – Nacionalno vijeće za kibernetičku sigurnost i Operativno-tehničku koordinaciju za kibernetičku sigurnost. Jedan od ciljeva ove strategije je i podizanje svijesti o kibernetičkom prostoru, pa je u sklopu akcijskog plana sa osam provedbenih mjera, jedna od glavnih mjera informiranje javnosti u slučaju računalnih incidenata koji mogu zahvatiti veliki broj korisnika [8], [9].

Nacionalna strategija kibernetičke sigurnosti, sukladno strateškim ciljevima Europske unije, ima slijedeće prioritete [8] :

- sustavni pristup u razvoju kaznenopravnog okvira
- provođenje aktivnosti i mjera za jačanje sigurnosti kibernetičkog prostora
- uspostava sigurnih mehanizama za razmjenu podataka
- jačanje javne svijesti o kibernetičkom prostoru
- obrazovni programi
- razvoj e-usluga
- poticanje istraživanja i razvoja
- međunarodna suradnja

Upravo na području međunarodne suradnje, Republika Hrvatska sudjeluje u radu Europske multidisciplinarne platforme za borbu protiv kaznenih djela (EMPACT), kao i u drugim aktivnostima sukladno članku 13. Direktive 2013/40/EU o napadima na informacijske sustave.

Neke od aktivnosti na međunarodnom planu u kojima Republika Hrvatska aktivno sudjeluje su [8], [9]:

- razvoj mehanizama za onesposobljavanje glavnih distributera zlonamjernog softvera
- prikupljanje informacija o zlonamjernom softveru koje bankarski sektor šalje Europskom centru za kibernetički kriminal (EC3 - European Cybercrime Centre) te prosljeđivanje EMAS-u (sustavu za analizu zlonamjernog softvera) EUROPOL-a (Europski policijski ured)
- razvoj metoda za sprječavanje pranja novca i povrata imovine

- razmjena najboljih praksi i iskustava

Strategija također definira pet područja kibernetičke sigurnosti, koji su strateški najvažniji za Republiku Hrvatsku [8], [10]:

- javne elektroničke komunikacije
- elektronička uprava
- elektroničke financijske usluge
- kritična komunikacijska i informacijska infrastruktura i upravljanje krizama
- kibernetički kriminalitet

Ujedno, Strategija definira i četiri poveznice kibernetičke sigurnosti koje su opisane rezultatima koje se želi postići [8], [10]:

- zaštita podataka
- tehnička koordinacija u obradi računalnih sigurnosnih incidenata
- međunarodna suradnja
- obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru

Na Slici 3. prikazani su elementi kibernetičke sigurnosti na kojima je naglasak u Nacionalnoj strategiji kibernetičke sigurnosti, kao i u radu Nacionalnog vijeća kibernetičke sigurnosti.

Implementacija mjera i standarda informacijske sigurnosti u različitim sektorima društva, nadzor provedbe istih, kao i definirana kritična komunikacijska i informacijska infrastruktura koja omogućuje neometan rad svim tim sektorima društva, osnovni su elementi kibernetičke sigurnosti. Usko vezana uz sigurnost kritičke infrastrukture, je i sigurnost zakonom zaštićenih podataka (klasificirani, osobni podaci, autorski sadržaj) [10].

Slika 3. Glavni elementi Nacionalne strategije kibernetičke sigurnosti [10]

4.3 Zakonski okvir Republike Hrvatske vezan uz informacijsku sigurnost

Neki od važnijih zakona povezanih sa informacijskom sigurnošću su navedeni u nastavku:

Zakon o informacijskoj sigurnosti (ZOIS) [11], definira terminologiju i područja informacijske sigurnosti, kao i standarde i nadležna tijela informacijske sigurnosti. Primjenjuje se na državna tijela lokalne i regionalne samouprave i pravna tijela sa javnim ovlastima koja koriste klasificirane i neklasificirane podatke.

Zakon o tajnosti podataka (ZOTP) [12], definira klasificirane i neklasificirane podatke, stupnjeve tajnosti, pristup zaštitu i nadzor istih.

Zakon o zaštiti osobnih podataka (ZOZOP) [13], uređivao je zaštitu osobnih podataka o fizičkim osobama i nadzor nad prikupljanjem, obradom i korištenjem istih u Republici Hrvatskoj, a koja je osigurana svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište. Navedeni zakon prestao je važiti , a 25.05.2018. stupio je na snagu Zakon o provedbi Opće uredbe o zaštiti podataka [14], o kojem će biti napisano više kasnije u tekstu.

Zakon o pravu na pristup informacijama (ZOPPI) [15], treba omogućiti i osigurati Ustavom Republike Hrvatske zajamčena prava na pristup informacijama fizičkim i pravnim osobama putem otvorenosti i javnosti djelovanja tijela javne vlasti.

Naravno, postoji još niz povezanih zakona kao npr. skupina zakona o intelektualnom vlasništvu i slično, no njima se nećemo posebno baviti unutar ovog rada.

4.4 Institucije nadležne za kibernetički kriminal u RH

Kaznenopravni progon počinitelja kaznenih djela, pa tako i djela kibernetičkog kriminala, obavlja Državno odvjetništvo RH, petnaest županijskih državnih odvjetništava, dvadeset dva općinska državna odvjetništva kao i Ured za suzbijanje korupcije i organiziranog kriminala. Obzirom da je broj kibernetičkih kaznenih djela u Republici Hrvatskoj relativno mali, u Hrvatskoj ne postoji državno odvjetništvo koje je specijalizirano isključivo za kibernetički kriminal [9].

Tijelo progona koje koristi Državno odvjetništvo organizirano je na nacionalnoj razini kroz Upravu kriminalističke policije, a 2008.-me u sklopu te uprave nastao je odjel Policijski nacionalni ured za suzbijanje korupcije i organiziranog kriminala (PNUSKOK). U sklopu PNUSKOK-a postoji Odjel za visokotehnološki kriminalitet čiji je zadatak borba protiv kibernetičkog kriminala [9].

Važan čimbenik u istražnim procesima je Centar za forenzična ispitivanja, istraživanja i vještačenja "Ivan Vučetić", koji zapošljava i dva digitalna forenzičara.

Nekoliko je osnovnih institucija nadležnih za upravljanje informacijskom sigurnošću u Republici Hrvatskoj [9]:

Nacionalni CERT (CERT – Computer Emergency Response Team) je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj. CARNet CERT je bio jedini CERT u Republici Hrvatskoj u periodu 1996. – 2008. godine, nakon čega CARNet osniva Odjel za Nacionalni CERT prema obvezama koje proizlaze iz ZoIS-a. Ustrojstvom Nacionalnog CERT-a započinje uspostava hijerarhijski ustrojene infrastrukture CERT timova nužnih za preventivno djelovanje i učinkovitu koordinaciju pri rješavanju sigurnosnih incidenata.

Zavod za sigurnost informacijskih sustava (ZSIS) je središnje državno tijelo zaduženo za poslove tehničkog područja informacijske sigurnosti državnih tijela pomoću standarda sigurnosti i sigurnosnih akreditacija IK sustava. Nadalje, bavi se upravljanjem kriptomaterijalima pri razmjeni klasificiranih podataka i koordinacijom prevencije i reakcija na ugroze sigurnosti IK sustava. ZSIS također obnaša ulogu NDA

(National Distribution Authority) i SAA (Security Acreditation Authority) u Republici Hrvatskoj. ZSIS, ako je potrebno, svojim stručnim znanjem pomaže tijelima kaznenog progona u istragama.

Ured vijeća za nacionalnu sigurnost (UVNS) je središnje državno tijelo za informacijsku sigurnost koje je ujedno i Hrvatski NSA (National Security Authority), a bavi se koordinacijom, usklađivanjem, donošenjem i nadziranjem primjene mjera i standarda informacijske sigurnosti u okviru slijedećih područja : sigurnosne provjere, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacijsko-komunikacijskog sustava, sigurnost poslovne suradnje u privatnom sektoru itd.

Agencija za zaštitu osobnih podataka (AZOP) je osnovana temeljem Zakona o provedbi Opće uredbe o zaštiti podataka, a obavlja upravne i stručne poslove u svezi sa zaštitom osobnih podataka, nadzire i ukazuje na zlouporabu u prikupljanju i obradi osobnih podataka. Također, AZOP sastavlja listu država i međunarodnih organizacija koje imaju odgovarajuće uređenu zaštitu osobnih podataka, rješava povrede prava zajamčenih Zakonom o provedbi Opće uredbe o zaštiti podataka, te vodi središnji registar zbirki osobnih podataka.

Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM) je neovisna, neprofitna pravna osoba sa javnim ovlastima u području Zakona o elektroničkim komunikacijama [16], Zakona o poštanskim uslugama [17] i Zakona o željeznici [18]. Svrha HAKOM-a je između ostaloga i regulacija tržišta elektroničkih komunikacija, učinkovito raspolaganje resursima, zaštita korisnika i njihovo informiranje te općenito razvoj, inovacije i ulaganja u tom području.

U slučaju kibernetičkog napada širih razmjera, ili napada na vitalne sustave Republike Hrvatske, reakcija bi bila uzajamna suradnja više entiteta, npr. Nacionalnog CERT-a, tijela kaznenog progona, kao i pružatelja telekom usluga. Davatelji telekom usluga imaju direktnu odgovornost za rad i zaštitu ključnih infrastruktura u ovakvim slučajevima. Nacionalnom strategijom kibernetičke sigurnosti i akcijskim planom za provedbu te Strategije predviđene su aktivnosti koje imaju za cilj prepoznavanje ključnih informacijsko-komunikacijskih sustava i infrastrukture, te uspostave minimalnih standarda sigurnosti za iste, kao i implementaciju tih mjera od strane davatelja telekom usluga [9], [10].

Za praćenje provedbe Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana, zaduženo je međuresorno tijelo - Nacionalno vijeće za kibernetičku sigurnost, koje čine predstavnici 18 institucija [10]:

- Ured Vijeća za nacionalnu sigurnost (predsjednik),
- Ministarstvo unutarnjih poslova (član),
- Ministarstvo vanjskih i europskih poslova (član),
- Ministarstvo uprave (član),
- Ministarstvo gospodarstva, poduzetništva i obrta (član),
- Ministarstvo znanosti i obrazovanja (član),
- Ministarstvo obrane (član),
- Ministarstvo pravosuđa (član),
- Ministarstvo mora, prometa i infrastrukture (član),
- Središnji državni ured za razvoj digitalnog društva (član),
- Sigurnosno-obavještajna agencija (član),
- Zavod za sigurnost informacijskih sustava (član),
- Operativno-tehnički centar za nadzor telekomunikacija (član),
- Državna uprava za zaštitu i spašavanje (član),
- Hrvatska akademska i istraživačka mreža – CARNET, Nacionalni CERT (član),
- Hrvatska regulatorna agencija za mrežne djelatnosti (član),
- Hrvatska narodna banka (član),
- Agencija za zaštitu osobnih podataka (član).

Nacionalno vijeće za kibernetičku sigurnost je ujedno i nositelj tri mjere Akcijskog plana vezano za postupke u kriznim situacijama izazvanim kibernetičkim napadima.

Operativno-tehnička koordinacija za kibernetičku sigurnost je tijelo osnovano radi osiguravanja operativne podrške radu Nacionalnog vijeća za kibernetičku sigurnost. Operativno-tehnička koordinacija za kibernetičku sigurnost ima osam članova [10]:

- Ministarstvo unutarnjih poslova (koordinator),
- Ministarstvo obrane (član),
- Sigurnosno-obavještajna agencija (član),
- Zavod za sigurnost informacijskih sustava (član),
- Operativno-tehnički centar za nadzor telekomunikacija (član),
- Hrvatska akademska i istraživačka mreža – CARNET, Nacionalni CERT (član),
- Hrvatska regulatorna agencija za mrežne djelatnosti (član),

- Hrvatska narodna banka (član).

4.5 Suradnja na međunarodnom planu

Na međunarodnom planu, Republika Hrvatska kao članica Europske unije od 2013. godine, teži usklađenju svojeg pravnog okvira sa odlukama, direktivama i preporukama Europskog parlamenta i Vijeća Europe, pa je tako i na području međunarodne suradnje najaktivnija upravo sa europskim institucijama, raznim regulatornim tijelima i tijelima kaznenog progona. Do sada postoje formalni zahtjevi suradnje sa EUROPOL-om, odnosno Europskim centrom za kibernetički kriminal EC3, EUROJUST-om (Ured Europske unije za pravosudnu suradnju) te ENISA-om (European Network and Information Security Agency).

Iako ne postoje posebni zakoni koji reguliraju ili stvaraju obavezu suradnje, Odluka Vijeća Europe 2009/371/PUP iz travnja 2009. o osnivanju Europskog policijskog ureda (EUROPOL) dala je pravni temelj za suradnju Republike Hrvatske sa tim uredom. Iako je inicijalno potpisan Sporazum o operativnoj i strateškoj suradnji Republike Hrvatske i EUROPOL-a još 2006., on je bio na snazi samo do ostvarivanja punopravnog članstva Republike Hrvatske Europskoj uniji 2013. EUROPOL se preferira kao glavni kanal za komunikaciju, osim kad su u pitanju treće strane, ne-članice Europske unije, kada je preferirani kanal INTERPOL (International Criminal Police Organization) [19].

INTERPOL povezuje 194 zemlje članice u borbi protiv terorizma, organiziranog kriminala i kibernetičkog kriminala. Svaka država članica surađuje sa INTERPOL-om ovisno o svom nacionalnom pravnom okviru. Republika Hrvatska u većini slučajeva traži podatke o kibernetičkim napadima, potrebne za provođenje istraga.

Jedan od vidova suradnje je npr. da nacionalna policija može pristupiti podacima koji su prikupljeni u INTERPOL-u, EUROPOL-u ili u drugim međunarodnim organizacijama.

Vezano uz prikupljanje klasificiranih podataka, prema Zakonu o tajnosti podataka, ZSIS nije dužan dijeliti informacije koje su klasificirane, osim ako postoji potpisan takav sporazum o sigurnosti između dviju zemalja koji dopušta dijeljenje takvih informacija. ZSIS će svakako podijeliti sve neklasificirane podatke o kibernetičkim napadima, ako to može pomoći u internacionalnim istragama.

Odnosi Republike Hrvatske sa ENISA-om (European Union Agency for Cybersecurity) su konzultativne prirode, te nema operativnog vida suradnje. Republika Hrvatska je do sada sudjelovala u rješavanju nekoliko incidenata sa EUROPOL-om, ENISA-om i CERT-ovima drugih država članica. Najveći slučaj je bila kampanja ZeuS kada je u proljeće 2014. zaražen veliki broj računala u Hrvatskoj. Hrvatska je predala sve svoje podatke EUROPOL-u i CERT-ovima drugih država članica [19].

EUROJUST je tijelo Europske unije osnovano radi ostvarivanja učinkovite pravosudne suradnje u kaznenim slučajevima između država članica Europske unije. Pristupanjem Republike Hrvatske Europskoj uniji 2013. godine, između ostaloga trebalo je implementirati Odluku Vijeća Europe o suradnji sa EUROJUST-om, što je u konačnici ugrađeno u Zakon o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije [20].

4.6 Statistički trendovi vezani uz kibernetički kriminal u RH

Broj kaznenih dijela povezanih sa računalnim ili kibernetičkim kriminalom u Europskoj uniji kao i u Republici Hrvatskoj, u stalnom je porastu. Najveći rast zamijećen je u obliku računalnih prijevara. Danas, u europskim državama broj kaznenih dijela vezanih uz kibernetički kriminal prelazi 20% ukupnih kaznenih dijela svih vrsta, a obzirom na spomenuti konstantni porast, kibernetički kriminal postati će jedan od najzastupljenijih kriminalnih radnji. Uska je povezanost kibernetičkog kriminala sa razvojem tehnologije, prodiranjem tih tehnologija u sve aspekte ljudskog djelovanja, kao i rastom e-ekonomije. Obzirom na nadolazeće razdoblje 4. industrijske revolucije, uz sve benefite novih tehnologija, borba protiv kibernetičkog kriminala postati će jedan od glavnih prioriteta globalno, kao i na nacionalnim nivoima.

Nacionalni CERT Republike Hrvatske (Computer Emergency Response Team) je odjel Hrvatske akademske i istraživačke mreže (CARNET). Njegovo područje djelovanja odnosi se na incidente na internetu, odnosno očuvanje informacijske sigurnosti ako se jedna od strana koje sudjeluju u incidentu nalazi u hrvatskom IP adresnom prostoru ili ima *.hr* domenu. Ako je jedna od tih strana tijelo državne uprave Republike Hrvatske, tada je za takve incidente nadležan CERT Zavoda za sigurnost informacijskih sustava (ZSIS).

4.6.1 Proaktivne mjere Nacionalnog CERT-a

U sklopu svojih redovitih aktivnosti, Nacionalni CERT provodi neke proaktivne mjere poput [21], [22]:

- svakodnevno izdavanje sigurnosnih preporuka za najpopularnije operativne sustave
- izdavanje i objavljivanje dokumenata o temama iz područja kibernetičke sigurnosti
- izdavanje i objavljivanje tehničkih informacija o sigurnosnim alatima
- praćenje i objavljivanje novosti u vezi sa sigurnošću interneta
- provjera ranjivosti ustanova članica CARNET mreže
- provjera ranjivosti drugih korisnika u Republici Hrvatskoj, prema dogovoru
- informiranje javnosti putem portala www.antibot.hr s ciljem suzbijanja *botova*
- sudjelovanje u televizijskim i radijskim emisijama
- sudjelovanje na predavanjima u sklopu konferencija i radionica
- održavanje predavanja i webinara o sigurnosti na internetu

Izvršene proaktivne mjere prema tipu mjera za 2017., nalaze se na slici 4. u nastavku:

Alati	8
Dokumenti	5
Novosti	108
Ukupno preporuka	2 645
Broj provjera ranjivosti	224

Slika 4. Izvršene proaktivne mjere u 2017. godini [21]

Za usporedbu, proaktivne mjere izvršene u 2018. godini prikazane su na slici 5. u nastavku:

Alati	10
Dokumenti	13
Novosti	139
Ukupno preporuka	3 070
Broj provjera ranjivosti	226
Broj izdanih elektroničkih certifikata	697

Slika 5. Izvršene proaktivne mjere u 2018. godini [22]

Kao što je vidljivo, osim nešto više produciranih preporuka i dokumenata vezanih uz proaktivne mjere za zaštitu od kibernetičkog kriminala, obim aktivnosti je otprilike u istom okviru.

4.6.2 Reaktivne mjere Nacionalnog CERT-a

Reaktivne mjere podrazumijevaju aktivnosti vezane uz rješavanje incidenata u kojima sudjeluju strane iz hrvatskog domenskog i adresnog prostora, kao i rješavanje drugih računalnih ugroza na kibernetičkom prostoru Republike Hrvatske.

Neke od reaktivnih mjera su kao što je navedeno [21], [22]:

- obrada incidenata za sve korisnike u Hrvatskoj
- prikupljanje podataka o kompromitiranim računalima, te njihova analiza
- prikupljanje i analiza podataka sa senzora ili drugih sustava
- Abuse služba CARNET mreže

Usporediti ćemo podatke reaktivne podrške u rješavanju incidenata navedene u godišnjim izvještajima Nacionalnog CERT-a Republike Hrvatske za zadnje dvije godine (2017. i 2018. godinu), te analizirati stanje u republici Hrvatskoj obzirom na kibernetički kriminal.

Nacionalni CERT je u 2017. godini zaprimio i obradio ukupno 732 prijave (slika 6.) koji se mogu klasificirati kao računalni incident, a ukupan broj takvih prijava u 2018. (slika 7.) je malo manji – 684 prijave.

TIP INCIDENTA	BROJ	TREND
Web defacement	370	▲
Phishing URL	127	▼
Phishing	59	▲
Malware URL	42	▼
Spam	29	▲
Nedozvoljena mrežna aktivnost	28	▲
Spam URL	26	▲
Bot	20	▲
Ostale vrste napada i zlouporabe	12	▲
DoS	10	▼
Malware domain	4	▲
Ostala kompromitirana računala	3	▼
C&C	2	–
UKUPNO	732	▲

Slika 6. Trendovi Incidenata po tipu u 2017. godini [21]

TIP INCIDENTA	BROJ	TREND
Web defacement	205	▼
Phishing URL	147	▲
Hoax	65	–
Malware URL	65	▲
Phishing	61	▲
Spam	38	▲
Prijevare	31	–
NMA	23	▼
Pogađanje zaporki	8	–
Ostale vrste napada ili zlouporaba	8	▼
OKR	7	▲
Pokušaj iskorištavanja ranjivosti	6	–
Sustav zaražen zlonamjernim kodom	5	–
DoS - Volumetrički napad	5	▼
C&C	3	▲
Kompromitirani korisnički račun	3	–
Spam URL	2	▼
Bot	1	▼
Nedozvoljene mrežne aktivnosti	1	▼
UKUPNO	684	▼

Slika 7. Trendovi incidenata po tipu 2018. godini [22]

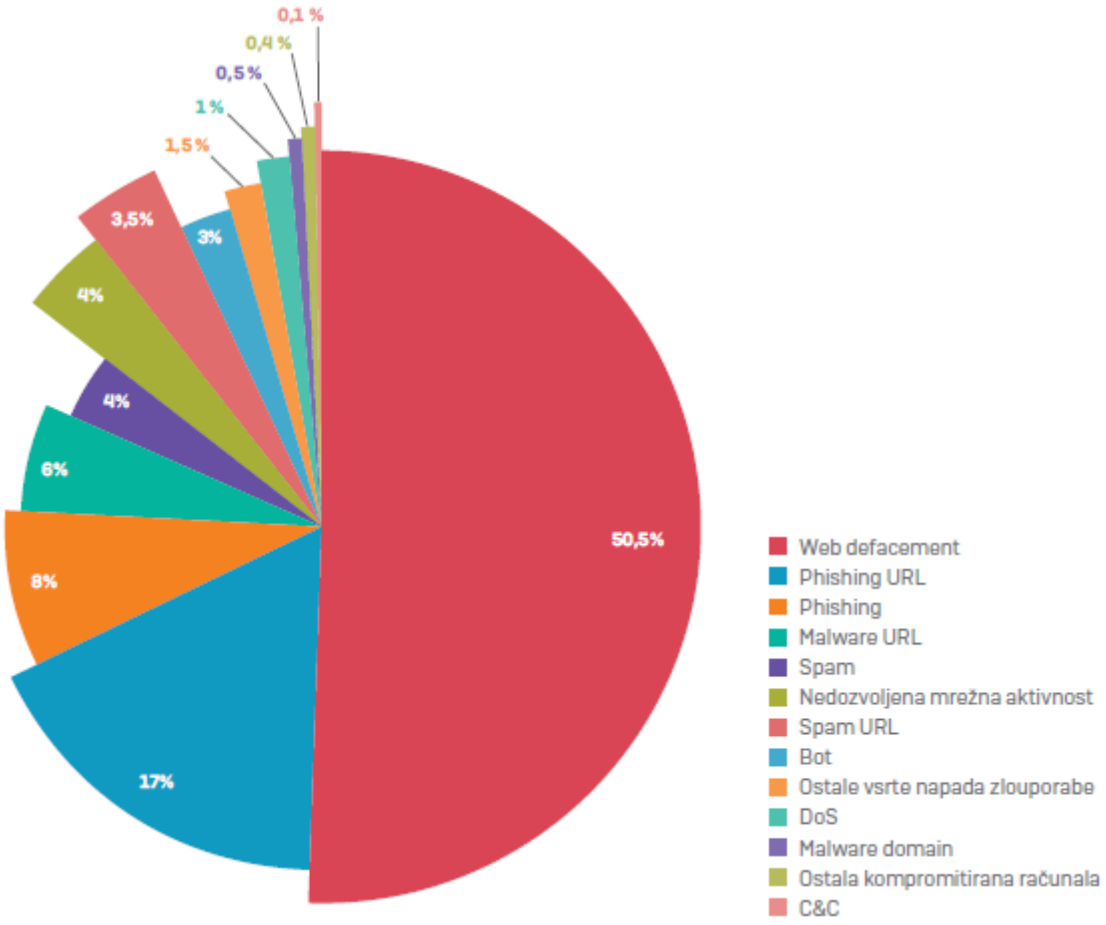
Analizom statističkih podataka o prijavama po tipu incidenta – kao i trenutnih trendova za te vrste napada, možemo donijeti i neke zaključke.

Vidljivo je da u 2017. godini vodeća tri napada po broju prijava su *web defacement*, *phishing URL i phishing*. U odnosu na godinu prije, *web defacement* i *phishing* napadi su u porastu, ali to je rezultat razvijanja alata unutar Nacionalnog CERT-a koji omogućuje otkrivanje takve vrste napada.

U 2018. godini, uz *web defacement* i *phishing URL* napade, pojavljuje se i *hoax* napad kao treći najučestaliji. *Hoax* se pojavljuje kao ucjenjivačka poruka kojom se korisniku prijeti da će objaviti neke njegove osjetljive podatke, ako ne uplati određenu količinu Bitcoin-a. Kompromitiranje web sjedišta u odnosu na 2017. je u padu za 26%.

Kakav je omjer između prijavljenih incidenata ovisno o tipu napada, možda je najlakše uočiti iz grafičkog prikaza statističkih podataka o broju prijava i tipu incidenta,

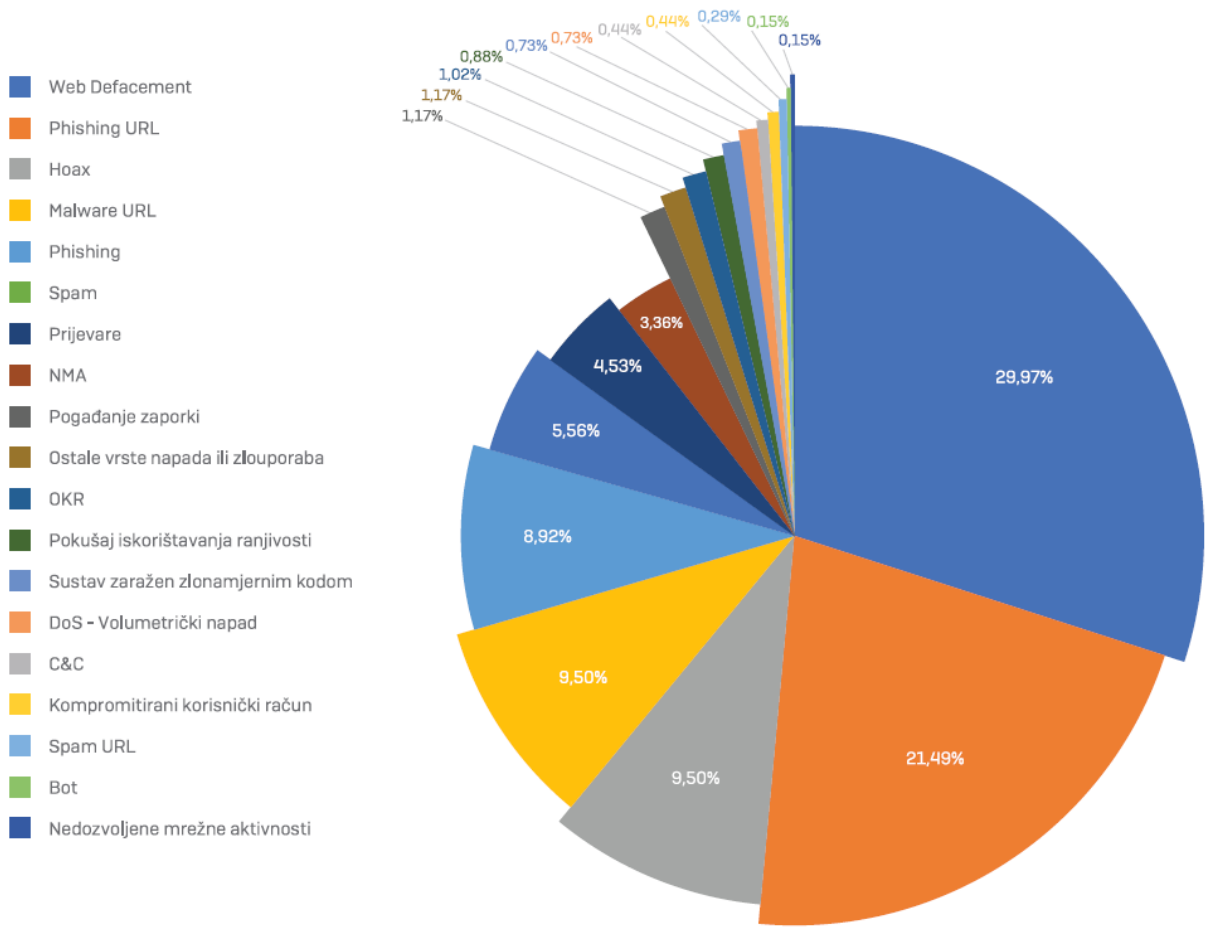
kao što prikazuje slika 8. za podatke iz 2017. godine i slika 9. za podatke iz 2018. godine.



Slika 8. Grafički prikaz tipova incidenata po zastupljenosti u 2017. godini [21]

Na slici 8. vidljiva je dominacija *web defacement* napada (kompromitirano web sjedište sa izmjenjenom naslovnom stranom) po broju prijava, nakon čega po broju prijava slijede *phishing URL* napadi (poveznice do lažnih web sjedišta sa ciljem krađe korisničkih podataka) i najznačajnija promjena od godine prije, povećan broj *phishing* napada kao rezultat nekoliko dobro pripremljenih *phishing* kampanja koje su imale za cilj korisnike iz Republike Hrvatske.

Prijavitelji incidenata, su kao i prethodne godine, mahom bili izvan Republike Hrvatske, ili su prijave zaprimljene od partnera na projektu ACDC (Advance Cyber Defense Center) u kojem Nacionalni CERT RH sudjeluje.



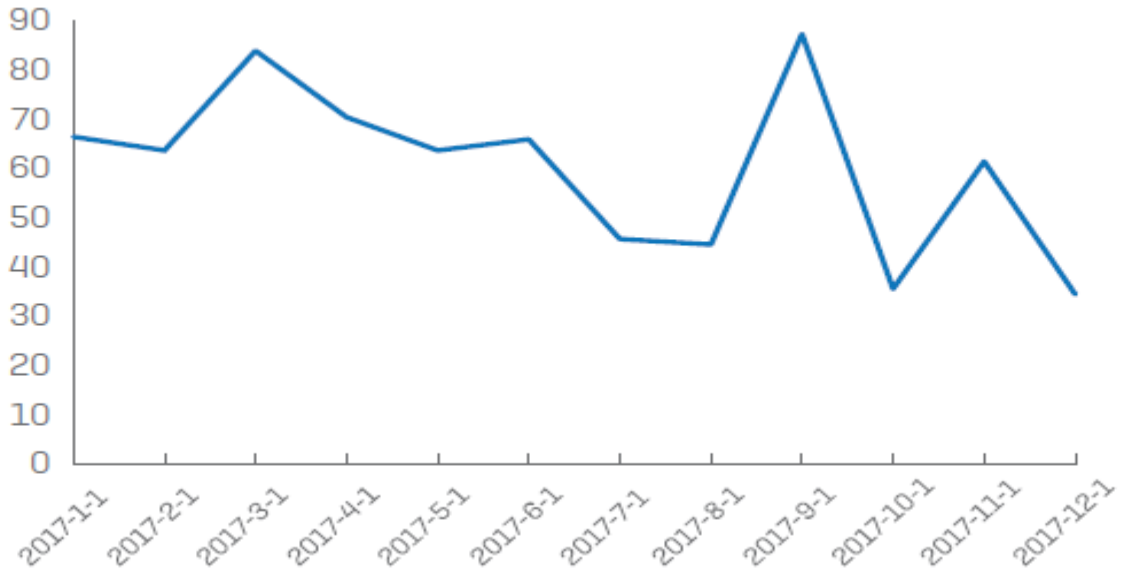
Slika 9. Grafički prikaz tipova incidenata po zastupljenosti u 2018. godini [22]

Na slici 9., jasno je vidljivo smanjenje broja *web defacement* napada, porast *phishing URL* napada, te pojavu sve učestalijih *hoax* napada (ucjenjivačke poruke).

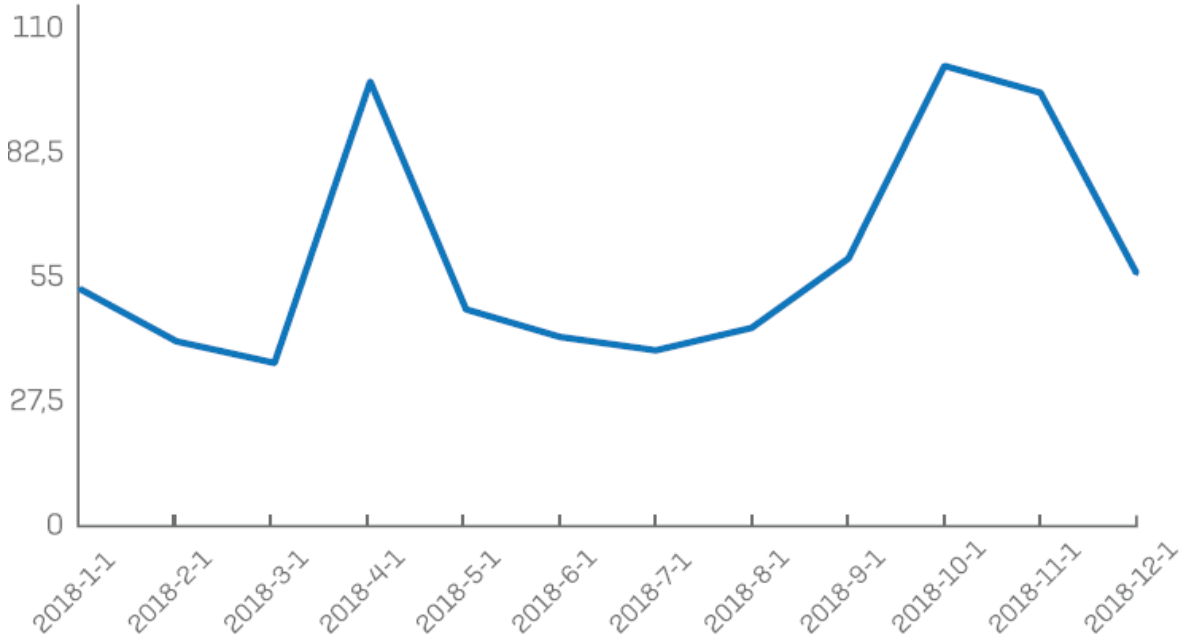
U nastavku, slika 10. prikazuje distribuciju broja obrađenih incidenata na mjesečnoj osnovi u 2017. godini, a slika 11. daje isti prikaz za 2018. godinu.

Za 2017. godinu prosječan broj incidenata po mjesecu je 61, sa svojim maksimumom u rujnu – 85 incidenata, i minimumom u prosincu, kada je zabilježeno samo 38 incidenata.

Za 2018. godinu prosječan broj incidenata mjesečno bio je 57, sa maksimalnim iznosom od 101 incidenta u listopadu i minimalnim brojem incidenata, njih 33, u srpnju 2018. godine.



Slika 10. Broj obrađenih incidenata na mjesečnoj osnovi u 2017. godini [21]



Slika 11. Broj obrađenih incidenata na mjesečnoj osnovi u 2018. godini [22]

U tablici 1. nalaze se nazivi vrsta kibernetičkih napada sa njihovim opisom, a koji su prijavljeni i evidentirani u Republici Hrvatskoj.

Tablica 1. Vrste kibernetičkih napada prijavljenih u RH [21]

POJAM	KRATKI OPIS
Bot/Botnet	Zaraženo računalo/mreža zaraženih računala
C&C	Komandni i kontrolni poslužitelj koji upravlja mrežom zaraženih računala
Phishing	Masivno zasipanje velikog broja osoba porukama u kojima se na prijevaru traži odavanje tajnih podataka
Spam	Neželjena elektronička poruka poslana zbog namjere oglašavanja raznog propagandnog sadržaja, ili u svrhu phishing napada, ili kao sredstvo distribucije poveznica do zlonamjernog softvera
Malware	Zlonamjerni softver namijenjen infiltraciji računala bez znanja njegovog vlasnika, odnosno korisnika
Web defacement	Izmjena izgleda stranica web sjedišta
Ransomware	Skup malicioznih programa koji korisniku onemogućuju korištenje računala
Phishing URL	Poveznica do lažne web stranice koja oponaša legitimnu stranicu na kompromitiranom web sjedištu s ciljem krađe povjerljivih korisničkih podataka
Malware URL	Poveznica do zlonamjernog sadržaja na kompromitiranom web sjedištu
Spam URL	Spam sadržaj na kompromitiranom web sjedištu koji se distribuira kroz spam poruke
DoS	Napad uskraćivanja usluge
Spyware	Vrsta malicioznog programa čija je namjena sakupljanje informacija te preuzimanje kontrole rada na računalu korisnika bez njegova znanja ili dozvole
Backdoor alati	Alati koji omogućuju drugom korisniku da se služi žrtvinim računalom dok je žrtva spojena na internet, bez znanja žrtve
SQL injection napadi	Napad umetanjem SQL koda koji iskorištava ranjivosti na sloju baze podataka
Brute-force napadi	Testiranje svih kombinacija slova, brojeva i posebnih znakova s ciljem otkrivanja zaporki

5. Utjecaj kibernetičkog kriminala na davatelje telekom usluga

Svijet današnjice je izuzetno dobro povezan i tehnološki ovisan. Ljudi, institucije, tvrtke imaju sve veću potrebu za komunikacijom u svakodnevnom životu. Globalna i besprijekorna povezanost danas je omogućena složenom telekomunikacijskom infrastrukturom koja se sastoji od velikog broja različitih tehnologija koje su u kontinuiranom procesu razvoja i inovacija. Međutim, globalna povezanost i jednostavan pristup modernoj tehnologiji također omogućuju kriminalne aktivnosti zlonamjernim korisnicima. Ove aktivnosti mogu biti različite prirode: počevši od pasivnog praćenja do destruktivnih napada koji onemogućavaju normalno funkcioniranje infrastrukture ICT-a (informacijske i komunikacijske tehnologije). Stoga se sve relevantne interesne skupine moraju temeljito pozabaviti sigurnosnim pitanjima telekomunikacijske infrastrukture. Iako svaka tehnologija uključuje određene sigurnosne mehanizme, potrebno je stvoriti dobro osmišljen sigurnosni koncept za infrastrukturu u cjelini, uzimajući u obzir ne samo tehnička pitanja, nego i politički okvir i pravne aspekte. Koncept mora biti predmet stalne revizije kako bi bio u toku s trenutnim prijetnjama. Upravo iz navedenih razloga, mrežna infrastruktura se mora uvijek pratiti i analizirati kako bi ju pratile učinkovite mjere protiv sigurnosnih prijetnji.

5.1 Generalne smjernice za zaštitu od sigurnosnih prijetnji

Mnoge telekomunikacijske tvrtke počele su raditi na strateškim inicijativama, uključujući okvire koji se temelje na rizicima i računalnoj sigurnosti u oblaku kako bi bolje zaštitili svoju informacijsku imovinu. Nakon laganog pada u 2014. godini, telekomunikacijske organizacije povećale su svoj proračun za informacijsku sigurnost za 37% [23]. Prema istraživanju, većina operatora ima dediciranu poziciju za CISO (voditelja informacijske sigurnosti) koji je zadužen za sigurnost, ulaganje u program osposobljavanja za sigurnost zaposlenika i program osvješćivanja, kao i za kibernetsku sigurnost u oblaku kao što su praćenje u stvarnom vremenu, uporaba alata za otkrivanje prijetnji za izgradnju realnih ili gotovo realnih vremenskih prijetnji ili sposobnosti otkrivanja napada. Neki također koriste *Big Data* analitiku kako bi bolje razumjeli unutarnje i vanjske prijetnje, kao i povećali vidljivost anomalija na mreži i u korisničkoj aktivnosti. Gotovo dvije trećine telekoma ima postojeću strategiju zaštite interesa vezanu uz IoT okruženja [23]. Mnogi telekomi proaktivno se udružuju s pružateljima usluga kako bi pomogle u osiguravanju usluga mobilnog plaćanja.

Pomažu riješiti rizike i smanjiti prijevare vezane uz zlonamjerni softver, ranjivosti uređaja i zaštitu osobnih podataka kupaca. Sa digitalizacijom, IP-om, telekomunikacijskim oblakom, itd., stavljena je veća pozornost na sigurnosti osnovne telekomunikacijske infrastrukture koja pokriva radijsku pristupnu mrežu, prijenosnu mrežu, jezgru mreže itd. [24].

Neke od predloženih kontrola zaštite osnovnog sloja su [24]:

- Izraditi i održavati popis ovlaštenih telekomunikacijskih uređaja i softvera, dakle definirati što je predmet štićenja
- Osiguravanje konfiguracija na svim telekomunikacijskim sustavima
- Izvršavanje neprekidne procjene ranjivosti i sanaciju oba sustava *Wireline* / *Wireless*)
- Izgraditi kontrolu upravljanja čvrstim identitetom i pristupom upravljanjem oko telekomunikacijskih sredstava
- Kontroliranje i praćenje povlaštenih ID-ova ili računa
- Održavati, pratiti i analizirati dnevnike revizije
- *E-mail* i *web* sigurnost
- Zaštita protiv zlonamjernog softvera, osobito protiv naprednih i sofisticiranih *malware*-a
- Ograničenja i kontrolirana uporaba mrežnih priključaka, protokola i usluga
- Izgraditi sposobnosti za oporavak podataka
- Izgraditi sigurnost perimetara uz odgovarajuće LAN zoniranje i kontrolu protoka podataka
- Uključiti sigurnosne kontrole usmjerene na podatke
- Snažne sigurnosne mjere za WiFi
- Sigurnosno nadgledanje ključnih računa i uređaja
- Izraditi sigurnosne kontrole nad aplikacijama koje pokrivaju cijeli njihov životni ciklus
- Upravljanje incidentima
- Periodično penetracijsko ispitivanje
- Izgraditi robusne sigurnosne procese i kontrolu upravljanja

Dakle, borba protiv kibernetičkog kriminala je sveobuhvatna, na svim nivoima unutar jednog telekoma, i zahtijeva konstantno unaprjeđenje i testiranje [24].

Poseban pritisak je definitivno na davateljima usluga preko internet *on-line* platformi koji se suočavaju sa brojnim problemima u pokušajima da kontroliraju svoj promet ili informacije koje korisnici dijele preko takvih *on-line* društvenih platformi.

Na slijedećem primjeru, vidi se koliko je ta problematika opširna i koliko ju je teško definirati a da se zadovolje sve strane i osiguraju sve slobode.

Dakle, jedan od najvećih takvih primjera je Google, koji je suočen sa brojnim optužbama vlasnika autorskih prava, farmaceutskih tvrtki i državnih odvjetnika, koji tvrde da zbog toga što se neki korisnici bave kršenjem autorskih prava, prodaju krivotvorene proizvode ili na drugi način potiču potencijalno kriminalne aktivnosti na Internetu, korisničke internetske platforme trebale bi biti odgovorne za te kriminalne radnje. Drugim riječima, Google bi trebao biti kažnjen zbog kršenja autorskih prava korisnika na YouTube-u, ili pak Facebook-u za zlostavljanje svakog korisnika i slično. Prema kritikama, ta bi poduzeća trebala pregledati sve govore korisnika i preuzeti ulogu urednika ili izdavača, umjesto da budu otvorene platforme za govor milijuna. Iako Google već ulaže značajne resurse u smanjenje kršenja, krivotvorenja i ostalih nezakonitih aktivnosti na svojim platformama, jedan državni odvjetnik optužio je Google da je "neuspjeh da se zaustavi ilegalne web stranice sa prodajom ukradene intelektualne imovine", kao da Google ima obvezu ili čak mogućnost uklanjanja kršenja autorskih prava prilikom svake objave na internetu [25].

Za one koji prate internetsku politiku, te vrste argumenata su poznate, ali još uvijek pogrešne. Ti argumenti više puta nisu uspjeli na federalnim sudovima ili sudu javnog mijenja.

Da bi se osigurale digitalne platforme za slobodno izražavanje korisnika, američki kongres je mudro smatrao da govorne platforme ne bi smjele biti krive za pogrešno ponašanje svojih korisnika.

Ipak, svakih nekoliko godina vidimo pokušaje potkopavanja imuniteta davatelja internetskih usluga u sličnim slučajevima. Iako mnogi takvi pokušaji mogu biti dobronamjerni, oni su manjkavi i prijete internetskoj ulozi kao motoru slobodnog izražavanja za stotine milijuna osoba diljem svijeta [25].

5.2 Sigurnosne zakonske i regulatorne obveze davatelja telekom usluga

Zakon o elektroničkim komunikacijama [16] koji je na snazi od 22.07.2017. uređuje područje elektroničkih komunikacija, tj. korištenje elektroničkih

komunikacijskih mreža i pružanje elektroničkih komunikacijskih usluga, pružanje univerzalnih usluga, zaštitu prava korisnika, gradnju i održavanje elektroničke komunikacijske infrastrukture, upravljanje frekvencijskim spektrom, adresnim i brojevnim prostorom, i ono što je predmet teme ovog rada – zaštitu podataka, sigurnost i cjelovitost elektroničkih komunikacijskih mreža i usluga, te obavljanje nadzora i kontrole u elektroničkim komunikacijama preko nacionalnog regulatornog tijela.

Zakon je usklađen sa nizom Direktiva Europske unije izdanih od 2002. godine do 2015. godine, a za njegovu provedbu zadužen je HAKOM – nacionalno regulatorno tijelo osnovano od strane vlade Republike Hrvatske. HAKOM podnosi godišnje izvješće o radu Agencije Hrvatskom saboru i Vladi Republike Hrvatske. Suradnja sa Europskom unijom u ovome području ostvaruje se preko BEREC-a (Body of European Regulators for Electronic Communications). Za navedenu suradnju sa institucijama i regulatornim tijelima na međunarodnom planu, odgovorno je Ministarstvo mora, prometa i infrastrukture [26].

Poglavlje XII. Zaštita podataka i sigurnost elektroničkih komunikacija Zakona o elektroničkim komunikacijama bavi se obavezama davatelja telekom usluga obzirom na sigurnost i zaštitu podataka.

Stavak (1) članak 99. spomenutog zakona glasi [16]:

"*Pružatelji internetskih usluga moraju poduzeti odgovarajuće tehničke i organizacijske mjere za zaštitu sigurnosti svojih usluga, a operatori javnih komunikacijskih mreža moraju poduzeti potrebne mjere za zaštitu sigurnosti elektroničkih komunikacijskih mreža i usluga. Tim se mjerama mora pružiti razina sigurnosti istovjetna postojećoj razini rizika za sigurnost mreže, uzimajući u obzir dostupna tehnička i tehnološka rješenja i povezane troškove. Poduzete mjere provode se kako bi se spriječio i na najmanju mjeru sveo učinak sigurnosnih incidenata na korisnike i međupovezane pružatelje mreža za elektroničku komunikaciju*."

Detaljnije pojašnjeno, davatelji telekom usluga moraju implementirati zaštitne mehanizme u sve aspekte svojih sustava, što je najčešće definirano preporukama i smjernicama međunarodnih organizacija poput ITU-a (International Telecommunication Union), u skladu sa trenutno postojećim tehnološkim mogućnostima za zaštitu sustava i informacija unutar njega, kao i obzirom na financijski aspekt – trošak štićenja mora biti razmjeran riziku i vrijednosti koja je štićena. U slučaju da postoji opasnost od krađe podataka ili onemogućenja usluge, koju davatelj telekom usluge ne može svojim sigurnosnim mehanizmima spriječiti,

obavezan je o tome obavijestiti korisnike svojih usluga, kao i o potencijalnim mjerama zaštite koju korisnici mogu sami poduzeti i troškovima istih.

Po Pravilniku o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga, operatori su dužni jednom godišnje Hrvatskoj regulatornoj agenciji za mrežne djelatnosti (HAKOM) dostaviti dokumentiranu sigurnosnu politiku za prethodnu godinu koja obuhvaća poduzete mjere sigurnosti i pripadajuće norme.

Nadalje, od operatera javnih komunikacijskih mreža i pružatelja internetskih usluga, bilo da su to pravne ili fizičke osobe, što je definirano u članku 108. istoga zakona, očekuje se da o vlastitom trošku provode tajni nadzor mreža i usluga. Taj dio zakona odnosi se na područje nacionalne sigurnosti [16], [26], [27].

U srpnju 2018. godine, Hrvatski sabor donosi Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga [28]. Svrha donošenja tog zakona je bila osigurati visoku razinu kibernetičke sigurnosti u pružanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti. Ovaj zakon je važan jer se njime postavljaju širi zahtjevi koji uključuju sva tri osnovna sigurnosna kriterija (povjerljivost, cjelovitost i raspoloživost), a za mrežne i informacijske sustave kojima se upravlja ključnim i digitalnim uslugama koje su u opsegu ovog zakona.

5.3 Čuvanje osobnih podataka

Posebna obveza odnosi se na čuvanje osobnih podataka, gdje davatelj telekom usluge mora garantirati da će takvim podacima imati pristup samo ovlaštena osoba i to u zakonske svrhe.

Strogo je zabranjeno čuvati prometne podatke korisnika, lokacije ili bilo kakve druge osobne podatke koje je davatelj telekom usluge obradio i pohranio, kada potreba za njima više ne postoji, osim ako nije dobivena privola korisnika za njihovo korištenje u druge svrhe ili ako su isti anonimizirani. Ova zabrana ne vrijedi u slučaju obaveze davatelja telekom usluge definirane u članku 109. Zakona o elektroničkim komunikacijama, gdje je davatelj usluge dužan čuvati podatke u njihovom izvornom stanju još dvanaest mjeseci nakon što je komunikacija obavljena. Za te podatke vrijede ista pravila o štićenju i ovlaštenom pristupu kao i za sve ostale podatke koji su još uvijek predmet obrade.

HAKOM i nadležno tijelo za zaštitu osobnih podataka imaju pravo nadzirati da li mjere koje su implementirane u svrhu zaštite osobnih podataka i cjelovitosti integriteta nuđene usluge zadovoljavaju obzirom na preporuke regulatornih tijela. U slučaju incidenta povezanih sa probojem sigurnosnih mjera, te krađe osobnih podataka, davatelj telekom usluge dužan je to odmah prijaviti HAKOM-u koji prema potrebi to prijavljuje ENISA-i i drugim regulatornim nacionalnim i međunarodnim tijelima [16], [26], [27].

5.4 Suradnja davatelja telekom usluga sa drugim institucijama

Davatelji telekom usluga imaju obavezu surađivati sa nacionalnim regulatornim tijelima, međunarodnim organizacijama – regulatornim i standardizacijskim, kao i sa tijelima kaznenog progona u svrhu osiguranja podataka relevantnih za istrage i forenziku počinjenih kriminalnih djela. Navedena suradnja ne podrazumijeva samo reaktivni dio, davanje podataka nakon počinjenja kriminalnog djela, nego podrazumijeva i proaktivni dio koji se odnosi na konstantno unaprjeđenje sigurnosnih mehanizama potrebnih za očuvanje integriteta nuđene usluge.

Sama suradnja davatelja telekom usluga na području kibernetičkog kriminala postoji i sa privatnim sektorom, i definirana je većinom Zakonom o elektroničkim komunikacijama [16] i Zakonom o elektroničkoj trgovini [29]. Dodatne smjernice za suradnju sa privatnim sektorom u borbi protiv te vrste kriminala sadrži i Nacionalna strategija kibernetičke sigurnosti. Dobar takav primjer je suradnja davatelja telekom usluga sa bankama, kartičnom industrijom, policijom i državnim tužiteljstvom, preko Odbora za prijevare s platnim karticama koji djeluje unutar Hrvatske udruge banaka, a na slučajevima prijevare i zloupotrebe kreditnih kartica. Međunarodna suradnja na području kartičnih prijevara postoji i sa izdavateljima kreditnih kartica (Visa, MasterCard, American Express), kao i sa INTERPOL-om i EUROPOL-om.

Tijela kaznenog progona Republike Hrvatske imaju suradnju i sa regionalnim davateljima telekom usluga, kao jedan od primjera je suradnja sa Google Hrvatska na jednom istražnom slučaju.

Već duži niz godina postoji suradnja između nadležnog Ministarstva mora, prometa i infrastrukture (MMPI) kao središnjeg tijela, Hrvatske regulatorne agencije za mrežne djelatnosti (HAKOM) kao regulatora, odnosno UVNS-a kao središnjeg tijela za informacijsku sigurnost i Nacionalnog CERT-a u području zaštite od kibernetičkog i

računalnog kriminala korisnika javnih elektroničkih usluga, i koordinatora rješavanja sigurnosnih incidenata između davatelja telekom usluga i Nacionalnog CERT-a. Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga, propisao je implementaciju obaveznih sigurnosnih mjera za davatelje telekom usluga, sukladno s međunarodnom normom ISO 27001. HAKOM, kao nadležno regulatorno tijelo, kontrolira provedbu mjera nadzorom davatelja telekom usluga. Također, na prijedlog MMPI, HAKOM imenuje svog predstavnika u Upravni odbor ENISA-e.

6. Pravo nadzora nasuprot prava privatnosti i slobode govora

Borba protiv kibernetičkog kriminala zahtijeva korištenje raznih mehanizama monitoriranja, praćenja i istražnih metoda bilo u svrhu prevencije kriminalnih radnji ove vrste kriminala ili u svrhu reaktivnog rješavanja računalnih incidenata, a koje nisu uvijek u skladu sa ljudskim pravima na privatnost i slobodu govora. U najmanju ruku, ta granica koja dijeli potrebu za nadzorom i ljudska prava, je vrlo tanka a nekada i teško odrediva.. Ljudska prava, sloboda govora, te da li je neki sadržaj okarakteriziran kao kriminalan – sve to uvelike ovisi o nacionalnim pravnim okvirima i zakonima, i tu može biti velikih razlika od države do države. Veliki utjecaj na to imaju povijest, kultura, vjerski običaji, mentalitet nacije i niz drugih faktora, koji onemogućuju globalizaciju ove tematike, kao i rješenje koje je uvijek primjenjivo.

6.1 Prava na privatnost i slobodu govora u Republici Hrvatskoj

Građanima Republike Hrvatske Ustav garantira slobodu mišljenja, govora i iznošenje osobnih stavova. Navedene slobode odnose se kako na osobne javne nastupe, tako i na druga sredstva priopćavanja, poput tiska i sve vrste digitalnih sredstava komunikacije. Cenzura je u tom smislu, kao takva, zabranjena. Dodatno, ustavna prava uređena su Zakonom o medijima [30], Zakonom o elektroničkim medijima [31] i Zakonom o Hrvatskoj radioteleviziji [32].

Nadalje, svakoj fizičkoj osobi neovisno o državljanstvu, prebivalištu, rasi, spolu, vjerskom ili političkom opredjeljenju, društvenom položaju ili bilo kakvom drugom opredjeljenju ili uvjerenju, u Republici Hrvatskoj garantira se pravo na zaštitu osobnih podataka. Navedeno pravo regulirano je Zakonom o provedbi Opće uredbe o zaštiti podataka [14]. Ovaj zakon primjenjiv je u procesuiranju kibernetičkog i računalnog kriminala ovisno o specifičnom slučaju, a vezano uz aktivnosti nadzora i istražnih postupaka.

U travnju 2013. donesen je Nacionalni program zaštite i promicanja ljudskih prava, koji također u prvi plan stavlja pravo na zaštitu osobnih podataka, slobodu medija i pravo na pristup informacijama.

Navedena ustavna prava mogu se privremeno ograničiti za vrijeme istrage kaznenih djela kibernetičkog i računalnog kriminala ako je to potrebno, odnosno ako se istraga ne može provesti na drugi način, a što je u skladu s člankom 332. Zakona o

kaznenom postupku. U takvim slučajevima nadležni sudac može dopustiti slijedeće dokazne radnje [19] :

- nadzor i snimanje telefonskih razgovora i drugih načina komunikacije na daljinu
- presretanje, prikupljanje i snimanje računalnih podataka
- ulazak u prostorije radi provođenja nadzora i snimanje prostorija
- tajno praćenje i snimanje osoba i predmeta
- uporabu prikrivenih istražitelja i pouzdanika
- simuliranu prodaju i otkup predmeta, simulirano davanje potkupnine i simulirano primanje potkupnine
- pružanje simuliranih poslovnih usluga ili sklapanje simuliranih pravnih poslova
- nadzirani prijevoz i isporuka predmeta kaznenog djela

Gore navedene mjere nadzora mogu se izvršiti i nad osobama koje se sumnjiči za direktnu ili indirektnu umiješanost u izvršenje računalnih kaznenih djela, na način da prenose poruke počinitelju ili od počinitelja navedenog kaznenog djela, kao i da počinitelj koristi njihovu računalnu ili telekomunikacijsku opremu i infrastrukturu.

Za tehničko omogućavanje ovih nadzornih mjera zadužen je Operativno-tehnički centar za nadzor telekomunikacija, koji ujedno surađuje po potrebi sa davateljem telekom usluga. Npr. po nalogu suca, Operativno-tehnički centar za nadzor telekomunikacija može od davatelja telekom usluga tražiti podatke o prometu, adrese uređaja koje su sudjelovali u komunikaciji kao i njihovu lokaciju, ili pak identifikacijske oznake uređaja koje su sudjelovale u spornim komunikacijama osumnjičenih osoba [19].

Vezano za uklanjanje neprimjerenog sadržaja sa internetskih platformi, odnosno sadržaja koji je nezakonit obzirom na pravni okvir Republike Hrvatske, sud može naložiti pružatelju internet usluge da se takav sadržaj ukloni ili da se internetska stranica obriše [19].

Hrvatska akademska i istraživačka mreža (CARNET), kao upravitelj nacionalne vršne domene, može u skladu s Pravilnikom o organizaciji i upravljanju nacionalnom internetskom domenom privremeno deaktivirati određenu hrvatsku (.hr) domenu ako su prekršene određene odredbe tog pravilnika ili ako postoji ozbiljna sumnja da korisnik djeluje suprotno načelima dobre vjere te se upotrebom domene krše prava trećih

strana i stoga uzrokuje ozbiljna i nepopravljiva šteta ili ako korisnik namjerava neovlašteno prenijeti registriranu domenu drugoj osobi.

6.2 Opća uredba o zaštiti podataka - GDPR

U Povelji Europske unije o temeljnim pravima u članku 8. stavci 1., kao i u Ugovoru o funkcioniranju Europske unije, članak 16. stavak 1., definirano je da svaki pojedinac ima pravo na zaštitu osobnih podataka. Navedeno pravo ipak, nije apsolutno pravo, nego ovisi o kontekstu tog prava sa promatranom funkcijom u društvu i drugih temeljnih prava u skladu sa načelom proporcionalnosti.

Brz tehnološki razvoj, kao i sveprisutna globalna povezanost, utjecali su na značajno povećanu količinu podataka koja se prikuplja i razmjenjuje, pa tako i osobnih podataka pojedinaca. Digitalizacija skoro svih aspekata djelatnosti, omogućuje privatnim tvrtkama, kao i javnim institucijama korištenje tih podataka na neograničene načine, i tu je nastao veliki izazov u zaštiti osobnih podataka pojedinaca, odnosno potreba za jasnim i usklađenim okvirom za zaštitu osobnih podataka građana Europske unije.

Opća uredba o zaštiti podataka ili GDPR (General Data Protection Regulation) novi je zakon o zaštiti osobnih podataka koji svih 28 država članica EU-a mora primijeniti, odnosno implementirati u svoje pravne okvire. Usklađenje pravnih okvira država članica olakšati će tvrtkama tranziciju poslovanja u skladu sa novim propisima na međunarodnom planu, ali svejedno standardi GDPR-a zahtijevati će značajne financijske investicije, kao i vrijeme i ljudske resurse za implementaciju mehanizama zaštite koji podupiru te propise [33].

Predmet GDPR-a je zaštita osobnih podataka porijeklom iz Europske unije. To znači da tvrtke koje obrađuju ili prikupljaju osobne podatke građana iz Europske unije, podliježu GDPR-u čak i ako se one ne nalaze u Europskoj uniji. Navedeno vrijedi i za razne udruge, međunarodne organizacije ili javna tijela koja obrađuju podatke građana Europske unije.

6.2.1 Što su osobni podaci

GDPR se odnosi samo na zaštitu osobnih podataka. Podaci koji se ne smatraju osobnima, kao i podaci koji su anonimizirani, zaštićeni su nacionalnim pravnim okvirima pojedinih zemalja i ne podliježu GDPR-u.

Zakonska definicija osobnih podataka kaže da su osobni podaci "*svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi*". Navedeno bi značilo da se osobnim podacima smatraju svi podaci koji bi mogli upućivati na točan identitet neke osobe, čak i ako iz tih podataka vi osobno ne možete zaključiti tko je ta osoba, ali netko drugi može.

GDPR pokriva sljedeće kategorije podataka klasificiranih kao osobni podaci [14], [33]:

- osnovni podaci – ime i prezime, broj osobne iskaznice, lokacijski podaci
- podaci s kreditnih kartica
- zdravstveni karton (invalidnost, povijest bolesti i sl.)
- biometrijski podaci (sken rožnice, otisci prsta itd.)
- genetski podaci (DNA i sl.)
- vjerska i filozofska uvjerenja
- etnička pripadnost
- ekonomsko stanje
- članstvo u sindikatu
- seksualna orijentacija i spolni život
- IP adrese
- osobne poruke e-pošte
- kolačići u pregledniku
- pseudonimizirani podaci

6.2.2 Načela obrade osobnih podataka

Bilo koji pravni subjekt koji prikuplja osobne podatke od korisnika, zove se "voditelj obrade", a voditelj obrade daje naredbe za obradu podataka "izvršiteljima obrade". U većini slučajeva isti pravni subjekt je i voditelj i izvršitelj, ali to nije pravilo koje vrijedi uvijek.

Ključni dio regulative su načela koja treba poštovati prilikom obrade podataka, a nepoštovanje tih načela predmet su velikih kazni. Načela su kako slijedi [14]:

- podaci se smiju obrađivati samo na valjanoj zakonskoj osnovi, na pošten i prema ispitaniku transparentan način
- obavezno navođenje svih svrha obrade u koje se podaci prikupljaju

- prikupljati smijete samo podatke koji su relevantni i potrebni za ispunjavanje svrhe u koju se obrađuju
- podaci trebaju biti točni i ažurirani
- podatke ne smijete pohranjivati duže od razdoblja potrebnog za ispunjavanje svrhe u koju su prikupljeni
- dužni se osobne podatke zaštititi od nezakonite i nedozvoljene obrade, slučajnog gubitka ili uništenja
- morate biti u stanju dokazati usklađenost s gore navedenim načelima

U obradi osobnih podataka, moguće je koristiti mehanizam "privole", koja je jedan od nekoliko zakonskih osnova za obradu podataka, međutim korištenje tog mehanizma povlači slijedeće dužnosti [14] :

- potrebno je ispitaniku pružiti izjavu o privoli prilikom prikupljanja podataka
- mora se zahtijevati privola za korištenje podataka
- mora se omogućiti povlačenje privole na jednostavan način
- potrebno je tražiti izričitu privolu ako prikupljate posebne kategorije osobnih podataka

6.2.3 Glavne metode zaštite podataka prema GDPR-u

U sklopu GDPR-a, definirane su i određene organizacijske i tehničke mjere u svrhu zaštite osobnih podataka koji su predmet prikupljanja i obrade. Obzirom da podaci koji su predmet obrade moraju biti u svakom trenutku zaštićeni, pravni subjekti koji su involvirani u prikupljanje i obradu osobnih podataka dužni su implementirati mjere zaštite podataka, uvesti kontrolu pristupa podacima, brisati podatke koji više nisu potrebni, kao i držati se načela integrirane zaštite privatnosti (*privacy by design*). U nastavku, navest će se šest glavnih metoda zaštite podataka [34] :

Procjene rizika

Potrebno je provesti procjenu rizika preko dva faktora – potencijalnim posljedicama gubitka podataka i vjerojatnosti gubitka podataka. Što je veći rizik po ova dva kriterija, to su podaci okarakterizirani kao osjetljiviji podaci i zahtijevaju veću mjeru štićenja. Ova metoda je jako bitna, jer napredni tehnološki mehanizmi štićenja podataka mogu biti vrlo skupi, te je jako bitno da odredimo koji podaci zaslužuju veći

a koji manji nivo zaštite. Također, kriva procjena osjetljivosti podataka i mehanizama branjenja istih, može uzrokovati gubitak ili krađu tih podataka a što se kažnjava vrlo visokim iznosima.

Sigurnosne kopije

Sigurnosne kopije omogućuju zaštitu na način da ako dođe do kibernetičkih napada bilo koje vrste, a koji mogu oštetiti, obrisati ili otuđiti navedene podatke, isti podaci su i dalje dostupni te ne uzrokuju prekide u poslovanju. Sigurnosne kopije se izrađuju u točno određenim intervalima. Za osjetljivije podatke ti intervali trebali bi biti što kraći. Pohrana takvih kopija treba taođer biti na sigurnom mjestu, sa kontrolom pristupa, u adekvatnim uvjetima i na adekvatnim medijima.

Ne treba zaboraviti, da u slučaju brisanja podataka na zahtjev ili podataka koji nisu više potrebni, treba obrisati iste podatke i sa sigurnosnih kopija.

Enkripcija

GDPR navodi enkripciju podataka kao primjer dobre prakse, jer npr. gubitak takvih podataka, osim ako ne postoji sigurnosna kopija, ne treba prijavljivati nadležnim nadzornim tjelima, jer se smatra da su enkriptirani podaci neupotrebljivi bilo kome drugome.

Osjetljivi podaci trebali bi biti enkriptirani tijekom cjelokupne eksploatacije istih, od trenutka zaprimanja podataka od korisnika (mrežni kriptografski protokoli), tijekom obrade (enkripcija memorije), kao i tijekom arhiviranja (RSA algoritam, AES enkripcija).

Pseudonimizacija

Pseudonimizacija podrazumijeva obradu osobnih podataka na način da se osobni podaci nakon tog postupka ne mogu povezati točno određenoj osobi bez uporabe dodatnih informacija, pod uvjetom da se takve odvojene informacije drže odvojeno pod tehničkim i organizacijskim mjerama koje onemogućuju utvrđivanje identiteta osoba čiji su podaci predmet obrade.

Ovaj postupak se koristi kada se prikupljaju i obrađuju statistički podaci i podaci korišteni u znanstvene svrhe.

Kontrola pristupa

Ljudski faktor je najčešći uzrok pogrešaka, pa tako i onih koje dovode do gubitka ili krađe podataka. Stoga, jedan od najefikasnijih načina da smanjimo mogućnost povrede podataka je da pristup osjetljivim podacima damo što manjem broju osoba, odnosno samo osobama koje su nužne za rukovanje tim podacima u zadanu svrhu. Jasna sigurnosna politika sa definiranim kontrolama pristupa, i edukacijom zaposlenika, jedna je od presudnih metoda u zaštiti osobnih podataka, kao i podataka bilo koje vrste.

Brisanje podataka

GDPR donosi pravilo da se osobni podaci moraju obrisati, tj. uništiti nakon što više nisu potrebni u svrhu u koju su prikupljani, ili moraju biti anonimizirani. Također, podaci se mogu izbrisati i na zahtjev određene osobe. Mora se paziti da se obrišu podaci na svim mogućim lokacijama, kao i na sigurnosnim kopijama.

Brisanje podataka jedan je od najsigurnijih načina da podaci ne dođu u krive ruke, a smanjuje se i trošak čuvanja tih podataka, od prostora koji zauzimaju do sigurnosnih mjera koje ih štite.

6.3 Zakon RH o provedbi Opće uredbe o zaštiti podataka

GDPR propisan Uredbom Europske unije 2016/679 Europskog parlamenta i Vijeća od 27.04.2016., koja regulira prava pojedinaca na zaštitu prilikom prikupljanja i obrade osobnih podataka, stupio je na snagu u svim državama članicama Europske unije, pa tako i u Hrvatskoj, u kojoj je 25.05.2018. donesen Zakon o provedbi Opće uredbe o zaštiti podataka [14].

Stupanjem na snagu ovoga zakona, prestaje važiti dotadašnji Zakon o zaštiti osobnih podataka, kao i Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka [35] i Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka [36].

Osobni podaci koji se koriste u svrhu istražnih postupaka, ili u svrhu zaštite nacionalne sigurnosti i obrane, ne podliježu ovome zakonu.

Nadzorno tijelo zaduženo za nadzor provedbe ovog zakona je Agencija za zaštitu osobnih podataka. Agencija je neovisno državno tijelo, koja odgovara direktno Hrvatskome saboru.

Zaduženja, odnosno poslovi koji su obaveza Agencije vezano uz navedeni zakon su slijedeća [37]:

- može pokrenuti kaznene, prekršajne, upravne i druge sudske i izvan sudske postupke zbog povrede Opće uredbe o zaštiti podataka i ovoga zakona
- donosi kriterije za određivanje visine naknade administrativnih troškova iz članka 43. stavka 2. ovoga zakona i kriterije za određivanje visine naknade iz članka 43. stavka 3. ovoga zakona
- objavljuje pojedinačne odluke sukladno člancima 18. i 48. ovoga zakona na mrežnim stranicama Agencije
- pokreće i vodi odgovarajuće postupke protiv odgovornih osoba zbog povrede Opće uredbe o zaštiti podataka i ovoga Zakona
- obavlja poslove neovisnog nadzornog tijela za praćenje primjene Direktive (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP
- obavlja druge zakonom propisane poslove

U svome izvješću o radu Agencije za zaštitu osobnih podataka za 2018. godinu [37], vezano uz telekomunikacijski sektor, posebno su izdvojene neke grupe slučajeva:

- slučajeve zlouporabe osobnih podataka u svrhu sklapanja lažnih pretplatničkih ugovora o pružanju usluga nastalih kao produkt krađe identiteta
- slučajevi koji su se odnosili na nezakonitu obradu osobnih podataka u telekomunikacijskom sektoru
- prosljeđivanje osobnih podataka od strane telekom operatera agencijama za naplatu potraživanja i zakonitost takove obrade

Zaprimljene pritužbe odnosile su se uglavnom na sklapanje pretplatničkih ugovora pomoću nezakonito prikupljenih osobnih podataka, poput izgubljenih osobnih

dokumenata, lažnih dokumenata ili ukradenih. Obzirom da ti slučajevi imaju obilježja kaznenog djela, proslijeđeni su nadležnim tijelima – Policiji i Državnom odvjetništvu.

Zahtjevi za povredom prava koji su odbijeni, odnosili su se na osobe koje ne podliježu Zakonu o provedbi Opće uredbe o zaštiti podataka, kao i slučajevi gdje nije ustanovljena povreda prava i da su svi osobni podaci točni.

Nadalje, pritužbi je bilo vezano uz prosljeđivanje njihovih podataka drugim pravnim osobama koje obavljaju djelatnost informiranja i izdavanja javnih imenika.

Bilo je i upita koji su se odnosili na vremenski period čuvanja njihovih podataka, kao i za ostvarivanje prava na brisanje njihovih osobnih podataka.

U sektoru Interneta i društvenih mreža, slučajevi pritužbi najčešće su se odnosili na postavljanje lažnih korisničkih profila, kao i objavu osobnih podataka na društvenim mrežama.

Velik broj slučajeva odnosio se na prikupljanje preslika osobnih dokumenata u svrhu provođenja lažnih nagradnih igara na lažnim Facebook stranicama voditelja obrade, što je okarakterizirano kao kazneno dijelo krađe identiteta, i zbog toga je obaviješteno Ministarstvo unutarnjih poslova., kao što je dan niz javnih priopćenja putem različitih medija, nakon čega je broj pritužbi pao.

7. Zaključak

Sveopća tehnološka globalizacija koja zadire u svaki aspekt ljudskog života, uz bezbroj benefita i mogućnosti, donijela je i jedan od najvećih izazova sa kojim se danas susrećemo – kibernetički kriminal. Kako osigurati zaštitu informacija u digitalnim procesima u kojima svakodnevno sudjelujemo od krađe ili gubitka, kako zaštiti sam tehnološki komunikacijski sustav od malicioznih napada, a opet zadržati pravo na privatnost i slobodu govora i izražavanja – cilj je jasno postavljen i definiran, ali tehnološka rješenja, metode i pravni mehanizmi koji bi to trebali osigurati imaju izuzetno kompleksan transnacionalni problem čije rješavanje zahtjeva globalni odgovor, uključenost svih strana, i konstantno praćenje i unaprjeđivanje kako se i okolina u kojoj se pojavljuje taj fenomen konstantno mijenja i biva sve kompleksnija.

Rezultati istraživanja pokazuju da bi toj temi na nacionalnom, europskom i svjetskom nivou trebalo posvetiti puno više pažnje, i donijeti mehanizme koji bi mogli pratiti trendove kibernetičkog kriminala, jer razvojem tehnologije – koji je sve brži i brži – pojavljuju se konstantno novi načini ugrožavanja sigurnosti tim putem, i pravni okviri koji to prate moraju biti puno fleksibilniji, i brži za implementaciju u nacionalne pravne sustave. Dakle, globalna konvencija na svjetskom nivou je nužnost u uspostavi efikasne borbe protiv kibernetičkog kriminala.

Iako je Konvencija o kibernetičkom kriminalu Vijeća Europe dobar temelj kojeg prihvaća sve više država u svijetu, mnogo je tu još suprotstavljenih interesa, kao i kulturnih i vjerskih razlika, da bi Konvencija postala globalno rješenje. Te razlike možda neće nikada biti pomirene u jedan zajednički pravni okvir, ali treba mu se pokušati približiti što je više moguće.

Hrvatska prati sve Direktive, Uredbe i smjernice Europske unije i kao država članica, implementira ih u svoj kaznenopravni okvir. U tom segmentu, kao i u segmentu međunarodne suradnje trudimo se biti proaktivni i sudjelovati na bilo koji način koji može pomoći u suzbijanju kibernetičkog kriminala. Izvješće Europske unije o Republici Hrvatskoj vezano uz borbu protiv kibernetičkog kriminala je zadovoljavajuće, uz napomenu da treba poboljšati međusobnu suradnju tijela i institucija unutar Republike Hrvatske.

Telekom operateri i davatelji internet usluga, obzirom na prirodu svoje djelatnosti, ključni su za borbu protiv kibernetičkog kriminala. Obzirom da je njihova infrastruktura ono što omogućava zlonamjerne aktivnosti i kaznena djela, efikasna,

stalno unaprjeđivana zaštita te infrastrukture je ujedno i globalni prioritet. Davatelji komunikacijskih i internet usluga su ujedno i najveći prikupljivači podataka korisnika – njihovi osobni podaci, lokacije, navike, preferencije i ostali privatni podaci sve su izloženiji krađi ili zloupotrebi. Ujedno, ti podaci su interesantni i drugim kompanijama u svrhu marketinških analiza te segmentizacije tržišta prema interesnim skupinama.
Navedene činjenice otvaraju još jedan veliki problem, a to je zaštita privatnosti, osobnih podataka i slobode govora i izražavanja. Borba protiv kibernetičkog kriminala iziskuje konstantan nadzor i mogućnost vršenja istraga u svrhu kaznenog progona, te je vrlo teško odrediti tu granicu neophodnog nadzora i prava na privatnost i slobodu govora. Postojećem problemu pokušava se doskočiti zakonima poput GDPR-a u Europskoj uniji, odnosno Zakonom o provedbi Opće uredbe o zaštiti podataka u Republici Hrvatskoj, međutim tim zakonima definirana su prava koja nisu apsolutna prava pojedinaca, odnosno ta prava ne vrijede ako je pojedinac u sumnji počinjenja kaznenog dijela.

Dodatni problem u ovoj tematici je što zakoni o osobnim slobodama nisu u svim državama isti, a davatelji internet usluga ili usluga *on-line* platformi jednostavno ne mogu pratiti sve korisnike, sve objave i tretirati ih u skladu sa pojedinačnim nacionalnim pravnim okvirima, a dok su istovremeno globalno dostupni medij. Zakonodavne institucije, nositelji autorskih prava i sve druge interesne skupine trebale bi jače i intenzivnije surađivati sa davateljima telekom usluga i vlasnicima internetskih tehnoloških platformi u svrhu poboljšanja sigurnosti i poštivanja zakona na javno dostupnim mrežama i servisima, a ne prejudicirati krivnju davatelja usluga za svaku objavu kojom je učinjeno neko kazneno dijelo.

Literatura

[1] **ITU Telecommunication Development Sector:** *Understanding cybercrime – phenomena, challenges and legal response*; rujan 2012.
Preuzeto sa www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
[Pristupljeno: svibanj 2019.]

[2] **Dennis M. A.:** *Cybercrime*; kolovoz 2016.
Preuzeto sa https://www.britannica.com/topic/cybercrime
[Pristupljeno: svibanj 2019.]

[3] **United nations:** *Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime*; Twelfth UN Congress on Crime Prevention and Criminal Justice; April 2010.
Preuzeto sa: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf
[Pristupljeno: svibanj 2019.]

[4] **Ponemon Institute:** *2018 Cost of Cyber Crime Study - Benchmark Study of Global Companies*; October 2018.

[5] **Zaharia A.:** *Cyber security & cyber crime statistics*; Comparitech, May 2019.
Preuzeto sa https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
[Pristupljeno: lipanj 2019.]

[6] **Harley B.:** *A global convention on cybercrime*; The Columbia - Science and Technology Law Review; March 2010.
Preuzeto sa: http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/
[Pristupljeno: lipanj 2019.]

[7] **Ermert M.:** *Konkurrenz fur Cybercrime-Konvention des Europarates*; Heise online; March 2010.
Preuzeto sa: https://www.heise.de/newsticker/meldung/Konkurrenz-fuer-Cybercrime-Konvention-des-Europarates-958368.html
[Pristupljeno: lipanj 2019.]

[8] *Nacionalna strategija kibernetičke sigurnosti*; Narodne novine br. 61/16

[9] **Vijeće Europske unije:** *Izvješće o ocjenjivanju sedmog kruga uzajamnih ocjenjivanja pod nazivom "Praktična provedba i djelovanje europskih politika o sprječavanju kiberkriminaliteta i borbi protiv njega" – Izvješće o Hrvatskoj*; dokument 5250/1/17 REV 1; ožujak 2017.
Preuzeto sa data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/hr/pdf+&cd=1&hl=hr&ct=clnk&gl=hr
[Pristupljeno: lipanj 2019.]

[10] **Ured vijeća za nacionalnu sigurnost:** *Organizacijski i ustrojbeni položaj tijela za kibernetičko djelovanje na nacionalnoj razini*; Zagreb, lipanj 2018.
Preuzeto sa https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Organizacijski%20i%20ustrojbeni%20polo%C5%BEaj%20tijela%20za%20kiberneti%C4%8Dko%20djelovanje.pdf
[Pristupljeno: lipanj 2019.]

[11] *Zakon o informacijskoj sigurnosti*; Narodne novine br. 79/07

[12] *Zakon o tajnosti podataka*; Narodne novine br. 79/07, 86/12

[13] *Zakon o zaštiti osobnih podataka*; Narodne novine br. 106/12, 130/11, 41/08, 118/06

[14] *Zakon o provedbi Opće uredbe o zaštiti podataka*; Narodne novine br. 42/18

[15] *Zakon o pravu na pristup informacijama*; Narodne novine br. 25/13, 77/11, 144/10, 172/03

[16] *Zakon o elektroničkim komunikacijama*; Narodne novine br. 73/08, 90/11, 133/12, 80/13, 71/14, 72/17

[17] *Zakon o poštanskim uslugama*; Narodne novine br. 144/12, 153/13, 78/15

[18] *Zakon o željeznici*; Narodne novine br. 32/19

[19] **Škrtić D.:** *Kaznenopravna zaštita informatičkih sadržaja*; doktorska disertacija Pravni fakultet Sveučilište u Zagrebu, studeni 2011.
Preuzeto sa
https://www.researchgate.net/publication/286624269_KAZNENOPRAVNA_ZASTITA_INFORMATICKIH_SADRZAJA_CRIMINAL_LAW_PROTECTION_OF_INFORMATICS_CONTENT
[Pristupljeno: srpanj 2019.]

[20] **Čule J.:** *EUROJUST - tijelo Europske unije za pravosudnu suradnju u kaznenim stvarima*; Zagreb, ožujak 2018.
Preuzeto sa http://pak.hr/cke/obrazovni%20materijali/Pravosudna%20suradnja%20putem%20Eurojust-a.pdf
[Pristupljeno: srpanj 2019.]

[21] **CARNET Hrvatska akademska i istraživačka mreža:** *Godišnji izvještaj nacionalnog CERT-a za 2017. godinu*; Zagreb, 2018.
Preuzeto sa https://www.cert.hr/wp-content/uploads/2018/03/CERT.hr_godisnji_izvjestaj_2017.pdf
[Pristupljeno: srpanj 2019.]

[22] **CARNET Hrvatska akademska i istraživačka mreža:** *Godišnji izvještaj nacionalnog CERT-a za 2018. godinu*; Zagreb, 2019.
Preuzeto sa https://www.cert.hr/wp-content/uploads/2019/02/CERT.hr_godisnji_izvjestaj_2018.pdf
[Pristupljeno: srpanj 2019.]

[23] **PwC :** *The Global State of Information Security Survey 2016*; USA 2016
Preuzeto sa https://www.pwc.com/gx/en/issues/information-security-survey/telecommunications-industry.html
[Pristupljeno: srpanj 2019.]

[24] **Alcatel-Lucent Enterprise:** *Information security - strategic iniciatives in telco industry for information security*
Preuzeto sa http://resources.alcatel-lucent.com/asset/200843
[Pristupljeno: srpanj 2019.]

[25] **Levine D.:** *Recurring myths about legal obligations of online platforms*; The Center for Internet and Society at Stanford Law School; September 2013. Preuzeto sa: http://cyberlaw.stanford.edu/blog/2013/09/recurring-myths-about-legal-obligations-online-platforms
[Pristupljeno: srpanj 2019.]

[26] **Marin D.:** *Telekomunikacijska legislativa i standardizacija*; Kigen, Zagreb 2006.

[27] **Kaštela S. i Horvat L.:** *Prometno pravo*; ŠK Zagreb 2008.

[28] *Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga*; Narodne novine br. 64/2018

[29] *Zakon o elektroničkoj trgovini*; Narodne novine br. 173/03, 67/08, 36/09, 130/11, 30/14, 32/19

[30] *Zakon o medijima*; Narodne novine br. 59/04, 84/11, 81/13

[31] *Zakon o elektroničkim medijima*; Narodne novine br. 153/09, 84/11, 94/13, 136/13

[32] *Zakon o Hrvatskoj radioteleviziji*; Narodne novine br. 137/10, 76/12, 78/16, 46/17, 73/17, 94/18

[33] **Europska unija:** *Uredba (EU) 2016/679 europskog parlamenta i Vijeća od 27. travnja 2016.*; Službeni list Europske unije
Preuzeto sa https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[Pristupljeno: srpanj 2019.]

[34] **GDPR Informer**: *Šest glavnih metoda zaštite podataka prema GDPR-u*; RH 2018.
Preuzeto sa https://gdprinformer.com/hr/gdpr-clanci/6-glavnih-metoda-zastite-podataka-prema-gdpr-u
[Pristupljeno: kolovoz 2019.]

[35] *Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka*; Narodne novine br. 105/04

[36] *Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka*; Narodne novine br. *139/04*

[37] **Agencija za zaštitu osobnih podataka:** *Godišnje izvješće o radu AZOP-a za razdoblje od 1. siječnja 2018. do 31. prosinca 2018.*; Zagreb, travanj 2019.
Preuzeto sa: https://azop.hr/images/dokumenti/217/izvjesce_azop_2018.pdf
[Pristupljeno: kolovoz 2019]

Popis slika

Popis tablica

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat mojeg vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom "Kaznenopravna zaštita od kibernetičkog kriminala i uloga telekom operatera", u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student :

U Zagrebu, 12.09.2019.