Funded by
the European Union

SPROVOĐENJE ONLINE PRAVA INTELEKTUALNE SVOJINE

VODIČ ZA IZVRŠITELJE

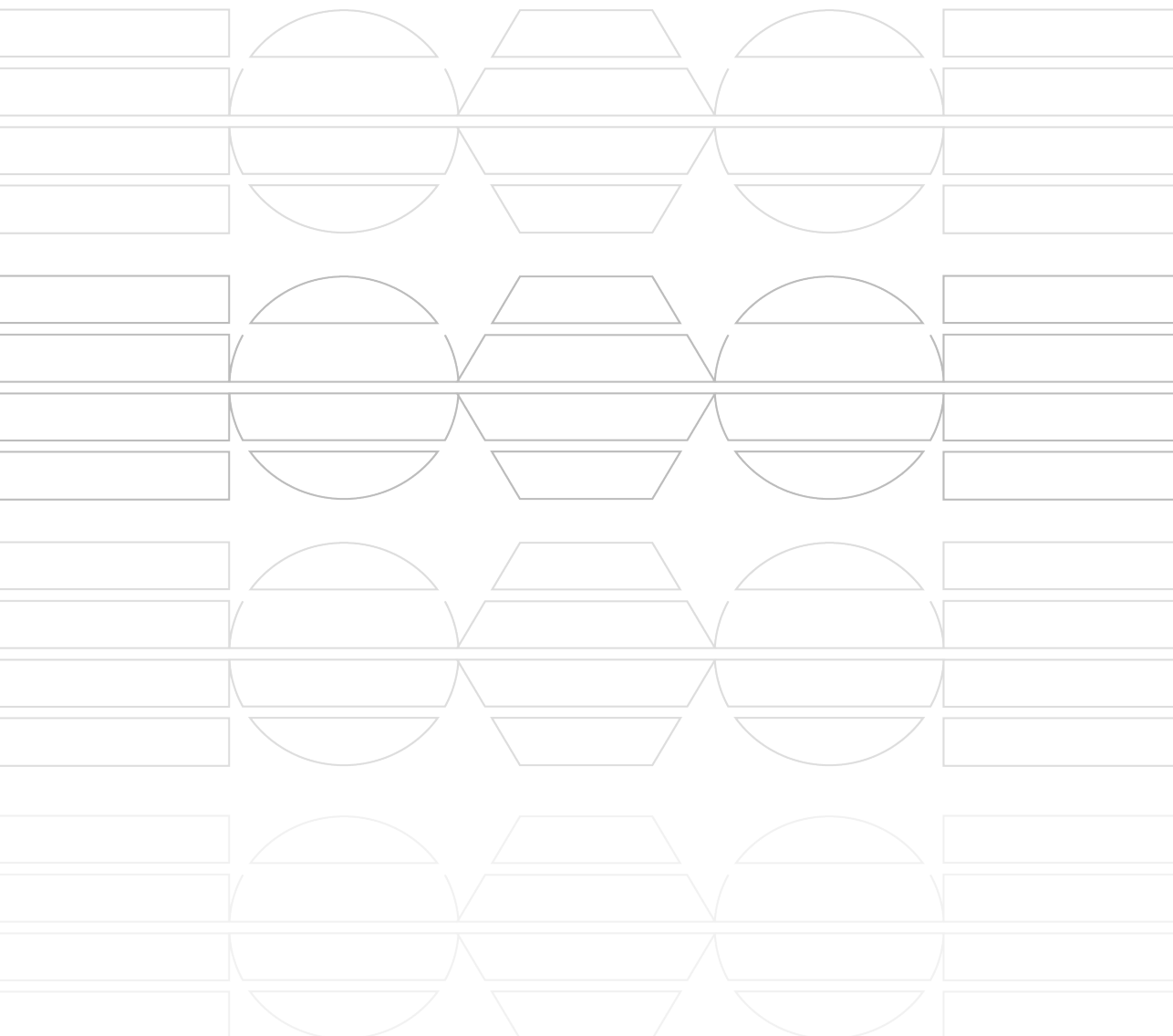
IPRproject
Intellectual Property Rights Project

Prishtinë, 2022

A project implemented by:

ibf INTERNATIONAL CONSULTING

EPLO European Public Law Organization



SKRAĆENICE

ACPO	Udruženje glavnih policijskih službenika.
CDN	Mreža za isporuku sadržaja.
DNS	Sistem imena domena (Domain Name System)
EUIPO	Kancelarija Evropske Unije za intelektualno vlasništvo.
BDP	Bruto domaći proizvod.
IEC	Međunarodna elektrotehnička komisija.
IIPCIC	(Međunarodni kolegijum istraživača krivičnih dela vezanih za IS.
IP	Internet protokol.
AIS	Agencija za industrijsku svojinu.
PIS	Prava Intelektualne Svojine.
IPTV	internet protokol televizija
ISO	Internet organizacija za standardizaciju.
OCRR	Ured za autorska i srodna prava.
OECD	Organizacija za ekonomsku saradnju i razvoj.
OSINT	Inteligencija Otvorenog Koda (Open Source Intelligence).
SEO	Optimizacija za pretraživače.
TCP	protokol kontrole prijenosa (Transmission Control Protocol).
TOR	Projekat Onion Router.
TRIPS	Sporazum o trgovinskim aspektima prava intelektualne svojine.
UNODC	Ured Ujedinjenih Nacija za Droge i Kriminal.
VCP	Prakse Dobrovoljne Saradnje.
VM	Virtuelna Mašina.
VPN	Virtuelna Privatna Mreža.
WCO	Svjetska carinska organizacija
WIPO	Svjetska organizacija za intelektualno vlasništvo.
WHO	Svjetska zdravstvena organizacija.

SADRŽAJ

9. Digitalni dokazi

9.1 Uvod
9.2 Mjesto zločina
9.3 Razmatranje opreme i alata za istraživanje
9.4 Vrste podataka
9.5 Zamke i bombe
9.6 Čuvanje i očuvanje digitalnih dokaza

10. Dalje čitanje

10.1 Kolegijum istraživača krivičnih dela intelektualne svojine

Aneks I - IP objekti
Aneks II - Kontaktne tačke
Aneks III - Zakonodavstvo
Aneks IV – Definicije

1. Uvod

1.1 Svrha Vodiča

Svrha ovog Vodiča je da podigne svest Policije Kosova o značaju intelektualne svojine i veoma realnoj pretnji po društvo od kršenja prava intelektualne svojine (IPR). Ovaj Vodič će takođe naglasiti nacionalni sistem intelektualne svojine i nacionalno zakonodavstvo koje se koristi za zaštitu i sprovođenje online intelektualne svojine. Pored toga, Vodič će opisati kako Kosovska policija može praktično da sprovodi prava online intelektualne svojine.

Drugi vodič pod nazivom “Krivično sprovođenje prava intelektualne svojine - Vodič za izvršioce” je pripremljen da pomogne Policiji Kosova da istražuje kršenja prava intelektualne svojine koje nisu izvršene u onlajn okruženju. Oba vodiča se međusobno dopunjuju i oba treba pročitati da biste dobili jasnu sliku o izazovima u primeni prava intelektualne svojine na Kosovu.

1.2 Intelektualna svojina

Prema Ujedinjenim Nacijama, zločin prava intelektualna svojine je transnacionalna kriminalna aktivnost kojom upravljaju iste kriminalne organizacije umešane u druge ozbiljne kriminalne radnje, uključujući trgovinu narkoticima, krijumčarenje oružja, trgovinu ljudima, korupciju i pranje novca[1]- ali šta je intelektualna svojina?

Intelektualno vlasništvo se odnosi na kreacije uma kao što su izumi, književna dela, umetnička dela, simboli, imena, slike i dizajni koji se koriste u trgovini.[2] Štaviše, intelektualna svojina se tradicionalno deli u dve kategorije: :

- **Industrijalna svojina** koja obuhvata žigove, industrijalne dizajnove, patente i geografske oznake; i
- **Autorska prava** koje obuhvata književna dela (npr. romane, stihove i prestave), filmove, muziku, umetnička dela (npr. crteže,

[1]Falsifikovanje. Globalno širenje. Globalna pretnja. UNICRI.
[2]Svjetska organizacija za intelektualnu svojinu - Šta je intelektualna svojina? www.wipo.int

slike, fotografije i skulpture), softver, i arhitektonski dizajn. Prava u vezi sa autorskim pravima obuhvataju prava izvođača u svojim nastupima, proizvođača fonograma u njihovim snimcima i emitera u njihovim radijskim i televizijskim programima.[3]

Da bi se obezbedila zaštita za **industrijsku svojinu** na Kosovu, uz nekoliko izuzetaka[4], kreator, odnosno vlasnik, mora da se registruje za zaštitu u vladinoj instituciji koja se zove Agencija za industrijsku svojinu (AIS). Međutim, zaštita **Autorskog prava** dobija se automatski pri fiksiranju dela bez potrebe registracije ili drugih formalnosti.

Vlasnici intelektualne svojine imaju određena prava, uključujući mogućnost da ovlaste i zabrane drugima da koriste njihovu intelektualnu svojinu. Zapravo, prava intelektualne svojine su kao i svaka druga imovinska prava. Oni omogućavaju kreatorima, ili vlasnicima, da imaju koristi od sopstvenog rada ili ulaganja u kreaciju. Ova prava su navedena u članu 27 Univerzalne deklaracije o ljudskim pravima, koja predviđa pravo na dobit od zaštite moralnih i materijalnih interesa koji proizilaze iz autorstva naučnih, književnih ili umetničkih ostvarenja. Pored toga, član 46(5) Ustava Kosova kaže da je „Intelektualna svojina zaštićena zakonom“.

Bez prava intelektualne svojine koja nagrađuje kreativnost i podstiče inovacije, teško da bi pronalazači ili kreatori imali finansijska sredstva ili motivaciju da otkriju nove lekove, kao što su lekovi protiv raka koji spasavaju život, ili da razviju tehnologije koje poboljšavaju kvalitet naših života, kao što su pametni telefoni. Shodno tome, od suštinske je važnosti da vlade i agencije za sprovođenje zakona sprovode prava intelektualne svojine ne samo da bi zaštitile prava vlasnika već i da bi olakšale napredak društva.

Postoji mnogo vrsta zaštićenih objekata intelektualne svojine na Kosovu, svi su navedeni u Aneksu I, ali Kosovska policija će se najčešće susresti sa zaštitnim znakovima i autorskim pravima:

- Žigovi su znakovi, uključujući reči i logotipe, koji identifikuju brendove i omogućavaju potrošačima da razlikuju robu i usluge na tržištu. Primeri žigova su reči „Coca Cola” i „Nike”; i

[3]Svetska organizacija za intelektualnu svojinu – Šta je intelektualna svojina? vvv.vipo.int/about-ip/en/
[4]Poznate tržišne marke su zaštićene bez registracije, član 6bis Pariske konvencije.

- Autorsko pravo štiti kreativna dela kao što su književna dela, filmovi, muzika, umetnička dela, softver i arhitektonsko projektovanje.

Žigovi i autorska prava mogu da rade zajedno da bi pružili zaštitu, na primer:

- Registrovani zaštitni znak štiti ime i simbol automobila; i
- Autorska prava štite softver automobila, vlasnički priručnik, pa čak i slike.

Zaštita intelektualne svojine je vremenski ograničena. Međutim, trajanje zaštite varira za svaki objekat intelektualne svojine. Na primer, autorska prava za pojedinačna dela zaštićena su za života autora plus 70 godina. Nasuprot tome, žigovi, koji su inicijalno zaštićeni 10 godina od trenutka podnošenja prijave AIS, potencijalno mogu biti zaštićeni na neodređeno vreme ako vlasnik nastavi da podnosi zahteve AIS za produženje svakih 10 godina.

1.3 Zločin intelektualne svojine – falsifikovanje i piraterija

Subjekat vrši kršenje prava intelektualne svojine kada koristi intelektualnu svojinu bez dozvole vlasnika. Neovlašćeno korišćenje intelektualne svojine je potencijalno teško krivično delo.

Falsifikovanje i piraterija su povrede prava intelektualne svojine koje se odnose na neovlašćeno korišćenje **žigova i autorskog prava.**

Organizovani kriminalci često krijumčare falsifikovanu i piratsku robu koristeći iste trgovačke rute razvijene za krijumčarenje narkotika i oružja. U stvari, profitabilnost falsifikovane i piratske robe često je veća od profitabilnosti drugih vrsta kriminala, uključujući narkotike.

1.4 Uticaj kršenja prava intelektualne svojine na društvo

Ekonomija

Studija iz 2019. koju su sproveli Kancelarija Evropske unije za intelektualnu svojinu (EUIPO) i Organizacija za ekonomsku saradnju i razvoj (OECD) procenjuje da je međunarodna trgovina falsifikatima i piratima vredna do 509 milijardi dolara godišnje. Međutim, ova procena nije obuhvatila proizvode koji krše autorska prava i koji se proizvode i konzumiraju u istoj zemlji ili ne-materijalne digitalne proizvode. Kad bi se ove vrste proizvoda uključile, studija EUIPO-a i OECD-a smatra da bi vrednost međunarodne trgovine falsifikata i pirata bila nekoliko stotina milijardi dolara više od 509 milijardi dolara.[5]

Studija EUIPO-a i OECD-a naglašava obim finansiranja koje vlade i legitimna preduzeća gube zbog trgovine falsifikatima i piratom. To su sredstva koja bi se mogla iskoristiti za unapređenje društva (npr. izgradnja škola, izgradnja bolnica itd.) i otvaranje radnih mesta.

Zdravlje i bezbednost

Studija EUIPO-a i OECD-a takođe je otkrila da falsifikovanje nije ograničeno na luksuzne predmete, kao što su dizajnerski satovi i odeća, već se proširilo na farmaceutske proizvode, hranu, piće, medicinsku opremu, predmete za ličnu negu, igračke, duvan i delove automobila, ugrožavajući zdravlje i bezbednost potrošoča.

Interpol navodi da „Falsifikovanje žigova i piraterija autorskih prava su ozbiljni zločini intelektualne svojine, koji obmanjuju potrošače, ugrožavaju zdravlje i bezbednost, koštaju društvo milijarde dolara u izgubljenim državnim prihodima, stranim investicijama ili poslovnim profitima i krše prava vlasnika žiga i autorskih prava. Imitacije proizvoda predstavljaju značajnu pretnju po bezbednost potrošača širom sveta. Kupci koji ništa ne sumnjaju dovode svoje zdravlje, pa čak i život, u opasnost svaki put kada koriste falsifikovane proizvode, falsifikovana alkoholna pića i prehrambene proizvode ili putuju automobilima i avionima koji su održavani nestandardnim falsifikovanim delovima."[6]

[5]Trendovi u trgovini falsifikovanom i piratskom robom, EUIPO i OECD, 2019.

[6]Međunarodni koledž za istražitelje zločina u oblasti intelektualne svojine, Interpol, 2016.

Svetska Zdravstvena Organizacija (SZO) tvrdi da „falsifikovani“ lekovi i drugi zdravstveni proizvodi mogu imati štetne efekte po zdravlje pacijenata, uključujući smrt.[7]

Organizovani kriminal

Kancelarija Ujedinjenih Nacija za drogu i kriminal (UNODC) procenila je da je globalno tržište ilegalnih narkotika preko 320 milijardi dolara.[8] Ovo je manje od procene EUIPO-a i OECD-a za vrednost međunarodne trgovine falsifikatima i piratom, koja iznosi do 509 milijardi dolara, i naglašava privlačnost falsifikovanja i piraterije za organizovani kriminal – posebno kada uporedite resurse koje vlade i organi za sprovođenje zakona agencije izdvajaju za borbu protiv nezakonite trgovine narkoticima sa sredstvima dodeljenih za trgovinu falsifikatima i piraterije.

Prema Interpolu, „Transnacionalni organizovani kriminalci generišu stotine milijardi dolara godišnje od proizvodnje i distribucije lažnih (falsifikovanih i piratskih) proizvoda, delimično zbog relativno niskog nivoa rizika i relativno visokog nivoa profita. Postoji sve veća potreba za olakšavanje i koordinaciju međunarodnih napora u borbi protiv ovog kriminala, koji deluje preko međunarodnih granica i ima veoma ozbiljne posledice po javnost.” [9]

1.5 Odricanje odgovornosti

Ovaj dokument ne zamenjuje, niti je namenjen da zameni obaveze međunarodnog prava, nacionalnih zakona ili bilo koje vladine uredbe ili politike.

[7]Međunarodna radna grupa za borbu protiv falsifikovanja medicinskih proizvoda, 2015
[8]Kancelarija Ujedinjenih Nacija za Kriminal i Droge, godišnji izveštaj, 2014.
[9]Међународни колеџ за истражиоце злочина у области интелектуалне својине, Интерпол, 2016.

2. SISTEM INTELEKTUALNE SVOJINE

2.1 Vladine institucije

Uvod

Na Kosovu, borba protiv kršenja prava intelektualne svojine, uključujući falsifikovanje i pirateriju, zahteva koordinaciju više institucija, uključujući:

- Agencija za Industrijsku Svojinu (AIS);
- Kancelarija za autorska i srodna prava (KASP);
- Carina Kosova;
- Tržišna inspekcija;
- Kosovska Policija;
- Tužilački Savet; i
- Sudski Savet.

Agencija za Industrijsku Svojinu

Agencija za Industrijsku Svojinu (AIS) je upravni organ u okviru Ministarstva trgovine i industrije. Sedište je u Prištini i ima sledeće odgovornosti:

- Razvoj postupaka za izdavanje patenata i sertifikata dodatne zaštite;
- Razvijanje postupaka za registraciju žigova, industrijskih dizajna, topografije integrisanih kola, oznake porekla i geografske oznake;
- Sastav i vođenje evidencije propisanih osnovnim zakonom;
- Predlaganje, oblikovanje i izdavanje Službenog glasnika AIS, koji sadrži informacije o zahtevima i dodeljenim pravima na in-

dustrijsku svojinu;
- Doprinosi, razvija i promoviše zaštitu industrijske svojine;
- Iniciranje i predlaganje ratifikacije međunarodnih ugovora u oblasti industrijske svojine;
- Pružanje informacionih usluga u vezi sa objektima industrijske svojine;
- Organizovanje testiranja za ovlašćene predstavnike u oblastima industrijske svojine;
- Priprema predloga za usvajanje zakonskih i podzakonskih akata u oblasti industrijske svojine;
- Saradnja sa drugim organizacijama na sprovođenju zakonskih odredbi koje regulišu industrijsku svojinu; i
- Predstavljanje Republike Kosovo pri međunarodnim organizacijama za industrijsku svojinu.[10]

AIS može pomoći policiji i tužiocima:

- Potvrditi da li je industrijska svojina (npr. trgovačka marka, industrijski dizajn, itd.) zaštićena na Kosovu; i
- Identifikovati vlasnika prava industrijske svojine.

Kancelarija za autorska i srodna prava

Kancelarija za autorska i srodna prava (KASP) je odeljenje u okviru Ministarstva kulture, omladine i sporta. Sedište je u Prištini i ima sledeće odgovornosti:

- Licenciranje organizacija za kolektivno upravljanje;
- Nadzor nad organizacijama za kolektivno upravljanje;
- Oduzimanje dozvola organizacijama za kolektivno upravljanje;
- Pružanje informacija autorima, nosiocima prava i široj javnosti o autorskim i srodnim pravima;

[10]Ministarstvo trgovine i industrije https://kipa.rks-gov.net/page.aspk?id=2,17

- Praćenje razvoja međunarodnog zakonodavstva u vezi sa autorskim pravima, i naknadno izdavanje preporuka Vladi.[11]

KASP može pomoći policiji i tužiocima da kontaktiraju organizacije za kolektivno upravljanje koje mogu:

- Potvrditi da li je neko autorsko ili srodno pravo zaštićeno na Kosovu; i
- Identifikovati vlasnika autorskih i srodnih prava.

Carina Kosova

Carina Kosova je deo Ministarstva ekonomije i finansija. Njihovo sedište je u Prištini, ali takođe imaju kontrolne tačke na:

Aerodromu.	Merdarima.	Qafa Morina.	Zubin Potok.
Bela Zemlja.	Mučibaba.	Čafa e Prušit.	Mitrovica.
General Janković (Hani i Elezit).	Mutivoda.	Vrmica.	Podujevo.
Interevropa.	Peć.	Leposavić.	Kula.[12]
Sedište Priština	Globočica		

Odgovornosti Carine Kosova uključuju sprečavanje uvoza i izvoza robe koja krši prava intelektualne svojine.

Svi carinski službenici su ovlašćeni da postupaju po službenoj dužnosti da presretnu robu za koju sumnjaju da krši prava intelektualne svojine, a pored toga, postoji i posebna jedinica za intelektualnu svojinu u okviru Operativnog istražnog odeljenja Uprave za sprovođenje zakona. Jedinica za intelektualnu svojinu se nalazi u sedištu i njene odgovornosti uključuju:

- Prijem zahteva za akciju od vlasnika prava intelektualne svojine;
- Distribucija prihvaćenih zahteva za PIS za akciju na kontrolnim tačkama;

[11]Ministarstvo kulture, omladine i sporta https://vvv.mkrs-ks.org/?page=2,102
[12]Carina Kosova vvv.dogana-ks.org

- Obuka o intelektualnoj svojini za carinske službenike; i
- Veza sa nosiocima prava intelektualne svojine.

Kosovska carina može policiji i tužiocima da dostavi detalje o pošiljkama koje su presreli i koje sadrže robu koja krši prava intelektualne svojine, uključujući ime uvoznika i/ili izvoznika. Carina Kosova takođe može da proveri istoriju pošiljki na adrese ili entitete, na meti policije i tužioca.

Tržišna inspekcija

Tržišna inspekcija je izvršni organ u okviru Ministarstva trgovine i industrije, koji vrši nadzor tržišta na teritoriji Kosova. Njihovo sedište je u Prištini, ali imaju kancelarije širom Kosova.

Organi tržišne inspekcije imaju nadležnost i resurse da:

- Inspektiraju lokacije povezane sa trgovinom;
- Kontrolišu poslovnu dokumentaciju;
- Inspektiraju robu i usluge;
- Zahtevaju informacije vezane za poslovanje;
- Zapleniti dokaze o krivičnom delu povezanom sa trgovinom;
- Sprečiti puštanje robe i usluga na tržište; i
- Suspendirati poslovanje preduzeća.

Tržišne inspekcije stara se da da roba i usluge koje se proizvode ili koriste u trgovini na Kosovu ne krše prava intelektualne svojine.

Tržišna inspekcija može pomoći policiji i tužiocima da istraže preduzeća za koja sumnjaju da proizvode, uvoze, izvoze ili prodaju robu ili usluge koje krše prava intelektualne svojine.

Kosovska Policija

Kosovska Policija je deo Ministarstva unutrašnjih poslova. Njihovo sedište je u Prištini, ali takođe imaju prisustvo u svim opštinama.

Svi policijski službenici mogu delovati po službenoj dužnosti kako bi sprečili kršenje prava intelektualne svojine. Međutim, žalbe u vezi sa kršenjem prava intelektualne svojine koje ne uključuju onlajn protokole, a koje zahtevaju istragu, treba da budu upućene Odeljenju za privredni kriminal, u Upravi za privredni kriminal i korupciju. Nasuprot tome, pritužbe u vezi sa kršenjem prava intelektualne svojine koje uključuju onlajn protokole treba proslediti Jedinici za sajber kriminal.

Državni tužilac

Državni tužilac je nezavisna institucija sa ovlašćenjima i odgovornošću za krivično gonjenje lica koja su optužena za izvršenje krivičnih dela ili drugih dela utvrđenih zakonom. Obuhvača:

- Osnovno tužilaštvo;
- Apelaciono tužilaštvo;
- Specijalno tužilaštvo; i
- Kancelariju Glavnog državnog tužioca.[13]

Državni tužilac nema posebnu jedinicu za intelektualnu svojinu, međutim, svi tužioci su nadležni da istražuju i krivično gone krivična dela intelektualne svojine, bilo po službenoj dužnosti ili po pritužbi.

Kontakt podaci za svaku od gore navedenih institucija mogu se naći u Aneksu II.

[13]Državni Tužilac https://vvv.rks-gov.net/EN/f46/judiciari/state-prosecutor

2.2 Saradnja

Državni savet za intelektualnu svojinu

U većini zemalja postoji više institucija zaduženih za zaštitu prava intelektualne svojine. Ove institucije često imaju preklapajuće nadležnosti. Shodno tome, na Vladi i institucijama je da razviju model saradnje koji će pružiti efikasnu i efektivnu zaštitu prava intelektualne svojine.

Na Kosovu, Vlada je osnovala Državni savet za intelektualnu svojinu da poboljša saradnju između institucija uključenih u zaštitu i sprovođenje prava intelektualne svojine.

Savet pruža savete i pomoć Vladi i drugim zainteresovanim stranama uključenim u zaštitu i sprovođenje prava intelektualne svojine.

Savet u svom sastavu ima predstavnike institucija navedeni u odeljku 2.1 Vladine institucije, konkretno:

- Agencija za Industrijsku Svojinu (AIS);
- Kancelarija za autorska i srodna prava (KASP);
- Carina Kosova;
- Tržišna inspekcija;
- Kosovska Policija;
- Tužilački Savet; i
- Sudski Savet.

Pored toga, pridruženi članovi Saveta su i predstavnici sledećih institucija:

- Agencija za lekove i medicinske proizvode, za savete o falsifikatima, uključujući falsifikovanim lekovima i medicinskim sredstvima;
- Agencija za veterinu i hranu, za savete o falsifikovanoj hrani i piću;

- Agencija za zaštitu životne sredine, za savete o pitanjima životne sredine; i
- Agencija za upravljanje zaplenjenom ili oduzetom imovinom za savete o oduzimanju imovine od kriminalaca intelektualne svojine.

Operativna grupa za borbu protiv piraterije i falsifikovanja

Vlada je 4. oktobra 2012. godine usvojila **Strategiju protiv piraterije i falsifikovanja,** koji obuhvata period od 2012. do 2016. godine. **Strategiju** je izradio KASP u saradnji sa drugim institucijama nadležnim za sprovođenje prava intelektualne svojine. **Strategija** ima za cilj stvaranje mehanizama za borbu protiv falsifikovanja i piraterije kako bi se poboljšao imidž i ekonomija Kosova.

Strategijom je uspostavljena Radna grupa sa sledećom misijom:

- Promovisati efikasnu saradnju između organa javne vlasti i društvenih i privrednih organizacija u oblasti zaštite autorskih prava;
- Osigurati i koordinisati sprovođenje Strategije i akcionog plana protiv piraterije i falsifikata;
- Razvijati i sprovoditi programe i kampanje za podizanje svesti javnosti; i
- Pripremiti i dostaviti predloge za izradu zakona koji se odnose na sprovođenje autorskih prava

Radna grupa obuhvata sledeće stalne članove:

- Direktor KASP;
- Glavni inspektor Tržišne inspekcije;
- Direktor AIS;
- Šef sektora za intelektualnu svojinu, Carina;
- Šef Sektora za istraživanje privrednih zločina, Policija;
- Šef Sektora za istraživanje kibernetičkog kriminala, policija;
- Predstavnik Državnog Tužioca; i
- Šef Agencije za upravljanje zaplenjenom ili oduzetom imovinom, Ministarstvo pravde.

Pored stalnih članova, na sastanke se mogu pozvati i sledeća tela:

- Izvršni Šef Nezavisne Komisije za Medije;
- Predsednik Odbor Direktora Regulatornog Organa za Poštanske i Elektronske Komunikacije; i
- Druge nezavisne institucije i organizacije.

Takođe je važno napomenuti da sledeće međunarodne organizacije imaju namenske jedinice za intelektualnu svojinu koje bi mogle da pomognu u izgradnji kapaciteta i u prekograničnim istragama:

- Europol;
- Interpol;
- Evropska komisija (generalni direktor za poreze i carinsku uniju);
- Svetska Carinska Organizacija (VCO); i
- EUIPO Opservatorija za kršenje prava intelektualne svojine.

Kontakt detalji svih gore navedenih institucija mogu se naći u Aneksu II.

3. ONLINE KRŠENjE PIS

3.1 Uvod

Kršenja prava intelektualne svojine sve se češće dešavaju u onlajn okruženju. Ova rastuća pretnja ne samo ekonomiji već i zdravlju i bezbednosti potrošača dovela je do nekoliko nedavnih najava politike od strane zainteresovanih vlada i agencija za sprovođenje zakona.[14]

Štaviše, povrede prava intelektualne svojine u onlajn okruženju su raznovrsne, kako u pogledu „sadržaja" povrede, tako i u pogledu tehnoloških sredstava koja se koriste.[15]

3.2 Vrste kršenja online prava intelektualne svojine

Ilegalna distribucija dela zaštićenih autorskim pravima.

Kršenje autorskih prava, ili piraterija, nastaje kad god se zaštićeno delo koristi bez odobrenja nosioca autorskog prava i kada se ova aktivnost ne može smatrati dozvoljenom upotrebom prema jednom od primenjivih izuzetaka ili ograničenja autorskih prava.[16]

U doba interneta, kršenje autorskih prava postalo je lakše, čak i kada se vrši u industrijskim razmerama. Četiri popularne metode koje se koriste za kršenje autorskih prava na mreži su:

- **Streaming (direktan prenos):** ova kategorija uključuje sve sajtove koji prvenstveno dozvoljavaju pristup neovlašćenom sadržaju putem onlajn strimovanja direktno iz veb pretraživača krajnjeg korisnika. Sajtovi obično nude širok spektar sadržaja, koji se mogu direktno pretraživati sa sajta. Neki sajtovi sami hostuju sadržaj koji krši autorska prava, ali većina pruža veze ka spoljnim hostovima (treba napomenuti da je Sud pravde Evropske unije[17] presudio da privremene kopije napravljene

[14]Europolova procena o teškim i organizovanim kriminalom (2017), Carinski akcioni plan EU za borbu protiv kršenja intelektualne svojine (2018-2022), Saopštenje Evropske komisije o akcionom planu za intelektualnu svojinu (COM 2020 760) i zajednička procena pretnje od zločina intelektualne svojine Evropola i EUIPO-a (2019).
[15]„Istraživanje onlajn poslovnih modela koji krše prava intelektualne svojine", EUIPO, 2016.
[16]Zakon br. 04/L-065 o autorskim i srodnim pravima, Poglavlje IV – Ograničenja autorskih prava.
[17]Iako nije članica EU, Kosovo je potencijalni kandidat za članstvo u EU.

na računaru krajnjeg korisnika tokom gledanja striminga predstavljaju, po pravilu, povredu prava na reprodukciju i ne smatraju se izuzetkom za privremene radnje reprodukcije).[18]

- **Preuzimanje:** uključuje sve sajtove koji prvenstveno dozvoljavaju korišćenje neovlašćenog sadržaja putem direktnog preuzimanja preko veb pretraživača korisnika. Sajtovi u ovoj kategoriji obično nude širok spektar sadržaja, koji se mogu direktno pretraživati sa sajta, i preuzeti u celini. Sajtovi retko sami hostuju sadržaj i povezuju se sa drugim sajtovima koji hostuju sadržaj;

- **Stream ripping (cepanje sadržaja):** sajtovi u ovoj kategoriji dozvoljavaju kopiranje, uglavnom audio zapisa, u datoteke za preuzimanje. Ovaj proces se odvija direktno u veb pretraživaču korisnika. Obično korisnik jednostavno treba da unese URL da bi odmah započeo preuzimanje MP3 datoteke. Cepanje sadržaja se obično koristi za cepanje (izdvajanje i preuzimanje) zvuka iz muzičkih spotova, često iz legitimnih izvora. Neki sajtovi dozvoljavaju korisnicima da cepaju (ripuju) video sadržaj i sačuvaju ga kao video datoteku; i

- **Torrent:** portal za preuzimanje torrenta omogućava posetiocu da pretraži bilo koji sadržaj, a zatim preuzme malu datoteku koja pokreće proces preuzimanja celog proizvoda. Korisnici torrent sajtova moraju imati poseban softver, koji se zove torrent klijent, koji se instalira na korisnikovom uređaju. Ovo je peer-to-peer (od korisnika do korisnika) proces preuzimanja, tako da se sadržaj ne prima direktno sa sajta, već dolazi od drugih korisnika torrenta koji dele isti sadržaj. Torrenting može biti javni, gde su svi portali za preuzimanje torrenta otvoreni za korišćenje, ili i privatni, gde samo članovi sajta mogu da se prijave i pristupe sadržaju sajta. Većina privatnih torrent sajtova ima politiku članstva samo po pozivu.

18 Slučaj CJEU C-527/15, Filmspeler.

Distribucija robe koja krši prava intelektualne svojine

Prema podacima Evrostata, oko 71 odsto korisnika interneta u EU kupovalo je na mreži 2019[19] a veliki deo ove trgovine odvijao se preko onlajn pijaca, platformi društvenih medija i veb prodavnica koje rade pod posedbnim imenom domena.

Rast zakonite trgovine na mreži je, međutim, uporedan sa rastom nelegalne trgovine. Shodno tome, prodavci na mreži, platforme društvenih medija i veb prodavnice koriste se ne samo za prodaju legalne robe već i za prodaju nedozvoljene robe kao što su falsifikovana odeća i falsifikovani mobilni telefoni.[20]. Štaviše, veb-sajtovi, koji na prvi pogled izgledaju kao zvanične veb stranice vlasnika određenog brenda, ponekad se ispostavljaju kao lažni sajtovi koji prodaju falsifikovanu robu. Ove veb stranice često koriste nazive domena koji uključuju zaštitni znak treće strane, a sadržaj i dizajn same veb lokacije podsećaju na same vlasnika brenda [21].

Prevara, iznuda i drugi tradicionalni sajber kriminal

Zaštitni žigovi se koriste za dela koja su od samog početka krivična dela, kao što je phishing prevare. Izraz phishing se koristi da opiše zlonamerne pokušaje sticanja novca, osetljivih informacija i/ili instaliranja zlonamernog softvera koji se pokreće putem kontakta sa potencijalnim žrtvama putem e-pošte, objavama na platformama društvenih medija, blogova ili tekstualnih poruka. Pokušaj krađe identiteta (phishing) će se činiti poslat u dobroj nameri i u legitimne svrhe. Štaviše, često će se činiti da ga je poslala poznata kompanija jer adresa pošiljaoca koristi naziv domena, koji može biti zaštitni znak, koji podseća na pravi naziv domena te kompanije.

Napadač će često uspostaviti lažnu veb lokaciju, odnosno veb lokaciju koja je bliska imitacija zvaničnog sajta lažne kompanije ili osobe, zbog čega poseta veb lokaciji ne stvara nikakvu sumnju u zlonamerne okol-

[19]Kao što je navedeno u Digital Agenda Scoreboard, 2019 https://ec.europa.eu/digital-single-market/en/use-internet i dostupno na http://ec.europa.eu/eurostat/statistics-ekplained/ indek.php/E-commerce_statistics_for_individuals

[20]Ilustrativni primeri se mogu naći u Canvas 8 i Canvas 9 u „Istraživanju o onlajn poslovnim modelima koji krše prava intelektualne svojine“, EUIPO, 2016.

[21]Pogledajte „Istraživanje onlajn poslovnih modela koji krše prava intelektualne svojine — Faza 2 Osumnjičeno kršenje žiga u e-prodavnicama koje koriste prethodno korišćena imena domena“, EUIPO 2017.

nosti.[22] Komunikacija o phishing-u obično će sadržati vezu (hyperlink) do pomenutog veb-sajta, ali veb-sajt se može posetiti i nezavisno. Na veb stranici, žrtva će biti zatraženo da otkrije informacije kao što su „ažurirani“ detalji o kreditnoj kartici, „potvrda“ lozinki i slične osetljive informacije.

U zavisnosti od toga šta je korisnik namamljen da radi, takva dela mogu dovesti do jednog ili više krivičnih dela. Prevara je ako napadač uspe da namami žrtvu da plati iznos za nepostojeću obavezu ili nepostojeći proizvod ili uslugu. Ako napad rezultira instaliranjem ransomvare-a (softvera za iznudu), to se može okarakterisati kao iznuda, a instalacija malvera može predstavljati vandalizam.

Sajber-skvoting i druge upotrebe imena domena koje krše prava intelektualne svojine

Sajberskvoting (Cyber squatting) je registracija i upotreba imena domena koji je identičan ili zbunjujuće sličan tuđem žigu i gde je registracija i upotreba u lošoj nameri i sa namerom da se na neki način profitira od registracije i korišćenja.[23]

Varijacija sajber skvotinga je tiposkuatting gde registrant dobije pogrešno napisano ime drugog domena sa namerom da uhvati i iskoristi saobraćaj koji je namenjen pravim veb stranicama.

Oba pojave nastavljaju da se dešavaju u velikom broju,[24] što se može objasniti ne samo implementacijom mnogih novih generičkih domena najvišeg nivoa kao što su .xyz i .top, već i kontinuiranim razvojem načina za sticanje prihoda od takvih registracija kao što su prihodi od ‘plaćanja po kliku’ i prihodi zasnovani na reklamnim šemama.[25]

[22] Vidi Canvas 16 u „Istraživanje onlajn poslovnih modela koji krše prava intelektualne svojine“, EUIPO, 2016
[23] VIPO Definicija sajber skvotinga.
[24]Prijave slučaja ciberskuattinga pri WIPO u naglom rastu na: https://vvv.vipo.int/amc/en/nevs/2020/ciberskuatting_covid19.html
[25]Vidi opis takvih šema prihoda u stavu 5.3.2 u „Istraživanje onlajn poslovnih modela koji krše prava intelektualne svojine“, EUIPO, 2016.

4. ZAKONODAVSTVO

4.1 Uvod

Određeni broj zakonodavnih mera je usvojen na međunarodnom i nacionalnom nivou kako bi se ojačala i uskladila zaštita i sprovođenje prava intelektualne svojine, uključujući na onlajn okruženje. Ove mere sadrže odredbe koje omogućavaju nosiocima prava i agencijama za sprovođenje zakona, kao što je policija, da efikasno primenjuju prava intelektualne svojine.[26]

4.2 Sporazum TRIPS

Sporazum o trgovinskim aspektima prava intelektualne svojine (TRIPS) obavezuje 164 članice Svetske Trgovinske Organizacije (WTO) da obezbede usklađene minimalne standarde koji se odnose na zaštitu i sprovođenje prava intelektualne svojine.[27] Konkretno, TRIPS sporazum sadrži sledeće odredbe vezane za sprovođenje, koje su relevantne ne samo za fizičko već i za onlajn okruženje:

- Član 47 – Pravo na dobijanje informacija o kršenju i prekršiteljima;
- Član 50 – Privremene mere za sprečavanje kršenja i očuvanje dokaza;
- Član 51. - Obustava puštanja u opticaj robe od strane carinskih organa; i
- Član 61. - Krivični postupci i kazne.

4.3 Konvencija o sajber kriminalu

Konvencija o sajber kriminalu, koju su potpisale i zemlje članice EU i zemlje koje nisu članice, uspostavila je niz instrumenata koji su od značaja za sprovođenje prava intelektualne svojine u onlajn okruženju. Konvencija izričito pokriva krivična dela koja se odnose na povredu

[26]Vidi pregled ovih zakonodavnih mera u nastavku u Poglavlju 7.
[27] https://vvv.vto.org/english/docs_e/legal_e/27-trips_01_e.htm

autorskog i srodnih prava, ali ne i druge objekte intelektualne svojine. Međutim, odredbe o kompjuterskom falsifikovanju i prevari mogu indirektno da se odnose zloupotrebu zaštitnih znakova trećih strana u phishing prevara.[28]

4.4 Nacionalno zakonodavstvo

Kosovo je usvojilo niz zakonodavnih instrumenata koji se mogu koristiti za borbu i sprečavanje kršenja online prava intelektualne svojine.

Materijalno zakonodavstvo o intelektualnoj svojini

Materijalni zakoni o intelektualnoj svojini, koje je donela Vlada Kosova, su:

- Zakon br. 04/L-026 o trgovačkim markama (izmenjen Zakonom br. 05/L-040);
- Zakon br. 05/L-058 o industrijskom dizajnu;
- Zakon br. 04/L-029 o patentima (izmenjen Zakonom br. 05/L-039);
- Zakon br. 04/L-065 o autorskim i srodnim pravima (izmenjen Zakonom br. 05/L-047 i Zakonom br. 06/L-120);
- Zakon br. 02/L-098 o zaštiti biljnih sorti;
- Zakon br. 05/L-051 o geografskim oznakama i oznakama porekla; i
- Zakon br. 03/L-165 o utvrđivanju prava i zaštiti topografija integrisanih kola.

[28]https://vvv.coe.int/en/veb/conventions/full-list/-/conventions/treati/185

Materijalno zakonodavstvo o intelektualnoj svojini predviđa način dobijanja zaštite intelektualne svojine i obim ekskluzivnih prava koja uživa nosilac prava, uključujući i činjenicu da nosilac prava može sprečiti treća lica da koriste prava intelektualne svojine bez dozvole.

Većina odredbi u materijalnom zakonodavstvu o intelektualnoj svojini je „tehnološko neutralna“, što znači da se odredbe primenjuju bez obzira na to koja se tehnološka sredstva koriste za proizvodnju zaštićenih kreacija ili koja sredstva se koriste za aktivnost koja krši autorska prava, npr. Član 8(2) Zakona br. 04/L-026 o žigovima navodi da nosilac žiga može zabraniti „upotrebu znaka na poslovnim papirima i u reklamiranju“. Ova odredba se ne odnosi samo na fizičke reklame.

nego i na upotrebu znaka koji krši autorska prava kao imena domena[29] ili AdVord[30].

Materijalno zakonodavstvo o intelektualnoj svojini takođe sadrži mere sprovođenja i pravne lekove, slične TRIPS sporazumu, koji su dostupni nosiocima prava i agencijama za sprovođenje zakona, uključujući:

- Pravo na dobijanje informacija o kršenju i prekršiteljima;
- Privremenim merama za sprečavanje kršenja i čuvanje dokaza.

Zakon o uslugama informacionog društva

Članovi 24 do 26 Zakona br. 04/L-094 o uslugama informacionog društva su takođe od velike važnosti sa sprovođenje prava online intelektualne svojine. Zakon o uslugama informacionog društva navodi odgovornost internet posrednika, što uključuje i njihovu odgovornost u slučajevima kada se njihove usluge koriste za kršenje prava intelektualne svojine. U tom kontekstu, Zakon o uslugama informacionog društva posluje sa tri kategorije posredničkih usluga, i to:

- ‘prosti provod’ – usluga koja se sastoji od prenosa informacija u komunikacionoj mreži od primaoca usluge ili pružanja pristupa komunikacionoj mreži;

[29]CJEU predmet C-657/11, BEST protiv Visis.
[30]CJEU, predmet C-236/08 et al., Google protiv Louis Vuittona

- ‘keširanje’- usluga koja se sastoji od prenosa informacija u komunikacionoj mreži za primaoca usluge, uključujući automatsko, posredno i privremeno skladištenje tih informacija, skladištenje koje se vrši isključivo u svrhu efikasnijeg daljeg prenosa informacija drugim primaocima usluge na njihov zahtev; i
- „hosting“ – skladištenje informacija koje pruža primalac usluge.

Član 28 od Zakon br. 04/L-094 o uslugama informacionog društva zasniva se na principu da posrednici nisu u obavezi da nadgledaju informacije koje šalju ili čuvaju, niti imaju opštu obavezu da aktivno traže činjenice ili okolnosti koje ukazuju na nezakonite aktivnosti. Međutim, ako je posrednik stekao saznanje ili je postao svestan takvih nezakonitih aktivnosti, od posrednika se zahteva da deluje ekspeditivno kako bi uklonio ili onemogućio pristup informacijama ako želi da ostane u okviru odredbi zakona o „sigurnoj luci“.

Krivični zakon

Krivična dela vezana za prava intelektualne svojine navedena u Krivičnom zakoniku (Zakon br. 06/L-074) su:

- Član 289. „Kršenje patentnih prava“;
- Član 290. „Kršenje autorskih prava“;
- Član 291. „Zaobilaženje tehnoloških mera“; i
- Član 292. „Obmanjivanje potrošača”.

Tačne formulacije krivičnih dela su navedene u Aneksu III.

Zakon o carinskom sprovođenju prava intelektualne svojine

Zakon br. 06/L-015 o carinskim merama za zaštitu intelektualne svojine daje proceduralna pravila za carinske organe za sprovođenje prava intelektualne svojine u vezi sa robom koja podlaže carinskom nadzoru ili carinskoj kontroli na granici. Ako se sumnja da takva roba krši prava intelektualne svojine, puštanje robe može biti obustavljeno i

roba može biti zadržana od strane carinskih organa na granici ako su ispunjeni uslovi propisani zakonom.

Zakon br. 06/L-015 o carinskim merama primenjuje se na robu koja je nabavljena i otpremljena sa lokacije van Kosova kupcu unutar Kosova, bez obzira da li je kupovina obavljena onlajn ili na drugi način.

Međutim, sprovođenje u oblasti nelegalne Internet protokol televizije (IPTV), predstavlja specifične izazove. To je zato što, iako set top uređaji krše autorska prava i direktno spadaju u delokrug carinskih radnji, „vanila“ uređaji (tj. set top box uređaji koji još nisu konfigurisani da primaju ilegalni striming) ne krše direktno bilo kakvu intelektualnu svojinu. Ovi uređaji se kao takvi mogu prodati krajnjim korisnicima, koji će ih zatim sami konfigurisati prateći uputstva koja su dali preprodavci ili koja se nađu na forumima i diskusionim grupama. Međutim, „vanila“ uređaji koje proizvode sumnjiva preduzeća mogu predstavljati opasne karakteristike koje ih čine nezakonitim prema bezbednosnim standardima.

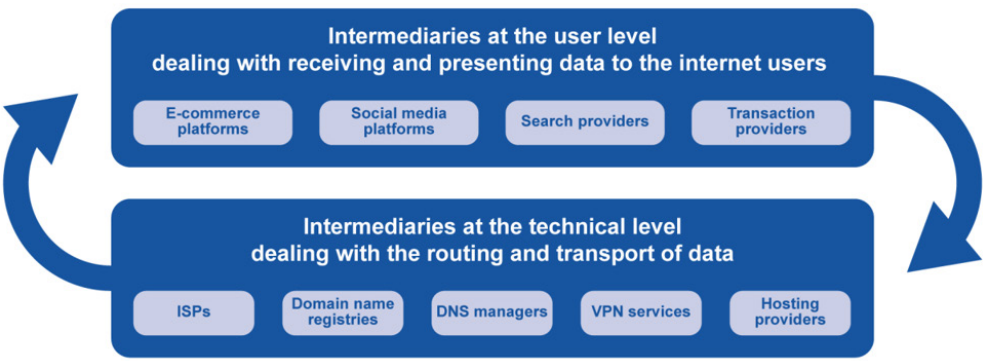
5. ONLINE MERE ZA SPROVOĐENjE PIS

5.1 Uvod

Proizvodnja, marketing, distribucija i prodaja nedozvoljene robe kao što je piratski softver ili falsifikovani brendovi su po definiciji nezakonite radnje. Onako kako je ranije navedeno, važeći zakoni o intelektualnoj svojini obezbeđuju nosiocu prava ekskluzivno pravo na originalne proizvode. Tradicionalno, nosilac prava može da goni proizvođača, distributera ili prodavca robe koja krši prava intelektualne svojine preko suda ili administrativnog sistema. Međutim, takve radnje su komplikovane kada se onlajn okruženje koristi za kršenje prava intelektualne svojine. Shodno tome, nosioci prava i agencije za sprovođenje zakona, uključujući policiju, tražili su druge načine da se bave kršenjem prava intelektualne svojine u prekograničnom onlajn okruženju.

Ovaj razvoj je doveo do situacije u kojoj su različiti onlajn posrednici postali „prirodne tačke kontrole“ kada je u pitanju sprovođenje prava intelektualne svojine.

Online posrednici su stekli važnu ulogu u menadžiranju onlajn ponašanja i sprovođenja prava korisnika interneta. Oni nude prirodnu tačku kontrole za praćenje, filtriranje, blokiranje i onemogućavanje pristupa sadržaju, što ih čini idealnim partnerima za sprovođenje građanskog, administrativnog i krivičnog prava na intelektualnu svojinu.[31]



Slika 1 – Primeri onlajn posrednika[32]

Onako kako je navedeno u Poglavlju 4, određeni broj zakonodavnih mera je usvojen na međunarodnom i nacionalnom nivou kako bi se ojačala i uskladila zaštita i sprovođenje prava intelektualne svojine uključujući u onlajn okruženju. Ove mere sadrže pravne lekove, koje omogućavaju nosiocima prava i agencijama za sprovođenje zakona, kao što je policija, da efikasno primenjuju prava intelektualne svojine, uključujući:

- Dobijanje informacija o računu;
- Blokiranje pristupa veb lokacijama;
- Akcije imena domena; i
- Akcije usmerene na domaćine (hostove).

[31]Citat sa str. 9 u Perel Filmar, Maaian i Elkin-Koren, Niva: Zakonodavstvo u algoritamskom sprovođenju autorskih prava (21. februar 2016.). Pregled Zakona od Stanford Technologi, Predstoji. Доступно на: ССРН: https://ssrn.com/abstract=2607910 ili http://dk.doi.org/10.2139/ssrn.2607910

[32]Studija o zakonodavnim merama u vezi sa kršenjem prava intelektualne svojine na mreži, EUIPO, 2018.

Pored specifičnih zakonskih mera koje su donete radi jačanja i harmonizacije zaštite intelektualne svojine u onlajn okruženju, istražni službenici ne bi trebalo da previde ili zaborave tradicionalne mere, kao što je pranje novca.

5.2 Dobijanje informacija o računu

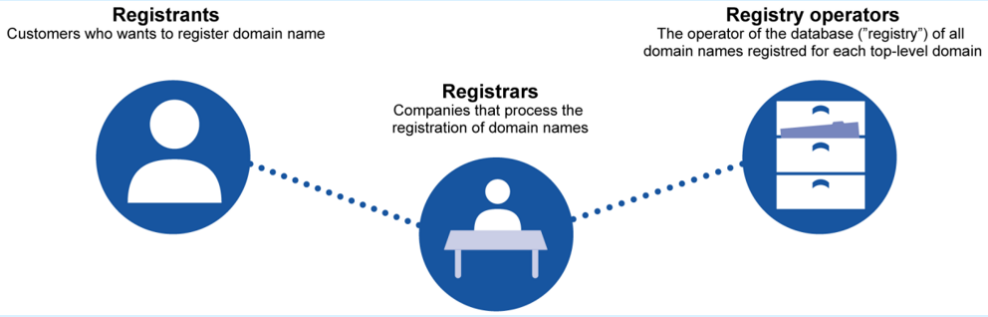
Utvrđivanje identiteta osumnjičenog za povredu prava intelektualne svojine je komplikovano kada je u pitanju onlajn okruženje, pošto identitet osumnjičenog prekršioca nije odmah dostupan.

Kada se strimuje materijal zaštićen autorskim pravima, poput muzike uživo, sportskih događaja i deljenja datoteka koje sadrže dela zaštićena autorskim pravima, kao što su filmovi i muzika, često je moguće utvrditi IP adresu koja je korišćena za aktivnosti koje krše autorska prava. Međutim, potrebne su dalje istražne radnje da bi se utvrdio identitet subjekta koji je koristio određenu IP adresu u izvršenju povrede prava intelektualne svojine. Pored toga, navodni prekršilac može sakriti svoju IP adresu tehničkim sredstvima ili koristiti IP adresu treće strane.

Ako se aktivnost koja krši autorska prava odvija na posebnoj veb lokaciji ili onlajn platformi treće strane, kao što je onlajn tržište ili platforma društvenih medija, možda je moguće identifikovati „račun“ navodnog prekršioca. Iako konkretna identifikacija vlasnika računa nije odmah dostupna trećim licima, takve informacije su dostupne operateru tržišta ili platformi društvenih medija.

Veb stranice koje se koriste za promociju ili distribuciju proizvoda ili usluga za koje se sumnja da krše prava intelektualne svojine treće strane retko – ako ikada – sadrže istinite i pouzdane informacije o strani koja kontroliše veb lokaciju, niti u obliku otiska niti u oblik drugih kontakt informacija. Registri domena održavaju javno dostupnu WHOIS databazu o registrantima, ali tačnost informacija u ovim bazama podataka u velikoj meri zavisi od tačnosti informacija koje daju registranti a

te informaciju nisu uvek istinite i tačne.[33] . Pored toga, u određenim domenima najvišeg nivoa, registranti imena domena mogu da se oslone na korišćenje usluge privatnosti ili proksi usluge, koja prikriva identitet pravog registranta u WHOIS registru.



Slika 2 – Registracija imena domena[34]

Stoga je važno – i u većini slučajeva od suštinskog značaja – utvrditi da li se onlajn posredniku, čije usluge koristi neki od njihovih klijenata za vršenje aktivnosti kršenja prava intelektualne svojine, može naložiti da otkrije informacije o identitetu klijenta koji oni poseduju.

Otkrivanje identiteta vlasnika određenog računa

Pravo na informacije u slučajevima kršenja prava intelektualne svojine propisano je materijalnim zakonodavstvom o intelektualnoj svojini, npr. Članom 100 Zakona br.04/L-026 o trgovačkim markama. Na primer, prema ovoj odredbi, nadležni pravosudni organi mogu narediti svakome ko je umešan u povredu prava intelektualne svojine da otkrije:

[33] Pitanje lažnih kontakt informacija pominje se nekoliko puta u Pregledu Stavova VIPO panela o određenim pitanjima UDRP (Jedinstvena politika za rešavanje sporova u vezi sa imenom domena), Treće Izdanje, dostupno na: <http://vvv.vipo.int/amc/en/domains/search/overviev3.0/>. Videti kao ilustrativni primer, odeljak 6B u predmetu VIPO DNL2017 „Dr. Martens' International Trading GmbH / „Dr. Maertens Marketing GmbH protiv Olge Olge' o nazivu domena <doktermartens.nl>.

[34] Studija o zakonodavnim merama u vezi sa kršenjem prava intelektualne svojine na mreži, EUIPO, 2018.

- Podaci o nazivima i adresama proizvođača, distributera, dobavljača i drugih ranijih vlasnika proizvoda i usluga, prodavaca na veliko i malo; i
- Informacije o proizvedenim, distribuiranim, primljenim i poručenim količinama kao i cenama proizvoda i usluga.

U krivičnim istragama, policija i/ili tužilac mogu podneti zahtev nadležnom pravosudnom organu da naloži internet posredniku da otkrije takve informacije o nalogu, ako zahtev ispunjava opšte proceduralne uslove da bude „opravdan i srazmeran“.

Kontakt informacije o vlasniku određenog naloga

U vezi sa kontakt informacijama za vlasnika određenog računa u onlajn mreži ili platformi, kao što je mreža društvenih medija ili digitalno tržište, moguće je da u parničnom postupku dobiti sudsku odluku kojom se nalaže pružaocu onlajn usluge da otkrije ove informacije.

U krivičnim istragama, policija i/ili tužilac mogu podneti zahtev nadležnom pravosudnom organu da naloži internet posredniku da otkrije takve informacije o računu određenih korisnika.

Kontakt informacije o entitetima koji koriste IP adresu za aktivnosti kršenja prava intelektualne svojine

Što se tiče kontakt informacija o licu ili entitetu koji koristi IP adresu ili stavlja na raspolagane server pod IP adresom koju je obezbedio njegov provajder pristupa, opšta slika je ista kao i za gore navedene informacije o nalogu: na Kosovu je moguće koristiti građanski zakon da dobijete sudsku odluku koja nalaže provajderu onlajn usluge da otkrije ove informacije.

U krivičnim istragama, policija i/ili tužilac mogu da podnesu zahtev nadležnom pravosudnom organu da naloži internet posredniku da otkrije kontakt podatke lica ili pravnog lica koje koristi IP adresu ili čini server dostupan pod navedenom IP adresom od svog provajdera pristupa.

5.3 Blokiranje pristupa veb stranicama

Uvod

Ako se aktivnost kršenja prava intelektualne svojine odvija na ili preko određene veb stranice, efikasan način da se poremete trenutne aktivnosti i spreči njihovo odvijanje u budućnosti je blokiranje pristupa veb stranici. Nalozi za blokiranje su, stoga, postali važni pravni lekovi koji često koriste i nosioci prava i policija/tužilaštvo.

Drugi razlog za efikasnost i popularnost ove mere je taj što su meta naloga za blokiranje različiti provajderi pristupa koji obezbeđuju tehnički pristup internetu. Ovi provajderi su postojeće kompanije koje se mogu odmah identifikovati i samim tim biti predmet pravnog postupka.

Međutim, blokiranje pristupa veb stranice je ograničena i ciljana pravna mera. Veb stranica kao takva će stoga i dalje postojati i može biti dostupna onim korisnicima interneta, čiji provajder pristupa nije obuhvaćen nalogom za blokiranje, uključujući provajdere u drugim jurisdikcijama.

Kosovski sudovi imaju nadležnost samo za pitanja koja su u vezi sa ili imaju uticaj na teritoriju Kosova. Nalozi za blokiranje mogu se, stoga, kao početna tačka izdati samo ako aktivnosti na predmetnoj veb stranici krše ili mogu narušiti prava intelektualne svojine koja su zaštićena na Kosovu.[35]

Odgovornost posrednika

Opšte pravilo o izuzeću od odgovornosti provajdera pristupa je navedeno u članu 24(1) Zakona 04-L/094 o uslugama informacionog društva i podrazumeva da provajder pristupa nije odgovoran za informacije koje šalje njegov kupac, ako su ispunjeni određeni, navedeni uslovi. Međutim, ova odredba „sigurne luke“ ne utiče na mogućnost da sudovi ili upravni organi zahtevaju od pružalaca pristupa da prekinu ili spreče kršenja. Iz toga sledi da su nosioci prava i agencije za sprovođenje

[35]CJEU predmet C-324/09, L'Oreal protiv eBay-a.

zakona u poziciji da podnesu zahtev za zabranu protiv posrednika čije usluge koriste treća lica za kršenje prava intelektualne svojine.

Privremene mere blokiranja

Privremena mera blokiranja je sudski nalog provajderu (pružiocu) pristupa da blokira pristup korisnika određenoj listi veb stranica. Pokazalo se da su ove zabrane efikasnije od naređenja ili zahteva provajdera usluga hostinga da uklone veb stranice koje čine kršenje. To je zato što operateri ovih veb stranica mogu lako da pređu na drugu uslugu hostovanja i da ponovo pređu na hostove koji se nalaze u udaljenim jurisdikcijama koji ne odgovaraju na zahteve za obaveštenja i uklanjanje. Nasuprot tome, zabrane blokiranja provajderima pristupa Internetu čine veb lokaciju nedostupnom korisnicima u zemlji u kojoj je izdat nalog bez obzira na host gde se veb stranica nalazi.[36]

Dinamične mere blokiranja

Privremene mere blokiranja može navesti ne samo ime domena i IP adresu veb-sajta(-ova) za blokiranje pristupa, već i sva dodatna imena domena pod kojima su počinjena kršenja istih prava. Takvi „dinamični" nalozi proširuju efikasnost blokiranja pristupa veb stranici i omogućavaju sprečavanje budućih kršenja.

Mere blokiranja za direktne prenose

Privremene mere blokiranja može da funkcioniše tako što zahteva od provajdera pristupa Internetu da blokiraju pristup korisnika serverima na kojima se nalaze strimovi sportskih događaja uživo, koji krše autorska prava. Takozvane naredbe za blokiranje „uživo" prenosa su posebno efikasne u borbi protiv nezakonitih IPTV-a, jer ciljaju posebno servere koji emituju ilegalni sadržaj tokom emitovanja događaja uživo.

Privremene mere deindeksiranja

[36]CJEU u UPC Telekabel (Predmet C-314/12) je utvrdio da je ova vrsta zabrane kompatibilna sa pravom EU, pod uslovom da ne lišava internet korisnike mogućnosti zakonitog pristupa dostupnim informacijama i ima efekat sprečavanja (ili otežavanja) pristup sadržaju koji krši autorska prava.

Ove privremene mere zahtevaju od pretraživača da deindeksiraju veb lokacije koje krše autorska prava, tako da se veze (link) do tih veb stranicama ne pojavljuju na listi rezultata pretrage.

5.4 Radnje imena domena

Uvod

Kao što je pomenuto u Poglavlju 3, imena domena igraju ključnu ulogu u različitim vrstama kršenja prava intelektualne svojine u onlajn okruženju, uključujući sajber skvoting i phishing prevare.

Imena domena se takođe koriste kao internet adrese za veb stranice koje sadrže sadržaj koji krši autorska prava, uključujući veb stranice sa linkovima ka nelegalnom digitalnom sadržaju, veb stranice koje doprinose video strimovanju i veb stranice sa torrent sadržajem.[37] U ovim situacijama nije ime domena samo po sebi ono što krši autorska prava, već sadržaj veb stranice.

Ako se ime domena koristi za aktivnosti kršenja prava intelektualne svojine, sud može naložiti prekršiocu da prekine aktivnosti koje krše prava pod imenom domena, kao što sud može izreći odštetu, novčane kazne i druge sankcije, bilo civilne, administrativne ili krivične.

U poslednjih nekoliko godina, agencije za sprovođenje zakona u nekoliko zemalja dobile su sudske naloge u kojima je zaplenjen veliki broj imena domena. Najznačajnija je „Operacija na Our Sites“ koju koordinira Europol[38] i zaplenila je 10.000 imena domena koji su korišćeni kao internet adrese za veb lokacije koje krše prava intelektualne svojine.

Pravni osnov koji se primenjuje za oduzimanje imena domena su obično opšte odredbe o oduzimanju. Međutim, pošto ime domena nije fizička roba koja se može zadržati, zaplena podrazumeva nalog da se nazivi domena ne budu preneti, izbrisati ili na drugi način pustiti u opticaj.

[37]Vidi opis poslovnih modela opisanu u Kanvasu 21, 22, 23 i 25 „Istraživanja onlajn poslovnih modela koji krše prava intelektualne svojine“, EUIPO, 2016.
[38]https://vvv.europol.europa.eu/activities-services/europol-in-action/operations/operation-in-our-sites-ios

5.5 Akcije usmerene na domaćine (hostove)

Uvod

Kako je pomenuto u Odeljku 5.1, različiti onlajn posrednici su postali „prirodne tačke kontrole“ kada je u pitanju sprovođenje prava intelektualne svojine. Ovo posebno važi za one posrednike koji deluju kao domaćini (hostovi) – kompanije koje upravljaju onlajn platformama sa ili na kojima se odvijaju aktivnosti kršenja prava intelektualne svojine. Primeri hostova su digitalna tržišta[39] i platforme društvenih medija.[40]

Odgovornost posrednika

Opšte pravilo o izuzeću od odgovornosti provajdera hostinga je navedeno u članu 26(1) Zakona 04-L/094 o uslugama informacionog društva i odredba podrazumeva da provajder nije odgovoran za informacije koje skladište njihovi kupci, ako su ispunjeni određeni uslovi. Međutim, ova odredba „sigurne luke“ ne utiče na mogućnost da sudovi zahtevaju od pružalaca hostinga da prekinu ili spreče kršenja PIS-a.

Shodno tome, postoji nekoliko postupaka koje se potencijalno mogu preduzeti protiv posrednika koji deluju kao hostovi, uključujući:

- Uklanjanje prodaje ili reklama za robu koja krši prava intelektualne svojine; i
- Blokiranje računa koje se koriste za distribuciju robe i usluga kojima se krše prava intelektualne svojine.

[39]Vidi Kanvas 8 marketinške robe ili digitalni sadržaj na veleprodajnom tržištu trećih strana (B2B) u „Istraživanju o onlajn poslovnim modelima koji krše prava intelektualne svojine. Faza 1 Pregled onlajn poslovnih modela koji krše prava intelektualne svojine“, EUIPO, jul 2016.

[40]Vidi Kanvas 9, Prodaja neoriginalne robe putem mreža društvenih medija, u „Istraživanju poslovnih modela na mreži koji krše prava intelektualne svojine. Faza 1 Pregled onlajn poslovnih modela koji krše prava intelektualne svojine“, EUIPO, jul 2016.

Uklanjanje prodaje ili reklama za robu koja krši prava intelektualne svojine

„Uklanjanje“ je na samom početku postupak u kojem treća strana može da podnese žalbu („obaveštenje“) operateru onlajn tržišta, platforme društvenih medija ili slične platforme i zatraži od operatera platforme da ukloni („ukloni“) proizvod koji treće lice nudi na prodaju ili oglašava na tržištu. Tada je individualni operater dotične platforme taj koji odlučuje da li će prihvatiti ili odbiti žalbu, odnosno da li će ukloniti listu koja krši autorska prava ili ne.

Takvi postupci „Obaveštenja i uklanjanja“ sprovode se i primenjuju na većini digitalnih tržišta, kao i na većini platformi društvenih medija i one su sastavni deo uslova i odredbi platforme. U mnogim zemljama, postupci„obaveštenja i uklanjanja“ se svakodnevno koriste u ogromnom broju i smatraju se efikasnim alatima kada je u pitanju sprovođenje prava intelektualne svojine u digitalnom okruženju.[41]

Međutim, ako operater odbije da reaguje, ne samo da postaje odgovoran za povredu prava intelektualne svojine, već je takođe moguće podneti zahtev za sudski nalog da se operater primora da deluje.

Blokiranje računa koje se koriste za distribuciju robe i usluga kojima se krše prava intelektualne svojine

Pored mogućeg uklanjanja stvarnih ponuda ili oglasa o prodaji, treća strana može uložiti žalbu operateru onlajn tržišta, platforme društvenih medija ili sličnim platformama i zatražiti od operatera platforme da blokira ili suspenduje račun koji se koristi za distribuciju robe i usluge kojima se krše prava intelektualne svojine. Tada je individualni operater dotične platforme taj koji odlučuje da li će prihvatiti ili odbiti žalbu.

Međutim, ako operater odbije da reaguje, ne samo da postaje odgovoran za povredu prava intelektualne svojine, već je takođe moguće podneti zahtev za sudski nalog da se operater primora da deluje.

[41] „Strategija jedinstvenog digitalnog tržišta za Evropu“, Saopštenje Evropske Komisije, 6. maj 2015, ЦОМ(2015) 192 final, Odeljak 3.3.2., str. 12; „Komunikacija o onlajn platformama i jedinstvenom digitalnom tržištu“ {COM(2016) 288}, odeljak 5.II), str. 7 ff.

5.6 Pranje novca

Kršenja prava intelektualne svojine u komercijalnim razmerama se po definiciji odnose na zaradu novca i, kao što je navedeno u odeljku 1.4, novac uključen u aktivnosti kršenja prava intelektualne svojine je ogroman.[42]

Pristup „prati novac“ smatra se važnim sredstvom za sprečavanje i borbu protiv nezakonitih aktivnosti, uključujući kršenje prava intelektualne svojine. Ovakav pristup ne samo da omogućava vlastima da identifikuju, zaplene i oduzmu novac, već omogućava ili bar olakšava identifikaciju počinilaca.

Švedski slučaj SveFilmer[43] ilustruje kako se istražni pristup „prati novac“ i mere za sprečavanje pranja novca mogu koristiti za istragu kršenja prava intelektualne svojine. U slučaju SveFilmer-a, striming nelicenciranih audio-vizuelnih dela i prateće aktivnosti pranja novca bili su centralni u istrazi. Glavni optuženi je kasnije optužen i za kršenje autorskih prava i za pranje novca. Slučaj je okončan u prvostepenom postupku utvrđivanjem krivice zbog čega je izrečena kazna zatvora i isplata štete nosiocima prava.

Član 302 Krivičnog zakonika Kosova i Zakon o sprečavanju pranja novca i finansiranja terorizma utvrđuje pranje novca kao krivično delo na Kosovu.

[42]Trendovi u trgovini falsifikovanom i piratskom robom, EUIPO i OECD, 2019
[43]Predmet Regionalnog suda u Varbergu br. T-1463-15 i Apelacioni sud u Goti, predmet br. B 1565-17, 22. februar 2018.

6. MERE DOBROVOLjNOG IZVRŠENjA

6.1 Uvod

Pošto se od nosilaca prava i agencijE za sprovođenje zakona ne može očekivati da istraže i pokrenu pravne radnje protiv svakog kršenja prava intelektualne svojine na mreži, oni su tražili druga rešenja za ometanje aktivnosti kršilaca prava intelektualne svojine, kao što su prakse dobrovoljne saradnje (PDS, ili VCP - Voluntary Collaboration Practices).

PDS-i imaju za cilj da poštuju i zakon i osnovna prava građana, dok se bore protiv kršenja prava intelektualne svojine, uključujući online povrede prava intelektualne svojine. PDS se obično sastoje od kodeksa ponašanja i praksi koji imaju za cilj uklanjanje sajtova koji krše prava intelektualne svojine, uklanjanje reklama sa sajtova koji krše prava intelektualne svojine ili uskraćivanje sajtovima koji krše prava intelektualne svojine pristup sistemima online plaćanja.

PDS obično imaju određene zajedničke karakteristike, posebno:

- Oni su dobrovoljni i stoga ne izriču prinudne sankcije za nepoštovanje obaveza i postupka koje su njima predviđene;
- Oni uspostavljaju preventivne i/ili proaktivne mere u cilju zabrane ili otkrivanja

  povrede intelektualne svojine; i
- Većina PDS-a ne snosi nikakve troškove ili naknade za zainteresovane strane.

6.2 Primer mere dobrovoljnog izvršenja

Na primer, u Austriji, nakon konsultacija sa nosiocima prava, austrijska reklamna industrija (Verberat) je razvila PDS kao deo svog samoregulatornog etičkog kodeksa za austrijsku reklamnu industriju.

Prema ovom austrijskom PDS-u, postavljanje reklama u nezakonitom okruženju je protivno načelima reklamiranja, kao na primer na stranicama koje krše autorska prava.

U praksi, po prijemu žalbe nosioca prava na reklamu, Verberat vrši preliminarno ispitivanje. Ako Verberat smatra žalbu opravdanom, podnosi zahtev nadležnoj reklamnoj agenciji ili oglašivaču da promeni oglas u roku od tri radna dana. Zahtevi Verberat-a nisu pravno obavezujući i Verberat ne može sankcionisati kršenje autorskih prava.

Ako oglašivač pristane da ukloni oglas, ne preduzimaju se nikakve dalje radnje. Međutim, ako oglašivač smatra pritužbu nosioca prava neosnovanom, žalba i razlozi za neslaganje oglašivača se upućuju (reklamnom) Malom senatu na odluku.

Ogromna većina oglašivača ukloni istaknutu reklamu bez sazivanja Malog senata, čime se prekršiocu oduzima prihod.[44]

Na Kosovu, nosioci prava i agencije za sprovođenje zakona, uključujući policiju, treba da rade sa posrednicima na razvoju PDS-a kako bi se sprečilo kršenje prava intelektualne svojine na mreži.

[44]Studija o praksama dobrovoljne saradnje u rešavanju onlajn kršenja, EUIPO, 2016.

7. ISTRAGE PUTEM INTERNETA

7.1 Uvod

Istrage obično pokreću nosioci prava koji ponekad daju organima vlasti kompletan dosije privatne istrage, što uključuje izjave, fotografije i dokumentaciju iz vršenja nadzora.

Važnost sveobuhvatnog doprinosa nosilaca prava mora da bude posebno naglašena, jer to pomaže da se obezbedi policijski rad visokog učinka kroz efikasno i delotvorno raspoređivanje resursa. Na primer, ako se nosioci prava unapred dogovore o strukturi, pristupu i formatu istražnog dosijea, to će za rezultat imati koordinisan i homogenizovan pristup, što pak omogućava agencijama za sprovođenje zakona da sprovedu efikasniju i efikasniju istragu.

Pored toga, kao što je već pominjano, da bi se prevazišle zakonske ograničenosti u vezi sa zakonima o intelektualnoj svojini, istražitelji treba da imaju na umu da se mogu počiniti i druga krivična dela koja često predstavljaju prilike za krivično gonjenje bez složenih poteškoća u pribavljanju izjava o pravima itd. Na primer, kršenja prava intelektualne svojine mogu da obuhvataju i sledeća krivična dela:

- Pranje novca;
- Utaja poreza;
- Kriminalna zavera;
- Reketiranje;
- Prevara (i zavera da se počini prevara); i
- Carinski prekršaji.

Bez obzira na sve, kritično važan prvi korak u istrazi o kršenju prava intelektualne svojine na Internetu – kao i u svakoj drugoj krivičnoj istrazi – jeste sticanje znanja o relevantnom zakonodavstvu i razmatranje onoga što je potrebno da bi se svako potonje krivično gonjenje dovelo do uspešnog završetka.

Dalje, u vezi sa kršenjem prava intelektualne svojine na Internetu postoje tri glavne metodologije koje istražitelji mogu da primenjuju, bilo odvojeno ili u kombinaciji:

- „Pratite tok“;
- „Pratite novac“; i
- „Pratite piksel“.

7.2 Istraga tipa „Pratite tok“

„Pratite tok“ se odnosi na identifikaciju stvarnog piratskog sadržaja od potrošača sve do njegovog izvora. Težak je zadatak istražiti i sačiniti mapu svake konkretne kriminalne mreže od početka do kraja (celokupan tok) jer može uključivati ne samo mapiranje čitavog ekosistema lavirinta ovih pirata, lavirinta koji međusobno povezuje mnoštvo aktera - legalnih i ilegalnih, već i zaobilaženje tehnologija za anonimnost koje mnogi prestupnici koriste da sakriju tragove svojih nezakonitih aktivnosti za isporuku piratskog sadržaja. Čak i kad je tako, nisu svi prekršioci prava intelektualne svojine jednako vešti na računaru ili dovoljno pažljivi da eliminišu tragove i efikasno sakriju svoje digitalne otiske. Shodno tome, istražitelji bi trebalo da nastoje da pažljivo prikupe različite tragove i indikatore (bilo u digitalnom ili u fizičkom obliku) iz mnogih izvora, kao i da obrate pažnju na paralelne istrage koje se mogu pojaviti.

7.3 Istraga tipa „Pratite novac“

Finansijska dobit je dominantni motiv u mnogim aktivnostima kompjuterskog („sajber“) kriminala, a kršenja prava intelektualne svojine nisu izuzetak. Kao rezultat ovoga, kada su akteri neuhvatljivi, još jedan potencijalni trag je trag novca. Prateći trag novca može se opisati cela operacija kršenja prava intelektualne svojine. Dok kriminalci pokušavaju da sakriju svoj identitet i svoje digitalne otiske, novac koji razmenjuju često je teško sakriti i teško je odrediti ga se. Iako elektronske, digitalne, virtuelne i kripto valute (kao što su Bitcoin i Monero) potencijalno mogu ponuditi viši nivo tajnosti i anonimnosti, izvršene transakcije se u principu i dalje mogu pratiti.

Dalje, kada se koriste provajderi za plaćanje, kao što su kreditne kartice ili „PayPal“, detalji povezanih naloga mogu se otkriti vlastima, u skladu sa nacionalnim zakonodavstvom. Pored toga, bankarskom organu može biti naloženo da zamrzne dotični račun. Od tog trenutka, svaki pristup ili pokušaj pristupa novcu mogao bi da otkrije vredne tragove i dokaze, kao što je IP adresa koja se koristi za prijavu na Internet stranicu, zatim provajder plaćanja ili druge službe i usluge.

U središtu svake finansijske istrage leži identifikacija transakcije i analiza plaćanja za nezakonite usluge. Zaplenjeni digitalni uređaji iz operacija za sprovođenje zakona mogu da otkriju dokaze o pretplatama koje vode do informacija o klijentima, uključujući ovde i to kako i kada su ilegalni akteri platili svoje usluge i konačnu cenu pruženih usluga. Analiza e-mail zapisa i drugih digitalnih tragova može da dovede do identifikacije bankovnih računa, plaćanja usluga, kretanja novca i da pruži dokaze za dobijanje podataka o poslovnom prometu.

Osnovni princip koji treba imati na umu jeste da, iako je novac motiv, istražitelji treba da pokušaju da ispitaju mehanizam prenosa novca koji se koristi i da pokušaju da ga poremete. Ometanjem toka novca, uključeni akteri ponekad mogu da budu primorani na očajničke poteze, što potencijalno može da poveća šanse za grešku. Stoga je „Pratite tok novca“ korisna istraga i može da dovede do identifikacije osumnjičenih ili osoba od interesa.

Ukratko, postoje dva pitanja koja, ako se odgovore, mogu da otkriju veliki deo mreže kršenja prava intelektualne svojine:

Pitanje „Ko je ovo platio?“:

- Ko je platio naziv Internet domena? (Ove informacije su dostupne u domenu najvišeg nivoa);
- Ko je platio uslugu hostinga? (Ove informacije su dostupne kod provajdera hostinga); i
- Ko je platio server za sistem imena domena (DNS)? (Ove informacije su dostupne kod dobavljača DNS usluga).

Pitanje „Gde ide novac?“:

- Ako su na Internet stranici pirata instalirani procesori za plaćanja (PayPal, Visa, itd.), ove informacije su dostupne u kompaniji koja je zadužena za upravljanje transakcijama kreditnim karticama; i
- Ako je u aplikaciji prekršioca instalirano mobilno plaćanje, ove informacije mogu da se dobiju od provajdera mobilne telefonije.

1.4 Istraga tipa „Pratite piksel“

Termin „Pratite piksel“ se koristi da obuhvati sve tehnologije vezane za oglašavanje na mreži, koje su sada sastavni deo usluga zasnovanih na Internetu. Termin „piksel“ u svetu društvenih mreža i Internet marketinga odnosi se na tehnologije koje se koriste za sprovođenje marketinških Internet kampanja, uključujući ovde i mogućnosti izveštavanja o njihovoj efikasnosti, kao i za distribuciju generisanog prihoda među uključenim stranama. Pošto takve aktivnosti zahtevaju identifikaciju korisnika, ova linija istraživanja daje veliku podršku i dopunu metodologijama „Pratite tok“ i „Pratite novac“.

Internet stranice i mobilne aplikacije koje krše prava intelektualne svojine su uglavnom podržane oglasima, gde su neki usvojili model pretplate, dok drugi prihvataju donacije korisnika. Shodno tome, nezakoniti prihodi mogu da dođu ne samo od pretplata i donacija, već u obliku prihoda od oglašavanja, generisanih uplatama po kliku, plaćanja po preuzimanju i plaćanja u vezi sa reklamnim površinama („banerima“) prikazanim na Internet stranicama.

Ovaj proces olakšavaju posrednici u oglašavanju, a oglasi mogu biti vidljivi na stvarnim Internet stranicama, iskačući u zasebnim karticama kada korisnik klikne na određene delove te Internet stranice ili putem „punjenja piksela“ – što se postiže uključivanjem malog oglasa. Razmaci (širine 1x1 ili 5x5 piksela) na vrhu ili dnu Internet stranice.

Još jedna nelegalna praksa je takozvano „slaganje oglasa jedan na drugi“, gde se više reklama postavlja jedna na drugu u jednom oglasnom prostoru. Kroz ovu agresivnu praksu, pirati ostvaruju veći profit, čak i u slučaju „besplatnih“ usluga za kršenje prava intelektualne svojine.

7.5 Najbolja praksa

Uvod

Sve veće prisustvo i korišćenje društvenih mreža i informacija otvorenog koda, zajedno sa njihovom potrebom da se reklamiraju i dopru do što većeg broja krajnjih korisnika, primoravaju prekršioce prava intelektualne svojine da izlože svoje podatke na mreži. Prikupljanje informacija o prekršiocima prava intelektualne svojine u istrazi na mreži ne može se smatrati za jednostavan zadatak. Sprovođenje istraga na mreži zahteva pripremu i određeni stepen sofisticiranog prethodnog planiranja kako bi se obezbedilo da se zadatak obavi na efikasan i fokusiran način, uz stalno prisutnu svest o tragovima koje istražitelj ostavlja za sobom.

Iako ne postoji savršeno primenjiva kontrolna lista tipa „jedna veličina za sve“, zbog velike složenosti i raznolikosti svakog slučaja postoje neka ključna razmatranja koja bi istražitelj trebalo da ima u vidu u fazi pre planiranja Internet istrage:

- Zaštitite svoju anonimnost;
- Pretražujte naširoko, vodite evidenciju i pravite rezervne kopije da biste učvrstili svoje nalaze;
- Dokumentujte SVE otkrivene dokaze na mreži odgovarajućim vremenskim oznakama;
    - Snimak ekrana svih dokaza sa jasnom identifikacijom vremena za svaku pojedinačnu stavku;
    - Napravite kopije Internet stranica;
- Zabeležite svaki trag (nadimak, e-mail, ID korisnika) koji se istražitelju „nudi“ na Internet stranici koja krši autorska prava, sa jasnim vremenskim oznakama;

- Dobro upoznajte okruženje pod istragom, da biste se dobro upoznali sa terminologijom koju koriste prekršioci prava intelektualne svojine, opcijama koje Internet stranice-sajtovi nude, itd; i
- U prekograničnim slučajevima, tražite međunarodnu pomoć.

Anonimnost

Kako društvene mreže i izvori informacija na Internetu ili omogućavaju ciljevima da vide ko ih istražuje ili daju neke očigledne naznake o tome ko gleda njihove informacije, istražitelji bi trebalo da skrivaju svoj identitet dok obavljaju istraživanje na mreži. Ovo su neke od radnji koje mogu da izvrše istražitelji kako bi sproveli anonimnu istragu na Internetu:

- Kreirajte novi e-mail nalog koji će se koristiti za istrage kada je to potrebno. Iako je anonimnost važna, istražitelji bi trebalo da počnu da stvaraju odgovarajuću ličnost koja nema nikakve veze sa njihovim identitetom. Ovaj e-mail nalog ne bi trebalo ni na koji način da upućuje na identitet istražitelja. Neki saveti za postizanje ovoga su sledeći:

    - Nemojte davati nikakve informacije koje bi potencijalno mogle da identifikuju pravi identitet istražitelja. Nema pravih nadimaka, datuma rođenja, brojeva znački, geografskih indikatora, sportskih timova ili imena dece u odeljku „User ID“;
    - Ne odgovarajte istinito na bezbednosna pitanja;
    - Nemojte povezivati ovaj e-mail nalog sa drugim legitimnim e-mail adresama;
    - Vodite evidenciju o tome šta je poslato i nemojte da zaboravite lozinku.
- Kreirajte nove naloge na društvenim mrežama povezane sa novim kreiranim e-mail nalogom. Kada su u pitanju tajni profili na društvenim mrežama, istražitelji bi trebalo da znaju (a) ko koga može da vidi preko ovih platformi; i (b) šta mogu da pronađu pregledajući ciljane naloge.
- Razmislite o korišćenju VPN rešenja. Korišćenje VPN rešen-

ja i usluga tokom sprovođenja istrage na mreži omogućava istražiteljima da se povežu na svoju mrežu preko VPN tunela i da u isto vreme izađu sa druge lokacije širom sveta. Na primer, nordvpn.com VPN nudi izlazne čvorove u preko 60 zemalja širom planete. Nažalost, većina VPN usluga i rešenja nije besplatna. Istovremeno, ne preporučuje se da istražitelji koriste besplatna proksi/VPN rešenja. Istražitelji uvek treba da imaju na umu da čak i ako je njihov saobraćaj šifrovan kako prolazi kroz VPN čvorove, osim ako ne postoji „end-to-end“ enkripcija, oni polažu određeni nivo poverenja u izlazni čvor koji dešifruje njihov saobraćaj onako kako izgleda u običnom tekstu.

- Razmislite o korišćenju TOR-a za anonimnost. TOR („The Onion Router“) je mreža čvorova koju je dizajnirala Laboratorija za pomorska istraživanja Sjedinjenih Država za američku mornaricu. Ova mreža čvorova se koristi za prosleđivanje saobraćaja korisnika do odredišnog hosta koristeći šifrovanje i rutiranje kroz nasumične putanje. TOR radi samo sa saobraćajem protokola kontrole prenosa (TCP) i samo odredišni host može da vidi IP adresu izlaznih čvorova dok izvorna IP adresa hosta koji je inicirao komunikaciju ostaje neotkrivena. Za sada je dobro, ali pošto je lista TOR izlaznih čvorova javno dostupna ako cilj istrage blokira pristup sa IP adresa koje dolaze za TOR čvorove, istražitelji neće moći da dođu do svog cilja. Još jedan ključ koji treba uzeti u obzir dok istražujete na Internetu putem TOR-a je da iako izvorna IP adresa istražitelja ostaje skrivena, njihov niz korisničkog agenta će i dalje biti prosleđen Internet stranici koja krši prava intelektualne svojine. Dakle, ako se, na primer, istražitelji pretvaraju da govore ruski, a njihov niz korisničkog agenta otkriva da je njihov jezik „EN-US“, to bi moglo izazvati sumnje. Dalje, ako se istražitelji pretvaraju da su locirani u SAD, ali su redovno na mreži s vremena na vreme u skladu sa nekim ko se nalazi u istočnoj vremenskoj zoni, to bi takođe moglo da skrene pažnju na metu; i
- Razmislite o korišćenju virtuelne mašine za sva istraživanja na mreži. Virtuelne mašine (ili VM) su aplikacije za virtuelizaciju na više platformi koje imitiraju ponašanje drugog (sekundarnog) računara u mašini istražitelja. Osim što omogućavaju ko-

risnicima da pokreću više različitih operativnih sistema na istom računaru – uz veliku fleksibilnost u konfiguraciji podešavanja i personalizaciji instaliranog softvera ili alata treće strane – VM takođe nude bezbednosne prednosti, posebno kada istražuju rizične aplikacije, datoteke i Internet stranice. Jednom u VM okruženju, istražitelji takođe imaju koristi od mogućnosti da kreiraju snimke na nivou sistema za oporavak ili vraćanje VM slika i usluga na zahtev.

8. OBAVEŠTAJNI PODACI IZ OTVORENIH IZVORA

8.1 Uvod

Obaveštajni podaci iz otvorenih izvora (OSINT) se odnosi na praksu prikupljanja informacija iz javno dostupnih izvora koji ne zahtevaju prikrivene ili tajne metode prikupljanja. Iako je OSINT relativno nova aktivnost za agencije za sprovođenje zakona, velike organizacije i agencije (kao što su Interpol i Europol) sistematski promovišu i ulažu u OSINT kroz radionice, seminare i druge aktivnosti, zbog njegovog značaja za krivične istrage.

Naročito u istragama o kršenju prava intelektualne svojine na mreži, OSINT je ključna i integralna aktivnost, a ne zavrtnje u procesu istrage. Ovo je očigledno iz ekosistema kršenja prava intelektualne svojine, gde suština kršenja zahteva da većina aktera ili ima interakciju koristeći Internet ili koristi osnovne internet infrastrukturne usluge za isporuku sadržaja koji krši autorska prava. Ovo poslednje predstavlja poseban izazov jer akter ne mora nužno da bude aktivno uključen u aktivnost koja krši autorska prava, slično kao na primer poštanska služba koja isporučuje ilegalne narkotike. Ipak, OSINT će morati da obuhvati sve relevantne informacije i potvrdi ih kako bi se omogućile naknadne tehničke ili pravne radnje.

Prilikom sprovođenja istrage zasnovane na OSINT-u treba poštovati principe Udruženja glavnih policijskih službenika Ujedinjenog Kraljevstva (ACPO). Iako OSINT ne podrazumeva nužno direktan pristup sistemima osumnjičenog, istražitelj će morati da poseduje dobro razumevanje osnovnih tehnologija na Internetu koje omogućavaju

određena delovanja kao što su DNS, autonomni sistemi, protokoli, standardi za kodiranje „strimova“, mreže za isporuku sadržaja, da pomenemo samo neke. Posebno je naglašena identifikacija lokacije usluga, domena i IP adresa, jer oni mogu biti sakriveni, zamaskirani i učinjeni anonimnim - ne nužno da bi se izbeglo otkrivanje, već da bi se pružio potreban nivo usluge, kao što je opisano u slučaju „Cloudflare“ i drugih usluge zaštite privatnosti, na primer.

Detaljno evidentiranje radnji i vremena (ACPO princip 3) je od najveće važnosti u OSINT-u. Traženjem i prikupljanjem informacija iz eksternih i potencijalno nepouzdanih izvora, istražitelj treba da shvati da su sistemi u osnovi složeni i dinamični i da se kao takvi njihovo stanje može značajno promeniti tokom istrage. Na primer, u pristupu „Pratite tok“, pošto sadržaj koji krši autorska prava može biti isporučen preko mreže za isporuku sadržaja (CDN), verovatno je da će domen ili IP adresa predstavljati više od jedne efektivne lokacije. Sa druge strane, istraga tipa „Pratite novac“ može da vrati nalaze (opet IP adrese i domene) koji su manje promenljivi, pošto se takva istraga fokusira na portale za naplatu, račune za plaćanje (kao što su PayPal i Bitcoin „novčanici“) i druge strukture koji imaju veće „vreme za život“. Ovo upozorenje važi i za mnoge spoljne OSINT izvore jer oni mogu da prikupljaju informacije u različitim prošlim vremenima i stoga da predstavljaju konfliktne ili nekompatibilne informacije. Kao takvi, neki OSINT alati zasnovani na forenzici pokušavaju da kompenzuju održavanjem vremenske linije podataka.

Ekosistem kršenja prava intelektualne svojine predstavlja i mogućnosti i izazove za istražitelja koji primenjuje OSINT. Uspeh poslovnog modela za kršenje prava intelektualne svojine je u velikoj meri zasnovan na premisi da su proizvodi i usluge koji krše prava lako uočljivi, vidljivi i dostupni krajnjem korisniku/kupcu. U tom cilju, OSINT može da bude veoma efikasan i ne zahteva posebne veštine da bi se otkrio nivo informacija sa kojim se suočava klijent.

Stoga, ne samo da su Internet stranice vidljive, već i vlasnici obavljaju aktivnosti optimizacije pretraživača (SEO) kako bi poboljšali svoje rangiranje.

Dobro je poznata i dobra praksa da istražitelj izgradi portfolio različitih alatki za obavljanje određenog zadatka kako bi potvrdio svoje nalaze.

Kod OSINT-a, posebno, ključno je koristiti više od jednog alata u izvođenju određene radnje. Zbog prirode OSINT podataka, od različitih alata se očekuje da proizvedu različite informacije, budući da su vezani njihovim lokalnim strategijama „keširanja“ („Cache“) i skladištenja, načinom na koji postavljaju upite u sisteme uživo i vremenskim vremenima upita. Zadatak istražitelja je da protumači i odredi prioritet informacija dobijenih OSINT vežbom.

Rezultati dobijeni iz OSINT alata, a posebno oni koji su otvorenog koda ili besplatni, treba da se koriste kao vodič, a istražitelj treba da postupa oprezno kada tumači rezultate. Podrška i pouzdanost besplatnog OSINT softvera može biti ograničena jer se možda neće dosledno održavati.

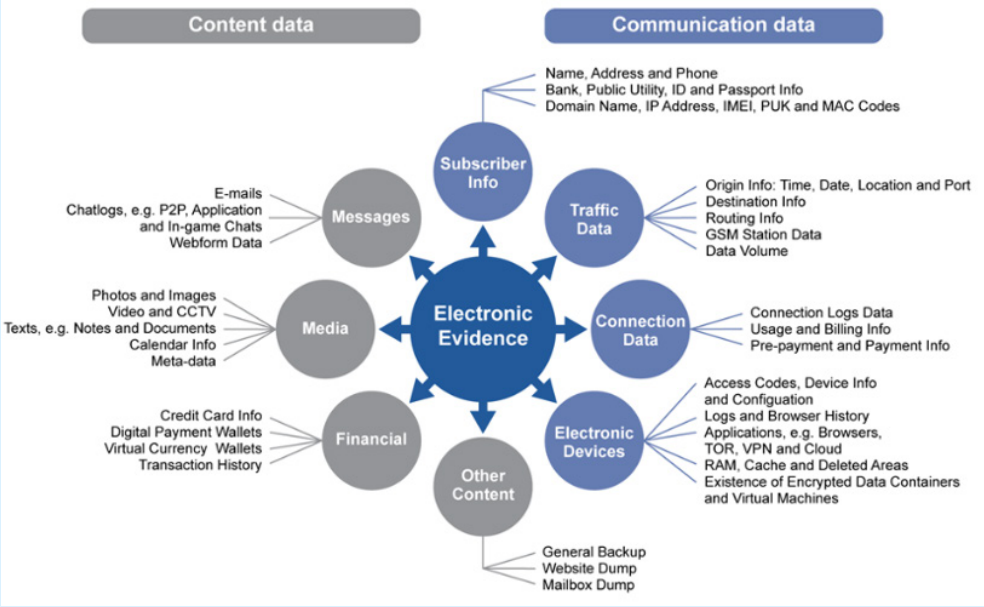
9. DIGITALNI DOKAZI

9.1 Uvod

U cilju suočavanja sa izazovima harmonizacije istražnih procesa preko granica kada se radi o povredama prava intelektualne svojine na mreži, ovaj odeljak je dizajniran da pomogne istražiteljima u svim fazama rukovanja potencijalnim digitalnim dokazima. Prema standardu ISO/IEC 27037, ove faze su **identifikacija, prikupljanje, akvizicija i očuvanje** digitalnih dokaza. Iako mnoge agencije imaju svoje nacionalne smernice, standardne operativne procedure i protokole, ključno je da oni koji prvi reaguju i istražitelji uvaže složenost koju mesta zločina mogu imati i krhkost digitalnih dokaza koji se mogu lako oštetiti ili izmeniti zbog neispravnog rukovanja, bilo slučajno ili namerno. Stoga, samo adekvatno obučeno osoblje treba da pokuša da zapleni osnovnu opremu, tako što će zadržati lanac nadzora nad svim digitalnim dokazima sa strukturiranim procesima koje sudovi prihvataju.

Jedna stvar koju istražitelji treba da imaju na umu jeste da mnogi slučajevi kršenja prava intelektualne svojine mogu zahtevati prisustvo dodatnih odgovornih lica (tj. forenzičkih islednika) na licu mesta da bi završili opsežnije procedure trijaže – to jest, davanje prioriteta i pristup strategiji sticanja digitalnih artefakata otkriveno na licu mesta

- ili slikanje i reagovanje na licu mesta. Na primer, kada se zaplene i nabave uređaji sa transponderima uživo, potrebno je pažljivo rukovati njima kako bi se uhvatile i evidentirale promenljive informacije (kao što su otvorene mrežne veze, ulazni tokovi sadržaja, itd.).



Slika 3 – Vrste digitalnih dokaza

9.2 Mesto zločina

Po dolasku na mesto zločina, istražitelj mora biti siguran ili imati pristup sledećem:

- **Obezbeđeno mesto zločina.** Ovo bi mogla biti jedna od ključnih uloga osobe koja prvi reaguje, da zadrži granicu na području oko lica mesta i zadrži sve po strani radi boljeg očuvanja dokaza i boljih šansi za vredne forenzičke rezultate. Takođe treba naglasiti da osumnjičenom ni pod kojim okolnostima ne bi trebalo dozvoliti da dodirne bilo koju elektronsku opremu koja je prisutna niti da komunicira sa bilo kim. Sistemi se mogu isključiti daljinski putem interneta ili mobilnog telefona ili čak putem pametnih uzoraka i važni dokazi mogu biti izgubljeni ili uništeni;

- **Vizuelni materijal** (tj. fotografije) mesta zločina zajedno sa sumnjivim sistemom (prednji i zadnji pogled i mrežna povezanost svih uređaja), kako bi se zvanično zapečatilo stanje mesta događaja i uređaja po dolasku hitnih službi. Ovaj materijal će takođe biti koristan timu forenzičkih ispitivača ako postoji potreba za repliciranjem uređaja i umreženog okruženja u laboratoriji;

- **Detaljna dokumentacija** svih preduzetih radnji;

- Dokumentacija **o stručnom nivou i stručnosti osumnjičenih**; i

- **Čuvanje dokaza.** Propust da se sačuvaju dokazi dovodi do neuspeha u krivičnom gonjenju.

9.3 Razmatranja o opremi i komplet alatki za istragu

„Alatka za prikupljanje digitalnih dokaza“ odnosi se na opremu i zalihe koje treba uzeti za rukovanje i upravljanje mestom zločina. U većini slučajeva, uređaji koji sadrže digitalne dokaze mogu se prikupiti uz upotrebu standardnih alata za zaplenu. Ipak, sva mesta zločina mogu se smatrati jedinstvenim, tako da ovu upotrebu alata treba prilagoditi svakoj situaciji. Mnoštvo i raznovrsnost uređaja na koje se može sresti tokom istrage o kršenju prava intelektualne svojine diktirali bi fleksibilan komplet alata koji bi takođe pratio niz procedura. Takođe se preporučuje istražiteljima da vode imenik resursa na koje bi se mogli obratiti, ako bi situacija zahtevala znanje i veštine koje prevazilaze njihove mogućnosti.

Ovaj istražni alat treba pripremiti unapred, uzimajući u obzir ili moguće uslove koji se moraju ispuniti na mestu zločina ili radnje koje će istražitelji biti pozvani da izvrše. Što se tiče radnji preduzetih na licu mesta, istražitelji bi trebalo da razmotre sledeće:

- Sprovođenje skeniranja mreže ako je moguće;

• Snimanje mrežnog saobraćaja za određene, specifične vremenske okvire koji svi moraju biti dokumentovani;

• Pristup računarima radi traženja administrativnih alata koji prikazuju korisničke informacije i e-mail naloge;

• Pokretanje provera datoteka evidencije;

• Identifikovanje IP adresa drugih korisnika;

• Traženje podataka o klijentima (bilo u digitalnom ili štampanom formatu);

• Traženje finansijskih informacija (bilo u digitalnom ili štampanom formatu);

• Preuzimanje podataka za prijavu – i korisničkih imena i lozinki (bilo korišćenjem specifičnog forenzičkog softvera ili intervjuisanjem osumnjičenih); i

• Detaljno dokumentovanje svih preduzetih radnji.

Dalje, treba napraviti posebnu listu opreme i rutinski ažurirati je kako bi se pomoglo istražiteljima dok su na licu mesta i za prikupljanje i za obradu dokaza. Ova lista treba da sadrži stavke kao što su:

- Beležnica i olovke (ako se dokumentacija uzima rukom);
- Standardizovani obrasci za dokumentaciju (ako su dostupni);
- Rukavice;
- Digitalni fotoaparat / diktafon (potpuno napunjen);
- Kućište za odvijač sa svim tipovima glava koje možete zamisliti;
- Papirne kese za dokaze;
- Antistatičke ili „faradej“ kese za skladištenje;
- Dokazne oznake;
- Lampe;
- Traka za dokaze i traka za pakovanje;
- Obične bojice za obeležavanje;
- Etikete;

- Gumice (ili vezice);
- Blokatori pisanja;
- Odgovarajuće dezinficirano skladištenje (različiti tipovi sterilnih medija);
- Adapteri;
- Kablovi;
- Laptop: platforma za forenzičku obradu; i
- Forenzička platforma mobilnih uređaja.

9.4 Vrste podataka

Postoje različite vrste podataka sa kojima će se morati rukovati tokom sprovođenja kompjuterske forenzičke istrage. Oni se obično klasifikuju prema stepenu promenljivosti:

- Nestabilni podaci - podaci koji nestaju kada se uređaj isključi. Shodno tome, predlaže se neposredna slika na licu mesta (tj. sa uređaja koji još uvek radi, u „živom“ stanju);
- Nepromenljivi podaci – podaci koji ostaju na uređajima i mogu se preneti na lokaciju na kojoj se mogu završiti odgovarajuće forenzičko snimanje i analiza.

Prema standardu ISO/IEC 27037, „digitalni dokazi mogu biti krhke prirode. Mogu se menjati ili uništiti nepravilnim rukovanjem ili ispitivanjem. Rukovaoci digitalnim dokazima treba da budu kompetentni da identifikuju i upravljaju rizicima i posledicama potencijalnih pravaca delovanja kada se bave digitalnim dokazima. Ako se digitalnim uređajima ne rukuje na odgovarajući način, potencijalni digitalni dokazi koji se nalaze na tim digitalnim uređajima mogu biti neupotrebljivi.

Da bi se izbeglo oštećenje i gubitak potencijalno kritično važnih podataka, manipulacija sistemom se može vršiti prema sledeća četiri opšta principa ACPO:

- Nikakva preduzeta radnja ne bi trebalo da promeni podatke koji se nalaze na računaru ili medijumu za skladištenje na koje se kasnije može osloniti na sudu;
- U okolnostima kada osoba smatra da je neophodno da pristupi

originalnim podacima koji se nalaze na računaru ili na mediju za skladištenje, ta osoba mora biti kompetentna za to i da bude u stanju da pruži dokaze koji objašnjavaju relevantnost i implikacije svojih radnji;
- Revizorski trag ili drugi zapis o svim procesima primenjenim na kompjuterski bazirane elektronske dokaze treba da se kreiraju i sačuvaju. Nezavisna treća strana treba da bude u mogućnosti da ispita te procese i postigne isti rezultat; i
- Osoba zadužena za istragu ima sveukupnu odgovornost da obezbedi da se zakon i ovi principi poštuju.

Proces identifikacije dokaza

Faza identifikacije je proces u tri koraka koji uključuje **traženje, prepoznavanje i dokumentovanje** potencijalnih dokaza koji su relevantni za incident kršenja prava na mreži. Izuzetno je važno da istražitelji daju prioritet prikupljanju dokaza na osnovu njihove nestabilnosti (pogledajte odeljak Tipovi podataka). Što se tiče **aktivnih** sistema, pravi redosled akvizicije je onaj koji prvo čuva najpromenljivije podatke. Neuspeh da se tačno identifikuju svi relevantni promenljivi podaci koji se moraju prikupiti može ozbiljno uticati na efikasnost i ishod istrage, ali takođe može biti osporeno na sudu.

U operaciji bilo koje veličine, istražitelji će morati da budu spremni da se suoče i zaplene nekoliko tipova uređaja koji mogu sadržati informacije koje opisuju pristup ekosistemu kršenja prava intelektualne svojine. Ovi uređaji su, ali nisu ograničeni na sledeće:

- Serveri (uključujući i trans-koderne uređaje);
- Računari i/ili laptopovi;
- Set Top Bok-ovi / prenosivi uređaji / pametni televizori;
- Tableti i pametni telefoni;
- Konzole za igru;
- Ruteri;
- Eksterne disk jedinice;
- USB fleš diskovi; i
- Čitači kartica i pametne kartice.

Informacije sačuvane na ovim uređajima mogu da pruže detalje o dve vrste istrage „Pratite tok“ ili „Pratite novac“. Vredi napomenuti da se od uređaja očekuje da sadrže ključne informacije u vidu e-mail naloga i korespondencije, opisivanje kako su pojedinci plaćali usluge, detalje o povezivanju sa IP adresama, kao i informacije o količini prenetih i primljenih podataka.

Suštinsko razmatranje procesa zaplene je da se zajedno sa gore navedenim uređajima prikupe i svi periferni uređaji (tj. ulazni ili kontrolni uređaji), pripadajući punjači i izvori napajanja, kablovi, pa čak i uputstva koja se nalaze na mestu zločina.

Još jedno razmatranje u ovoj fazi jeste da se obezbedi da budu preduzete neophodne radnje za zaštitu prolaznih ili promenljivih podataka koji se mogu brzo izgubiti ili oštetiti. U tu svrhu moraju se nabaviti softverske ili hardverske tehnike za preuzimanje memorije. Dalje, pošto je mrežna aktivnost promenljiva i dinamična, mora se izvršiti mrežna forenzička istraga o istorijskim i trenutnim mrežnim aktivnostima, hvatajući mrežne događaje i aktivnosti kako se dešavaju u realnom vremenu. Shodno tome, preporučljivo je da istražitelji izvrše kompletno snimanje mreže paketa, kako bi uhvatili i snimili mrežne veze i aktivnosti osumnjičenog dokumentujući tačno vreme tih događaja.

9.5 Zamke i bombe

Istražitelji uvek treba da imaju na umu da zlonamerni softver koji deluje kao zamka ili logička bomba mogu biti skriveno postavljeni u sistemu koji se istražuje. Nije nepoznato da uređaj može biti zarobljen kako bi se uništili potencijalni dokazi ili sam uređaj. Ovi tipovi sofisticiranog, unapred učitanog softvera (ili skupa komandi) su dizajnirani da unište kritične podatke koji se nalaze na uređajima koji će biti zaplenjeni kada se ispuni unapred definisani uslov. Na primer, osumnjičeni ih može aktivirati pomoću daljinskog upravljača ili čak mogu da se pokrenu sami kada otkriju da je pokrenut određeni softver, komanda ili upit, kao što su „nmap“, „netstat“, „whois“ itd.

Najzad, istražitelji mogu da naiđu na bilo koji od ova tri tipa unapred učitanog zlonamernog softvera:

- „Bomba sa vrućim tasterom“: odnosi se na bilo koju dodeljenu kombinaciju tastera koja može da izvrši komanda ili serija komandi;
- „Zamka sa minom“: unapred instaliran softver koji izgleda da obavlja određenu funkciju, ali zapravo radi nešto drugačije; i
- „Rezidentni program Prekini i ostani“: softver koji ostaje rezidentan u memoriju računara tako da se može (ponovno) aktivirati prekidom sistema.

Iako retki, ovakvi scenariji se mogu javiti. Shodno tome, dok su na licu mesta, istražitelji bi trebalo da budu svesni potencijalnih tehnologija (kao što su infracrveni uređaji) koje bi osumnjičenom mogle da daju daljinski pristup sistemu, ili čak postojanja destruktivnih programa sa zamkom na uređajima koji bi mogli da oštete ključne dokaze potrebne za identifikaciju i krivično gonjenje krivac.

Obezbeđivanje da niko ne dodiruje tastaturu (što je najčešće pravilo koje se primenjuje pri izvršenju naloga u vezi sa digitalnim dokazima) sprečiće namerno ili nenamerno pokretanje bilo kakvog niza događaja koji bi mogli da oštete krhke podatke na uređajima.

9.6 Skladištenje i očuvanje digitalnih dokaza

Sve procedure prikupljanja za pakovanje i označavanje fizičkih dokaza moraju se primeniti na elektronske uređaje kako bi se zaštitio njihov integritet i sačuvali u prvobitnom stanju. Zbog toga, istražitelji moraju da poštuju strogi protokol lanca nadzora, da precizno i pažljivo rukuju digitalnim uređajima kako bi ih zaštitili od fizičkog oštećenja i oštećenja od elektromagnetnih izvora. Izloženost faktorima kao što su ekstremne temperature, velika nadmorska visina, statički elektricitet, vlaga ili elektromagnetnim izvorima kao što su radio frekvencije i magneti smatraju se potencijalnim izvorima oštećenja digitalnih dokaza. Prema ISO/IEC 27037, osnovne aktivnosti kojima bi se istraživači trebali baviti su sledeće:

- Nosite rukavice bez vlakana;
- Označite sve potencijalne digitalne dokaze i uređaje u skladu sa

specifičnim zahtevima nacionalne jurisdikcije u vezi sa formatom obeležavanja dokaznog materijala;
- Zapečatite nalepnicama koje štite digitalne uređaje koji imaju otvore i/ili pokretne delove;
- Digitalne uređaje sa priključenim baterijama treba redovno proveravati kako bi imali adekvatno napajanje;
- Koristite odgovarajuće kontejnere da zaštitite uređaj od potencijalnih pretnji. Razmislite o korišćenju antistatičke kese; papirne kese ili kartonske kutije su i dalje prihvatljive, ali ih nikada ne čuvajte u plastičnim kesama;
- Pakovanje digitalnih uređaja na način koji sprečava oštećenja od udara, vibracija, visokih temperatura, nadmorska visina, ekstremne temperature i radio frekvencije tokom transporta;
- Obratite posebnu pažnju na magnetne uređaje za skladištenje koji se moraju čuvati u pakovanjima koja su magnetno inertna, antistatička i bez čestica; i
- Budite oprezni u okolnostima u kojima digitalni uređaji sadrže latentne tragove ili biološke dokaze, jer prikupljanje takvih dokaza mora biti sprovedeno pre digitalnog snimanja dokaza.

10. DALJE UČENJE

10.1 IP Koledž za krivične istražitelje

Ako Kosovska policija želi da poveća svoje znanje o tome kako da istražuje kršenje prava intelektualne svojine u onlajn okruženju, preporučuje se da posetite Međunarodni koledž za istrage intelektualne svojine (IIPCIC).

IIPCIC-om upravlja Interpol i predstavlja potpuno interaktivnu Internet ustanovu za obuku o kriminalu u vezi sa intelektualnom svojinom koja nudi kurseve engleskog, španskog, francuskog, arapskog, mandarinskog i portugalskog.

Preko 150 zemalja posetilo je Internet stranicu IIPCIC od njenog pokretanja, a preko 600 agencija za sprovođenje zakona se upisalo za obuku. IIPCIC ima mandat da razvija, koordinira i administrira pro-

grame obuke u cilju podrške međunarodnim naporima za sprečavanje, otkrivanje, istragu i krivično gonjenje transnacionalnog organizovanog kriminala u vezi sa intelektualnom svojinom.

Kurs je besplatan za službenike institucija za sprovođenje zakona, ali korisnici prvo moraju da pribave detalje za prijavljivanje na:

www.iipcic.org

ANEKS I - PREDMETI INTELEKTUALNE SVOJINE

Uvod

Intelektualna svojina (IP) se odnosi na kreacije uma: pronalaske, književna i umetnička dela, i simbole, imena, slike i dizajne koji se koriste u trgovini.

IP je podeljen u dve kategorije:

- industrijska svojina, koja uključuje pronalaske (patenti), žigovi, industrijski dizajni i geografske oznake izvora; i
- autorska prava, koja obuhvataju književna i umetnička dela kao što su romani, pesme i drame, filmovi, muzička dela, umetnička dela kao što su crteži, slike, fotografije i skulpture, i arhitektonski dizajn. Prava u vezi sa autorskim pravima obuhvataju prava izvođača u svojim nastupima, proizvođača fonograma u njihovim snimcima i prava emitera u njihovim radio i televizijskim programima.[45]

Industrijska imovina

Svrha sistema prava industrijske svojine je da podstakne i motiviše pronalazače i stvaraoce, da zaštiti njihova prava i da uliva poverenje u održavanje poslovnih aktivnosti Prava industrijske svojine obuhvataju sledeće:

[45]Svetska organizacija za intelektualnu svojinu (World Intellectual Property Organisation) www.wipo.int/about-ip/en/

- Patenti;
- Žigovi;
- Industrijski dizajn;
- Geografske oznake i oznake porekla, i
- Topografije integrisanih kola.

Nosioci prava treba da registruju svoju industrijsku svojinu kod IPA da bi dobili zaštitu na Kosovu. Nosioci prava, uključujući tu i inostrane subjekte, koji ne registruju svoju industrijsku svojinu kod IPA-e možda i dalje imaju određena prava, ali njihov status uvek treba da bude razjašnjen sa IPA pre pokretanja istrage.

Patenti

Patent je ekskluzivno zakonsko pravo za pronalazak. Pronalazak je proizvod ili proces koji pruža novi način da se nešto uradi, ili nudi novo tehničko rešenje problema.

Žigovi

Žig je karakteristični znak koji razlikuje određenu robu ili usluge kao one koje pruža određeno lice ili preduzeće od istih dobara ili usluga drugih preduzeća. Njegovo poreklo datira iz antičkih vremena, kada su zanatlije reprodukovale svoje potpise, ili „oznake“ na svojim umetničkim ili upotrebnim proizvodima. Tokom godina ove oznake su evoluirale u današnji sistem registracije i zaštite. Sistem pomaže potrošačima da identifikuju i kupe proizvod ili uslugu, jer njegova priroda i kvalitet, naznačeni jedinstvenim zaštitnim znakom, zadovoljavaju njihove potrebe.

Industrijski dizajn

Industrijski dizajn je ukrasni ili estetski aspekt predmeta. Dizajn se može sastojati od trodimenzionalnih karakteristika, kao što su oblik ili površina predmeta, ili od dvodimenzionalnih karakteristika, kao što su šare, linije ili boje. Industrijski dizajn se primenjuje na širok spektar proizvoda industrije i zanatstva: od tehničkih i medicinskih instrumenata do satova, nakita i drugih luksuznih predmeta; od predmeta i elek-

tričnih uređaja do vozila i arhitektonskih objekata; od dizajna tekstila do robe za slobodno vreme. Industrijski dizajn mora privući oko. To znači da je industrijski dizajn prvenstveno estetske prirode i da ne štiti nikakve tehničke karakteristike predmeta na koji se primenjuje.

Geografske oznake i oznake porekla

Geografska oznaka (GI) je naziv regiona, određenog mesta ili u posebnim slučajevima naziv države, koji se koristi da opiše proizvod poreklom iz tog regiona, određenog mesta ili države, koji poseduje kvalitet, reputaciju ili drugo specifične karakteristike koje proizilaze iz geografskog porekla, proizvodnje i/ili prerade i/ili pripreme koje se u potpunosti odvijaju u definisanom nazivu geografske oblasti koji se koristi za označavanje da proizvod potiče iz zemlje ili regiona ili određenog mesta čije je dato kvalitet, ugled ili druga karakteristika se u suštini mogu pripisati njegovom geografskom poreklu; i najmanje jedan od koraka proizvodnje koji se odvija na definisanom geografskom području.

Oznaka porekla (DO) je naziv regiona, određenog mesta ili, u posebnim slučajevima, naziv države, koji se koristi da opiše proizvod poreklom iz tog regiona, specifičnog mesta ili države, čiji kvaliteti ili karakteristike su suštinski ili isključivo kao rezultat određenog geografskog okruženja sa prirodnim i ljudskim faktorima nasleđenim iz ove sredine, i kao rezultat proizvodnje, prerade i pripreme proizvoda koji je u potpunosti razvijen na definisanom geografskom području.

Topografije integrisanih kola

Topografija integrisanog kola je trodimenzionalni raspored elemenata, od kojih je najmanje jedan aktivni element, i nekih ili svih interkonekcija integrisanog kola, ili takav trodimenzionalni raspored pripremljen za integrisano kolo namenjen za proizvodnju.

Integrisano kolo označava proizvod, u svom konačnom ili srednjem obliku, u kojem su elementi, od kojih je najmanje jedan aktivni element,

i neke ili sve međusobne veze integralno formirane u i/ili na komadu materijala a koji je namenjen za obavljanje elektronske funkcije.

Topografija je zaštićena ako je originalna, odnosno ako je rezultat sopstvenog intelektualnog truda njenih kreatora i nije uobičajena među kreatorima dizajna rasporeda i proizvođačima integrisanih kola u vreme njenog nastanka.

Autorsko pravo

Autorsko pravo i prava povezana sa autorskim pravom

Autorsko pravo kakvo postoji u sistemu kontinentalne Evrope kojeg se pridržava Kosovo naziva se „autorska prava“ i bavi se pravnom zaštitom autora u njihovim delima. Autori su, po pravilu, zaštićeni za dela u književnoj, umetničkoj, muzičkoj, naučnoj i sličnim oblastima, kao što su romani, pesme, muzičke kompozicije, skulpture, slike, crteži, kinematografska dela, arhitektura, koreografija, fotografija i kao; takva dela moraju biti intelektualne tvorevine i ispunjavati određeni nivo kreativnosti. Za takva dela autori su redovno zaštićeni van-privrednim i ekonomskim pravima. Neprivredna prava štite lični i umetnički interes autora u njegovom delu i nazivaju se moralnim pravima; oni posebno uključuju pravo očinstva (pravo da budete imenovani kao autor dela, da ostanete anoniman ili da izaberete pseudonim), pravo na otkrivanje (prvi čin stavljanja dela na raspolaganje javnosti u bilo kom obliku), pravo na integritet dela (naročito pravo na prigovor na bilo kakvo sakaćenje ili drugu neželjenu modifikaciju), kao i pravo na povlačenje (pravo na opoziv ustupanja prava svojine ako za to postoje ozbiljni moralni razlozi, pod uslovom da se asignatu nadoknadi šteta prouzrokovana takvim opozivom). Pored toga, imovinska prava redovno priznaju isključivu kontrolu autora nad eksploatacijom njegovih dela, tako da se zabranjuje ili dozvoljava širok spektar upotrebe. U nekoliko slučajeva, zakon priznaje samo zakonsko pravo na naknadu umesto ekskluzivnog prava. Ekskluzivna prava podležu eksplicitno regulisanim ograničenjima i izuzecima u korist opšte javnosti. Trajanje zaštite je obično ograničeno na 70 godina nakon smrti autora. Pravo otkrivanja i pravo povlačenja prema kosovskom Zakonu o autorskim pravima važe za života autora. Ovakva zaštita ima za cilj da prepozna značaj

stvaralaštva za kulturu omogućavajući autoru da dobije nagradu od eksploatacije svojih dela.

Pošto da autorska prava ne štite nijedno nestvaralačko ostvarenje, već su takva druga dostignuća međunarodno priznata kao od velike vrednosti za dostupnost kulture u društvu, zemlje evropskog kontinentalnog pravnog sistema su uvele i tzv. prava povezana sa autorskim pravom. Njihova glavna karakteristika je da ne štite „dela“ u smislu autorskih prava, već slična dostignuća koja delimično promovišu ili pomažu da se dela učini dostupnim javnosti. Glavna srodna prava priznata širom sveta su prava izvođača (pevača, drugih muzičara, igrača, glumaca i drugih koji izvode dela); proizvođači fonograma; producenti filmova; i radiodifuzne organizacije. U drugim zemljama uvedene su dodatne vrste srodnih prava. Takođe, trajanje zaštite je kraće od trajanja autorskih prava. Dok su izvođači zaštićeni zbog svog umetničkog ostvarenja, na primer, izvođenja dela, ostali nosioci srodnih prava zaštićeni su zbog tehničkog, organizacionog i finansijskog ulaganja u proizvodnju snimaka, u radiodifuznu delatnost itd.

Zaštita autorskih prava se daje bez ikakvih formalnosti. Dakle, zakon na Kosovu ne zahteva registraciju prava. Ona nastaje čim se delo stvori.

ANEKS II – KONTAKT ADRESE

Kosovo – Kontakt adrese

Agencija za Industrijsku Svojinu

Adresa: Ministarstvo trgovine i industrije
Ul. „Muharem Feiza“, bb. Bolničko naselje,10000 Priština
Telefon: +381 (0) 38 200 36 544
Faks: Nije dostupan
Veb: vvv.kipa-ks.org
Email: nezir.gashi@rks-gov.net

Kancelarija za autorska i srodna prava

Adresa: Ministarstvo kulture, omladine i sporta
Trg Majke Tereze bb., Priština
Telefon: +381 (0) 38 200 563
Faks: Nije dostupan
Web: http://www.autori-ks.com/
Email: valon.kashtanjeva@rks-gov.net

Kosovska policija, Jedinica za privredni kriminal

Adresa: Ul. "Luan Haradinaj" 10000 Priština-Kosovo
Telefon:
Faks:
Web: www.kosovopolice.com
Email: info@kosovopolice.com

Kosovska Policija, Jedinica za sajber kriminal
Adresa: Ul. "Luan Haradinaj" 10000 Priština-Kosovo
Telefon:
Faks:
Web: www.kosovopolice.com
Email: info@kosovopolice.com

Carina Kosova

Adresa: Veternik 1, Industrijska Zona - Priština
Telefon: +381 (38) 540 350
Faks: +381(38)542065
Web: www.dogana-ks.org
Email: info@dogana-ks.org
Info: http://dogana.rks-gov.net/en/Contact

Tržišna inspekcija

Adresa: Ministarstvo trgovine i industrije
Ul. „Muharem Feiza“, bb. Bolničko naselje,10000 Priština
Telefon: +381 (38) 512407,
Fax: tel:038512798
Web: www.mti-ks.org
Email:

Državni tužilac

Adresa:
Telefon:
Faks:
Veb:
Email:

Tužilački Savet

Adresa:
Telefon:
Faks:
Veb:
Email:

Sudski Savet

Adresa:
Telefon:
Faks:
Veb:
Email:

Agencija za lekove i medicinske proizvode

Adresa:
Telefon:
Faks:
Veb:
Email:

Agencija za veterinu i hranu

Adresa:
Telefon:
Faks:
Veb:
Email:

Agencija za zaštitu životne sredine

Adresa:
Telefon:
Faks:
Veb:
Email:

Agencija za upravljanje zaplenjenom ili oduzetom imovinom

Adresa:
Telefon:
Faks:
Veb:
Email:

Nezavisna komisija za medije

Adresa:
Telefon:
Faks:
Veb:
Email:

Regulatorni organ za poštanske i elektronske komunikacije

Adresa:
Telefon:
Faks:
Veb:
Email:

Međunarodni – Kontakt adrese

EUIPO opservatorija

Adresa: Avenida de Europa, 4, E-03008 Alicante, Spain
Telefon: +34 96 513 9100
Email: observatory@euipo.europa.eu
Web: https://euipo.europa.eu/ohimportal/en/web/observatory/home

Interpol (trgovina nedozvoljenom robom i falsifikovanje)

Adresa: General Secretariat 200, quai Charles de Gaulle
69006 Lyon France
Telefon: +33 (0)4 72 44 71 63
Email: info@iipcic.org
Web: http://www.iipcic.org

Europol (IP Crime)

Adresa: Eisenhowerlaan 73, 2517 KK The Hague, The Netherlands
Telefon: +31 7 03 531575
Email: o3@europol.europa.eu
Web: http://www.europol.europa.eu

Svetska carinska organizacija (grupa za falsifikovanje i pirateriju)

Adresa: Rue du Marché, 30, B-1210 Brussels, Belgium.
Telefon: +32 2 209 92 11
Web: http://www.wcoomd.org/
Email:

Svetska organizacija za intelektualnu svojinu (VIPO)

Adresa: 34, chemin des Colombettes, CH-1211 Geneva 20, Switzerland
Telefon: +41 22 338 9111
Web: www.wipo.int
Email:

ANEKS III – ZAKONODAVSTVO

Krivični zakon

Član 289 - Povreda patentnih prava

1. Ko u sklopu neke privredne delatnosti neovlašćeno koristi patent koji je registrovan ili zaštićen zakonom, ili registrovanu topografiju zatvorenog kola poluprovodnika, kazniće se novčanom kaznom ili kaznom zatvora u trajanju do tri (3) godine.

2. Predmeti iz stava 1. ovog člana koji su neovlašćeno proizvedeni za upotrebu, biće oduzeti.

Član 290 - Povreda autorskih prava

1. Ko pod svojim imenom ili imenom drugog prikaže ili na drugi način prenese javnosti delo zaštićeno autorskim pravom ili interpretaciju, u celini ili delimično, kazniće se novčanom kaznom i kaznom zatvora u trajanju od tri (3) meseca do tri (3) godine.

2. Ko prilikom korišćenja dela zaštićenog autorskim pravima ili interpretacije hotimično ne navede ime, pseudonim ili oznaku autora ili izvođača kad je to zakonom propisano, kazniće se novčanom kaznom i kaznom zatvora u trajanju do jedne (1) godine.
3. Ko izmeni, preradi ili na drugi način ošteti delo zaštićeno autorskim pravom ili interpretaciju, i u takvom obliku ga objavi ili ga u takvom obliku na neki drugi način prenese javnosti, kazniće se novčanom kaznom ili kaznom zatvora u trajanju do jedne (1) godine.

4. Ko prikaže ili u nekom drugom obliku prenese javnosti delo zaštićeno autorskim pravom ili interpretaciju na neodgovarajući način koji vređa i ugled autora ili izvođača dela, kazniće se novčanom kaznom ili kaznom zatvora u trajanju do jedne (1) godine.

5. Ko neovlašćeno koristi delo zaštićeno autorskim pravom ili teme stvari koje su povezane sa tim pravom, kazniće se kaznom zatvora u trajanju do tri (3) godine.

6. Ako je u toku izvršenja krivičnog dela iz stava 5. ovog člana izvršilac za sebe ili drugog stekao imovinsku korist od najmanje deset hiljada (10,000) i ne više od pedeset hiljada (50,000) evra, kazniće se novčanom kaznom i kaznom zatvora u trajanju od tri (3) meseca do pet (5) godina.

7. Ako je izvršilac krivičnog dela iz stava 5. ovog člana za sebe ili drugog stekao imovinsku korist veću od pedeset hiljada (50,000) evra, kazniće se novčanom kaznom i kaznom zatvora u trajanju od šest (6) meseci do osam (8) godina.

8. Predmeti i oprema za njihovu izradu biće oduzeti.

Član 291 - Izbegavanje tehnoloških mera

1. Ko izvrši delo izbegavanja neke od efikasnih mera tehnološke zaštite, ili delo brisanja ili izmene elektronskih prava za upravljanje podacima, kao što je propisano u odredbama zakona o autorskim pravima i drugim srodnim pravima, kazniće se kaznom zatvora u trajanju do tri (3) godine.

2. Predmeti i oprema za njihovu izradu iz stava 1. ovog člana biće oduzet.

Član 292 - Obmana potrošača

1. Ko u obavljanju privredne delatnosti a u nameri da obmane kupce ili potrošače, kao svoje ime ili znak ili kao određen znak za svoju robu, koristi tuđe ime ili znak, ili znak tuđe robe ili znak tuđe usluge, ili tuđi znak koji se odnosi na geografsko poreklo, ili neki drugi posebni znak za robu ili njene sastavne delove, ili navedeno poseduje u nameri da ih koristi, kazniće se kaznom zatvora u trajanju do tri (3) godine.

2. Ko u nameri da obmane kupce ili potrošače neovlašćeno koristi u proizvodnji tuđe znake ili tuđi model, ili pusti u promet robu proizvedenu na taj način, kazniće se kaznom iz stava 1. ovog člana.

3. Predmeti i oprema za njihovu izradu biće oduzeti.

ANEKS IV – DEFINICIJE[46]

Online kršenja: Prekršaji koji se dešavaju na otvorenom delu interneta[47] a primarni fokus je na povredama komercijalnih razmera, što znači da se dela kršenja „izvode radi direktne ili indirektne ekonomske ili komercijalne koristi“.[48] Upotreba termina onlajn i onlajn okruženje

[46]Studija o zakonodavnim merama u vezi sa kršenjem prava intelektualne svojine na mreži, EUIPO, 2018.

[47]Vodič stoga ne pokriva aktivnosti na neindeksiranim delovima interneta, koji se često nazivaju darknet. Vidi definiciju „darknet“ na str. 14 u „Istraživanju o onlajn poslovnim modelima koji krše prava intelektualne svojine. Faza 1. Faza 1 Pregled onlajn poslovnih modela koji krše prava intelektualne svojine“, EUIPO, jul 2016.

[48]Kao što je definisano u Uvodnoj Izjavi 14 Direktive 2004/48 o sprovođenju prava intelektualne svojine. Studija se

u ovom Vodiču uključuje bilo koju aktivnost na otvorenom Internetu, uključujući veb-stranice, stranice nižeg nivoa, profile korisnika na veb-stranicama društvenih mreža, onlajn aukcije i platforme za trgovanje, e-poštu i aplikacije povezane internetom na mobilnim uređajima.

Posrednici: Internet posrednici su entiteti - obično kompanije - koji okupljaju ili olakšavaju transakcije među trećim stranama na internetu. Oni daju pristup, hostuju, šalju ili indeksiraju sadržaj, proizvode i usluge koje potiču od trećih strana na internetu ili pružaju usluge zasnovane na internetu takvim trećim stranama.[49]
Ime domena: Sistem imena domena (Domain Name System - DNS) služi suštinskoj i centralnoj funkciji olakšavanja mogućnosti internet korisnika da se kreću internetom[50]. Ime domena je adresa prilagođena korisniku, numeričke IP adrese određenog računara (pogledajte definiciju u nastavku). Ime domena 'euipo.europa.eu' je na primer vezan za računar sa numeričkom IP adresom 109.232.208.177, što znači da umesto pamćenja i kucanja '109.232.208.177' u internet pretraživač, korisnik interneta može da ukuca 'euipo.europa.eu' da bude povezan sa veb-sajtom EUIPO-a.

Tehnički, DNS radi kroz mrežu distribuiranih baza podataka kojima upravljaju određeni registri imena domena. Ove baze podataka sadrže liste imena domena i njihovih odgovarajućih IP-numeričkih adresa i obavljaju funkciju mapiranja imena domena u njihove numeričke IP adrese za usmeravanje zahteva za povezivanje računara na Internet.

Imena domena moraju biti registrovana u registru[51] koji je odgovoran za određeni domen najvišeg nivoa, a registracije moraju biti podnete preko akreditovanog registratora imena domena. Na primer, ako kompanija želi da registruje ime domena .eu, kompanija mora da kontaktira akreditovanog registratora .eu i zatraži od registratora da podnese zahtev za registraciju imena domena u ime kompanije. Ako je ime domena upražnjeno i sve ostale formalnosti su ispunjene, ime domena će biti registrovano i uneto u .eu DNS bazu podataka.

stoga ne fokusira na povrede autorskih i srodnih prava koje čine privatna lica kao takva.

[49]https://www.oecd.org/internet/ieconomy/44949023.pdf

[50]Internet Korporacija za Dodeljena Imena i Brojeve (ICANN) je ta koja koordiniše ključne tehničke funkcije DNS-a i definiše politike o tome kako treba da rade 'imena i brojevi' interneta.

[51]Mnogi TLD primenjuju model deljenog registra, u kom slučaju registratori imaju pristup registraciji imena domena direktno u bazi podataka registra. Bazu podataka registra tada administrira posebni administrator registra.

Sva imena domena će biti povezana sa jednim ili više servera imena domena, koji je „kompjuterski server koji sadrži bazu podataka javnih IP adresa i njihovih povezanih imena domaćina, i u većini slučajeva služi za rešavanje ili prevođenje tih uobičajenih imena u IP adrese prema zahtevu'.[52] DNS serverima upravljaju subjekti koji su za to ovlašćeni od strane registara – koji se često nazivaju „menadžeri servera imena" (DNS menadžeri). Mnogi od akreditovanih registratora su takođe ovlašćeni da rade kao DNS menadžeri.

Registri ne ispituju prijave za novo ime domena u odnosu na prethodna prava trećih lica kao što su žigovi, nazivi kompanija ili lična imena. Nosioci prava trećih lica stoga su primorani da ostvare svoja prava nakon što je ime domena registrovano, ako otkriju da registrovano ime domena krši njihova prava.[53]

IP adresa: termin je skraćenica za adresu internet protokola, što je identifikator koji se dodeljuje svakom računaru ili drugom uređaju (npr. mobilnom uređaju) koji je povezan na internet ili na drugu mrežu koristeći TCP/IP protokol. IP adresa se koristi za lociranje i identifikaciju uređaja u komunikaciji sa drugim uređajima na mreži.

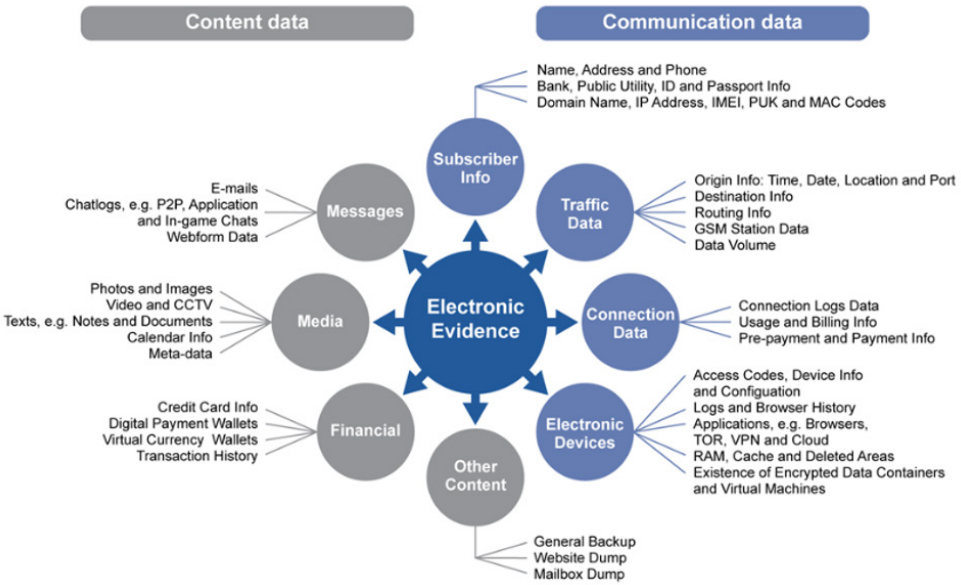
IP adresa može biti statična što znači da će adresa biti ista svaki put kada korisnik koristi svoj račun kod provajdera za povezivanje na internet. Dinamička IP adresa znači da će provajder pristupa dodeliti jednu od IP adresa koje ima na raspolaganju u svom „pulu ili spisku adresa" korisniku kada se on ili ona prijavi, ali će pomenuta IP adresa biti dodeljena samo za ograničenu količinu vreme, odnosno za određenu sesiju. IP adresa može se kasnije dodeljiti novom korisniku.[54] Ugovorom između korisnika i njegovog provajdera pristupa određuje se koja vrsta IP adrese će se primenjivati za uređaje koji su obuhvaćeni ugovorom o usluzi. Međutim, mobilni uređaji kao što su laptopovi, tableti i mobilni telefoni mogu biti i vrlo često povezani na internet preko provajdera pristupa čije su usluge dostupne na mestu gde se korisnik trenutno nalazi. Takve usluge obično koriste dinamičke IP adrese.

[52]Kako je definisao LIFEVIRE, https://vvv.lifevire.com/vhat-is-a-dns-server-2625854

[53]Definicija od gore navedenog „Istraživanja onlajn poslovnih modela koji krše prava intelektualne svojine", EUIPO, 2016.

[54]Dodatne informacije o IP adresama možete, između ostalog, pronaći u članku „Šta je statička IP adresa?" https://vvv.lifevire.com/vhat-is-a-static-ip-address-2626012. Izraz „pul ili spisak adresa" potiče odavde.

Digitalni dokazi: Imena domena i IP adrese su samo dve vrste digitalnih dokaza. Kao što slika u nastavku ilustruje, postoje mnoge druge vrste digitalnih dokaza koji mogu biti relevantni za prikupljanje u određenim slučajevima koji uključuju onlajn kršenje prava intelektualne svojine.



Slika 4 – Različite vrste digitalnih dokaza[55]

55Studija o zakonodavnim merama u vezi sa kršenjem prava intelektualne svojine na mreži, EUIPO, 2018.

IPRproject
Intellectual Property Rights Project

Rr. ”Johan V. Hahn”,
10000 Priština, Kosovo
Tel: 038 726 688
IPRKosovo