Univerza v Ljubljani
Pravna fakulteta

KAZENSKOPRAVNI VIDIKI VARSTVA ZASEBNOSTI IN RAČUNALNIŠTVO V OBLAKU

(magistrsko diplomsko delo)

Avtorica: Anja Češarek

Mentor: izr. prof. dr. Primož Gorkič

Ljubljana, september 2019

POVZETEK

Razvoj informacijsko-komunikacijske tehnologije nam omogoča, da se preko nosilca elektronskih podatkov in omrežne povezave priključimo na internet ter tako dostopamo do svojega oblaka, kateri uporabniku omogoča hiter in preprost dostop do njegovih podatkov ter aplikacij, kadar koli, s kjer koli na svetu. Oblak je postal neomejena zbirka podatkov, kateri se lahko za potrebe pregona kibernetskih kaznivih dejanj v kazenskem postopku uporabijo kot elektronski dokazi. Ti se lahko nahajajo bodisi na elektronskem nosilcu podatkov ali v samem oblaku uporabnika. Podatki v oblaku, kateri so pomembni za postopek (bodisi vsebujejo dokaze o kibernetskem kaznivem dejanju ali pa predstavljajo elemente, potrebne za identifikacijo storilcev) se nahajajo na (večinoma ameriških) serverjih ponudnikov storitev, ki so lahko tudi na drugem delu sveta, zato je nujno potrebna mednarodna pravna pomoč med državami v kazenskem postopku. V veljavi so že nekateri ključni pravni in mednarodni mehanizmi za reševanje pridobivanja elektronskih dokazov, vendar ustvarjalce prava in preiskovalce kibernetskih kaznivih dejanj čaka še veliko usklajevanj. Pri pregonu tovrstnih kaznivih dejanj se pojavljajo vprašanja kot so identifikacija storilcev in nosilcev podatkov, vprašanja jurisdikcije, uporaba elektronskih dokazov v postopku in vrsta vprašanj, s katerimi se soočajo digitalni forenziki pri pridobivanju teh dokazov. V prihodnje bo zato potrebna uskladitev preiskovalnih dejanj in procesnih pravil, kot tudi zagotovitev novih pravnih okvirjev, ki bodo organom pregona omogočale neposredno pridobitev relevantnih podatkov od ponudnika storitev v oblaku.

Ključne besede: Kibernetska kriminaliteta - računalništvo v oblaku - pravica do zasebnosti – jurisdikcija – identifikacija storilcev – digitalna forenzika – evropski preiskovalni nalog– mednarodna pravna pomoč – Konvencija o kibernetski kriminaliteti - Cloud act

ABSTRACT

The development of information and communication technology enables user to connect to the Internet via an electronic data carrier and a network connection and thereby accessing to his Cloud. Cloud Computing enables user to access quickly and easily to his data and applications from anywhere, anywhere in the world. The Cloud has become an unlimited database that can be used as electronic evidence for the purpose of prosecuting cybercrime in criminal proceedings. These may be located either on an electronic storage medium or in the user's cloud itself. The process-relevant cloud data (either containing evidence of cybercrime or representing the elements needed to identify the perpetrators) is located on (mostly US) servers of service providers, which may also be located in another part of the world, so it is imperative required international legal assistance between states in criminal proceedings. There are already some key legal and international mechanisms in place to deal with the acquisition of electronic evidence, but there is still a great deal of harmonization for law makers and cybercrime investigators. Issues such as the identification of perpetrators and data carriers, jurisdictional issues, the use of electronic evidence in proceedings, and the type of issues facing digital forensics in obtaining such evidence arise when prosecuting such crimes. Therefore, harmonization of investigative procedures and procedural rules will be required in the future, as well as the provision of new legal frameworks that will enable law enforcement agencies to directly obtain relevant data from a cloud service provider.

Keywords: Cloud computing – Cybercrime – data privacy – hackers - right to privacy - jurisdictional problem - identifying perpetrators - digital forensics - European search warrant - international legal aid - Cybercrime Convention - Cloud act

KAZALO

1. UVOD

Pojav interneta je omogočil nepredstavljivo hiter razvoj informacijsko-komunikacijske tehnologije (IKT; t.i. moderne tehnologije)[1], brez katere si dandanes ne moremo predstavljati življenja. Prisotna je v vseh sferah našega življenja, saj jo uporabljamo tako za zasebne kot za poslovne namene. Naši dokumenti so se iz fizične oblike preoblikovali v elektronsko obliko in nosilci podatkov (npr. računalnik ali mobilni telefon) nam s pomočjo omrežne povezave omogočajo, da preko njih dostopamo do interneta in posledično tudi do svojih dokumentov, ki jih shranjujejo v oblaku (angl. *cloud computing*).

Oblak je postal neomejena zbirka posameznikovih podatkov, med katerimi so lahko tudi najbolj osebni podatki posameznika, kot tudi visoko tajni podatki držav, bank ali podjetij. Vse to se sliši nadvse fascinantno, vendar se uporabniki premalokrat zavedamo pasti, ki jih prinaša uporaba moderne tehnologije. Kot navaja Kovačič, je »problem interneta predvsem v tem, da tehnologija že sama po sebi, zaradi svojih lastnosti, omogoča nekatere zlorabe zasebnosti v večji meri, kot bi bile mogoče v fizičnem prostoru.«[2] To misel lahko navežemo tudi na storilce kaznivih dejanj, ki izkoriščajo prednosti tehnologije za zlorabe zasebnosti uporabnikov na internetu. Storilcem današnji splet omogoča izvršitve kaznivih dejanj, katerih v preteklosti nismo poznali ali pa jim splet in uporaba IKT omogoča izvrševanje že poznanih kaznivih dejanj na moderen, inovativen in prikrit način. Pri tem splet seveda ni omejen le na meje nacionalnih držav, ampak deluje po celem svetu.

Ali smo s shranjevanjem naših podatkov v oblaku varni pred drugimi, tudi državo? Pod kakšnimi pogoji lahko organi pregona dostopajo do naših podatkov ob spoštovanj pravice do zasebnosti? Kako je v primeru preiskovanja kaznivih dejanj ob elementu čezmejnosti, ko so podatki v našem oblaku na drugem kontinentu? Posvetila se bom vsem tem vprašanjem, predvsem pa elementom, ki otežujejo kazenski pregon in preiskovanje kibernetske kriminalitete ter kako, in če, mednarodni in pravni mehanizmi rešujejo z zasebnostjo povezana vprašanja pri pridobivanju podatkov iz oblaka za namen kazenskega pregona in preiskovanja.

V prvem delu svoje naloge se bom osredotočila na opredelitev samega pojma računalništva oblaku, kako ta deluje, , katere so njegove prednosti in slabosti oziroma kateri pravni izzivi ga spremljajo. Nadalje bom uvrstila računalništvo v oblaku v pojem kibernetske kriminalitete, katera kazniva dejanja virtualnega sveta poznamo, opredelila digitalno forenziko in elektronske dokazeter obravnavala izzive in elementi, ki vplivajo na pregon in preiskovanje kriminalitete v oblaku. V drugem delu pa se bom posvetila z zasebnostjo povezanim vprašanjem, ki se odpirajo z metodami pridobivanja digitalnih dokazov kot posegi v oblaku. Po splošni opredelitvi zasebnosti, bom le-to razmejila na dva aspekta zasebnosti in ju aplicirala na primere sodne prakse in se za namene končnega dela naloge navezala na mednarodno pravno pomoč. Nenazadnje pa se bom posvetila in opredelila do pravnih ter mednarodnih mehanizmov, ki organom pregona omogočajo pridobivanje čezmejnih (elektronskih) dokazov. Kako so ti vpeljani v evropsko in ameriško zakonodajo, ali delujejo, pa bom presodila na koncu naloge.

---

[1] Informacijsko-komunikacijske tehnologije (IKT) je skupen izraz za skupino najrazličnejših računalniških, informacijskih in komunikacijskih naprac, kot tudi aplikacij, omrežij in storitev. URL: https://ii.feri.um.si/sl/studij/osnovni-pojmi-itk/ (14.1.2019).

[2] Kovačič, Nadzor in zasebnost v informacijski družbi, (2006), str. 8.

2. RAČUNALNIŠTVO V OBLAKU

Z razvojem IKT se je razvil internet in posledično tudi računalništvo v oblaku. Ta s pomočjo že obstoječih tehnologij omogoča končnemu uporabniku dostop do njegovega oblaka, kjer ima shranjene dokumente. Dandanes nam ponudniki storitev oblaka[3] nudijo veliko možnosti – npr. Google sam nam omogoča vrsto svojih storitev v okviru *Google apps*[4]; od shranjevanja slik v foto knjižnici *Google Photos*, za shranjevanje datotek nam nudi *Google Drive*, za uporabo spletne pošte *Google Mail*. Potrebujemo le registrirano uporabniško ime, elektronsko napravo in internetno povezavo.

Enotne pravne definicije za opredelitev RO ni, poenostavljeno pa bi lahko RO opredelili kot hiter in preprost dostop do naših podatkov ter aplikacij s pomočjo informacijske tehnologije, kadar koli, s kjer koli na svetu ob uporabi internetne povezave.

Poročilo statističnega portala »Statista« je napovedalo, da bo storitev računalništva v oblaku v letu 2018 uporabljajo 3.6 milijarde uporabnikov, v primerjavi z letom 2013, ko je RO uporabljalo 2.4 milijarde uporabnikov.[5] Cisco[6] ocenjuje, da bo do leta 2021 95% vsega prometa podatkovnih centrov v oblaku in verjetno je reči, da bo ta odstotek kaj kmalu narastel na 100%.[7] Strokovnjaki ocenjujejo, da bo do leta 2020 celotni trg vreden čez 250$ milijard in do 2021 preko 300$ milijard.[8]

2.1. KONCEPT IN GLAVNE ZNAČILNOSTI RAČUNALNIŠTVA V OBLAKU

Med vsemi definicijami prevladuje definicija Nacionalnega inštituta za standarde in tehnologijo[9] iz leta 2011, ki opredeljuje RO kot »model, ki s kjer koli in kadar koli omogoča vseobsegajoči, praktični dostop na zahtevo do skupine prilagodljivih računalniških virov, kot so npr. omrežja, strežniki, pomnilniki, aplikacije in storitve, ki so v skupni rabi. Viri so hitro prilagodljivi in omogočajo uporabo z minimalnim upravljanjem ali ponudnikovim posredovanjem«.[10] Ponudniki uporabe omrežij[11] (ang. *CSP*) so ponudniki oddaljenih strežnikov, ki jih gostijo na

---

[3] Največji ponudniki oblačnih storitev so AWS (Amazon Web Services), Microsoft Azure, Google Cloud, Salesforce in IBM. URL: https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-salesforce-dominates-saas/ (21.9.2019).

[4] Ime za skupek aplikacij, ki jih ponujajo.

[5] URL: https://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/ (20.2.2019).

[6] Cisco Systems, Inc. je ameriška multinacionalka, vodilni svetovni »ponudnik rešitev« (kot sami sebe opisujejo), na področju IT, omrežij in kibernetske varnosti. Cisco razvija, proizvaja in prodaja omrežno strojno opremo, telekomunikacijsko opremo in druge storitve ter izdelke visoke tehnologije. URL: www.cisco.com (15.1.2019).

[7] B. Schafer, How far can Cloud Computing go?, URL: https://marketbrothersmedia.com/how-far-can-cloud-computing-go/ (3.6. 2019).

[8] Ibidem.

[9] Ang. *»National Institute of Standard Technology«, (v nadaljevanju NIST).*

[10] *»Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*." P. Mell, J. Grance, The NIST Definition of Cloud Computing, URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (12.2.2019).

internetu, da shranjujejo, upravljajo in obdelujejo podatke, bodisi na lokalnem strežniku ali na osebnem računalniku[12].

NIST je v svoji definiciji določil tudi pet bistvenih značilnosti računalništva v oblaku[13]:

1. »samopostrežba« na zahtevo: uporabnik storitev RO lahko po potrebi, enostransko in brez poseganja ponudnika PUO spreminja oziroma zakupi računalniške zmogljivosti, ki jih od njega najema;
2. »širok mrežni dostop«: uporabnik lahko preko internetnega omrežja in digitalne IKT dostopa do podatkov oziroma storitev od kjer koli, kadar koli po svetu;
3. »združevanje virov«: »je bistvena lastnost računalništva v oblaku, kadar več uporabnikov hkrati pristopa do istih tehnoloških virov«[14]. Pri tem več uporabnikov oziroma odjemalcev lahko uporablja isti server ponudnika storitev v oblaku (angl. *multi-tenant cloud*[15]), pri tem izgubijo dejanski nadzor in informacijo o točni lokaciji podatkov[16];
4. »prilagoditev zmogljivosti«: glede na svoje povpraševanje in potrebe, se lahko zmogljivosti najetih storitev po željah uporabnika spreminjajo hitro in prilagodljivo;
5. »merljiva« storitev: preko samodejnega natančnega nadziranja in optimiziranja z merljivimi storitvami lahko oblačni sistemi spremenijo vire, primerne glede na vrsto storitve, kar omogoča plačilo glede na porabo. Tako zagotavljajo transparentnost ponudnika kot tudi odjemalca storitev.

Islovar[17] »oblak« definira kot: oblák -a [Obla:k] m (angl. *Cloud*) programske rešitve, računalniška okolja in informacijska infrastruktura, ki so na voljo kot storitev prek omrežja.

2.2. STORITVENI MODELI

Infrastruktura oblaka[18] je sestavljena iz strojne opreme[19], platforme[20] in uporabniške programske opreme[21]. Zdaj že uveljavljena klasična delitev RO deli različne storitvene modele glede na *obseg storitev*, ki jih PUO lahko

---

[11]V nadaljevanju naloge bo uporabljen tudi izraz »ponudnik storitev«, »ponudnik oblačnih storitev« ali samo okrajšava PUO, ki je sopomenka ponudnikom uporabe omrežij.

[12] URL: https://searchitchannel.techtarget.com/definition/cloud-service-provider-cloud-provider (12.2.2019).

[13] P. Mell, J. Grance, The NIST Definition of Cloud Computing, URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (12.2.2019).

[14] Varstvo osebnih podatkov in računalništvo v oblaku, smernice Informacijskega pooblaščenca, 2012, str. 5. URL: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_rac_v_oblaku.pdf (12.2.2019)

[15] *Multi-tenant cloud,* slov. »oblak z več najemniki« je arhitektura računalništva v oblaku, ki strankam omogoča skupno rabo računalniških virov v javnem ali zasebnem oblaku. Podatki vsakega najemnika so izolirani in ostajajo nevidni drugim najemnikom. V oblačnem sistemu z več najemniki imajo uporabniki individualiziran prostor za shranjevanje svojih projektov in podatkov. URL: https://searchcloudcomputing.techtarget.com/definition/multi-tenant-cloud (21.9.2019).

[16] URL: https://www.techopedia.com/definition/29545/resource-pooling (12.2.2019).

[17] Islovar je terminološki slovar informatike, razlagalni in informativni slovar, ki strokovno izrazje pomensko in jezikovno opisuje, vrednoti in kateremu so dodani angleški ustrezniki, navadno kot ameriška različica. URL: http://www.islovar.org/islovar (12.2.2019)

[18] URL: https://searchcloudcomputing.techtarget.com/definition/cloud-infrastructure (10.9.2019).

[19]ang.»*hardware*«; strojna oprema in računalniška strojna oprema. URL: http://www.islovar.org/islovar (12.2.2019).

[20]ang.»*middleware*«; programska oprema, ki povezuje posamične programe, programske komponente. URL: http://www.islovar.org/islovar (12.2.2019).

ponudi svojim uporabnikom, in sicer na: infrastruktura kot storitev, platforma kot storitev ter *software* kot storitev.[22]

1. SaaS[23] (slov. *Programska oprema kot storitev)* – je model RO, pri katerem PUO ponuja uporabniku dostop do uporabniške programske opreme, kar tudi dovoljuje uporabniku dostop do že izoblikovanih aplikacij v oblaku ter njenih podatkov oz. zmogljivosti, s katere koli naprave povezane na internet. Tukaj uporabnik nima nobene kontrole nad uporabo oz. nastavitvami oblačnih virov, ima le prosti dostop do aplikacij preko brskalnika ter dostopa do interneta. Ta model RO je med končnimi uporabniki najbolj priljubljen, saj od njega ne zahteva dodanega tehničnega znanja ali dodatnih prispevkov k izoblikovanju aplikacije. Primer SaaS je npr. Google apps (Gmail), Microsoft (npr. Office 365).
2. PaaS[24] (slov. *Platforma kot storitev)* – je model RO, pri katerem ima uporabnik bolj proste roke pri oblikovanju aplikacij na najeti infrastrukturi ponudnika, vendar potrebuje za to že določeno strokovno znanje. Aplikacije lahko izoblikuje z uporabo programskih jezikov, datotek, storitev in orodij, ki jih zagotovi ali omogoči ponudnik RO ali pa jih uporabnik razvije sam. Uporabnik pa tudi tukaj nima možnosti prilagaditve nastavitev strežnika ali pomnilnika. Primer PaaS je npr. Windows Azure.
3. IaaS[25] (slov. *Infrastruktura kot storitev*) – je najbolj osnovni model RO, ki pa je med vsemi modeli najmanj uporabljen. Čeprav daje uporabniku največ svobode pri izbiri načina uporabe virov, zahteva od njega tudi največ strokovnega znanja. Tu mu PUO nudi zgolj uporabo strežnika, procesorja, pomnilnika, uporabnik pa mora sam zagotoviti storitve, vključno z operacijskim sistemom. Primer IaaS je npr. Amazon AWS.

Po nekaterih raziskavah je bilo v letu 2018 kar 160 milijard dolarjev porabljenih za storitve in infrastrukturo RO, kar 23,2% povečanje v primerjavi z letom 2017.[26]

2.3. IZVEDBENI MODELI

Izvedbeni modeli se razlikujejo glede na to, kakšen dostop ima lahko nekdo do oblaka oz. do sheme delitve virov. Na posamezno vrsto izvedbenega modela se nanašajo tudi različne stopnje tveganj glede varnosti ter zasebnosti informacij shranjenih v oblaku. Na splošno se izvedbeni modeli delijo na[27]:

1. Javni oblak[28]– viri javnega oblaka so dostopni preko interneta širši javnosti, brez omejitev kdo jih lahko vse uporablja. Je najbolj poznana in razširjena vrsta RO, ki pa glede varnosti predstavlja največje tveganje.

---

[21]ang.»*application software*«: programska oprema, namenjena uporabnikom. URL: http://www.islovar.org/islovar (12.2.2019).
[22]P. Mell, J. Grance, The NIST Definition of Cloud Computing, 2011, str. 2-3.
[23]ang. »*software as a service*«
[24]ang. »*platform as a service*«
[25]ang. »*infrastructure as a service*«
[26]B. Darrow, *Yes, the cloud computing category can grow (almost) forever*, 2018. Spletni vir: https://www.cio.com/article/3268684/budget/yes-the-cloud-computing-category-can-grow-almost-forever.html. (februar 2019)
[27] P. Mell, J. Grance, The NIST Definition of Cloud Computing, URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (12.2.2019).
[28] *ang. »Public Cloud«*

2. Zasebni oblak[29] – viri zasebnega oblaka so dostopni le določenemu krogu omrežja znotraj posamezne organizacije. Pomeni, da je infrastruktura v zasebni lastni podjetja, upravljanje storitev pa je lahko zaupano tudi tretjemu. Ker je tu dostop omejen le na določeno število uporabnikov oz. na prav določeno osebo, je primeren za tiste, ki si želijo svoj oblak, storitve pa bodo dosegljive preko interneta ali preko navidezno zasebnih omrežij. Pri vpeljavi zasebnega oblaka v organizacijski proces podjetja strokovnjaki svetujejo podelitev avtoriziranega dostopa dotičnim zaposlenim (dejstvo je, da le redki potrebujejo dostop do vseh informacij celotnega podjetja), saj v nasprotnem primeru lahko pride do groženj izliva podatkov s strani zaposlenih oz. »notranjih akterjev« v podjetju.
3. Skupnostni oblak[30] - je sestavljen iz več zasebnih oblakov in je dostopen skupinam, organizacijam oz. podjetjem, ki imajo skupne značilnosti oz. jih povezujejo isti interesi. Delijo si infrastrukturo, ki jo lahko upravljajo sami ali pa nekdo tretji, ta pa je lahko locirana v njihovih prostorih ali pa pri samem upravljalcu. Tudi pri tej vrsti oblaka strokovnjaki svetujejo nadzorovano podelitev avtoriziranega dostopa zaposlenim.
4. Hibridni oblak[31] - je kombinacija dveh ali več oblakov (po navadi javnega in zasebnega oblaka), kjer subjekti določenega oblaka ohranjajo svojo edinstvenost, čeprav so »zvezani« še z drugim oblakom.

Izmed vseh storitvenih oblik ima zasebni oblak še nekako najvišjo stopnjo kontrole oz. zasebnosti, v nasprotju z javnim oblakom, ki jo ima še najmanj. Nekje vmes je hibridni oblak, ki je po definiciji kombinacija več oblakov skupaj.

2.4. PREDNOSTI IN SLABOSTI OBLAKA

2.4.1 Prednosti

Najverjetneje največja prednost koriščenja storitev v RO je *prihranek stroškov*. Dejstvo je, da uporabniki, tako posamezniki kot podjetja, pri svojem delovanju stremijo k zaslužku s hkratnih ohranjanjem kapitalskih in operativnih stroškov na minimumu[32]. Če to apliciramo na uporabo oblaka kot storitve, ugotovimo, da le-ta temelji na uporabi oddaljenih strežnikov[33] (angl. *server storage*), kar posledično za uporabnike pomeni, da ne potrebujejo v podjetju fizično svojih strežnikov oz. dodatnih zahtev glede aplikacij. To dejstvo predstavlja zelo velik prihranek operativnih stroškov, v smislu, da ne potrebujejo plačevati dodatne elektike, prezračevanja teh prostorov in s tem povezanih administrativnih stroškov. Stranka plačuje le toliko, kot tudi koristi storitve oblaka.

Dodatna zelo pomembna prednosti uporabe oblaka prav njegova *dostopnost* s kjer koli, kadar koli po svetu preko internetne povezave. Podatki so varovani v samem oblaku, za kar je zadolžen prav ponudnik storitev v okviru njegove Pogodbe s stranko.

---

[29] *ang. »Private Cloud«*
[30] *ang. »Community Cloud«*
[31] *ang. »Hybrid Cloud«*
[32] URL: https://www.esds.co.in/blog/the-cost-benefits-of-cloud-computing/ (10.9.2019).
[33] Strežnik za shranjevanje je vrsta strežnika, ki se uporablja za shranjevanje, dostop, varnost in upravljanje digitalnih podatkov, datotek in storitev. Namenjen je strežniku, ki se uporablja za shranjevanje in dostop do majhnih do velikih količin podatkov v skupni mreži ali prek interneta. Strežnik za shranjevanje se lahko imenuje tudi datotečni strežnik. URL: https://www.techopedia.com/definition/9550/storage-server (10.9.2019).

Čeprav literatura[34] opredeljuje še številne prednosti RO, pa so elementi *večje učinkovitosti, računalniške moči in lažjega vzdrževanja* eni izmed pomembnejših. Preko ponudnika storitev je upravljanje s storitveno platformo oblaka veliko bolj *zanesljivo, poenostavljeno in dosledno* kot pa s samo notranjo informacijsko infrastrukturo. Odvisno od Pogodbe o ravni storitve[35] (angl. *service-level agreement – SLA*, v nadaljevanju Pogodba) pa večina ponudnikov nudi upravljanje, ki zagotavlja 24/7/365 in 99,99% razpoložljivost. Ponudnik storitev je tako zadolžen za posodobitev in vzdrževanje IT infrastrukture, hkrati pa opravi vse potrebno, da je za stranko dostop do programske opreme, aplikacij in storitev popolnoma enostaven.

2.4.2. Slabosti

Uporabo informacijske tehnologije spremljajo tako prednosti, kot tudi slabosti, in oblak ni tukaj nobena izjema. Kljub vsem prednostim koriščenja storitev ponudnika oblaka, smo pri uporabi le-tega *popolnoma odvisni od dostopnosti do internetnega omrežja*. Že res, da lahko dostopamo do oblaka od kjer koli, s kjer koli po svetu, vendar samo ob uporabi internetne povezave[36].

Ponudniki storitev stremijo k zagotavljanju dostopnosti storitev oblaka ves čas oziroma v skladu s Pogodbo. Kljub skrbnemu upravljanju in vzdrževanju storitev se vendarle lahko pripeti, da postanejo ponudniki preobremenjeni, kar lahko vodi v *service downtime*[37]. To za stranko pomeni začasno prekinitev njenih poslovnih procesov in nezmožnosti dostopa do podatkov.[38]

Ker je infrastruktura v oblaku v celoti v lasti, upravljanju in spremljanju PUO, prenese na stranko minimalen nadzor nad podatki. Stranka pri posredovanju gradiva v omrežje oblaka (angl. *upload*) izgubi dejanski nadzor nad podatki in ne more vedeti, kje se ti geografsko nahajajo, nadzoruje lahko le tiste aplikacije, podatke in storitve, ki jih upravlja sama in ne same infrastrukture kot take. To pomeni, da ima *omejen nadzor nad podatki* v oblaku.

Slabost, ki spremlja oblak je tudi njegova vprašljiva prenosljivost (angl. *vendor lock-in)*[39]. Za zaklep prodajalca gre v primeru, ko stranka koristi oblačne storitve enega ponudnika storitev in želi prenesti svoje podatke na drugega, ob tem pa naleti na velike tehnične težave, da ne govorimo o izjemnih finančnih stroških. To je lahko velika ovira oz. prepreka predvsem zaradi pomanjkanja standardizacije. Čeprav ponudniki storitev

---

[34] URL: https://www.ibm.com/cloud/learn/benefits-of-cloud-computing. (10.9.2019).
[35] Pogodba (lahko tudi Dogovor) o ravni storitve je pogodba med ponudnikom storitve in stranko, v kateri se določijo bistveni elementi o koriščenju oblaka kot storitve glede razpoložljivosti, možnosti upravljanja in delovanja. URL: https://cloud.oracle.com/sl_SI/iaas/sla (10.9.2019).
[36] Res pa je, da nekatere aplikacijo omogočajo *download* (slov. *naložitev*) svojih storitev na elektronski nosilec, katere lahko uporabljamo tudi, ko nimamo internetne povezave (npr. Google maps, Netflix, Google doc itd).
[37] Slov. *čas onesposobljenosti.* Nekateri ponudniki storitev v pogodbi o zagotavljanju storitev zagotavljajo 99,99% razpoložljivost storitev, kar se v primeru *downtime-a* lahko izkaže kot zelo draga določba v obliki visoke povrnitve stroškov glede izpada dobička podjetja. Vir: https://www.networkworld.com/article/3394341/when-it-comes-to-uptime-not-all-cloud-providers-are-created-equal.html (september 2019).
[38] Ibidem.
[39] »Zaklep prodajalca« je omejena ali lastniška uporaba tehnologije, rešitve ali storitve, ki jo je razvil prodajalec. Ta tehnika je lahko onesposobljena in demoralizirana, ker kupcem učinkovito preprečimo prehod na nadomestne prodajalce. Vključitev prodajalca je znana tudi kot lastniško zaklepanje ali zaklepanje kupca. (primer: Microsoft, Apple). URL: https://www.forbes.com/sites/forbestechcouncil/2017/12/14/four-ways-to-avoid-vendor-lock-in-when-moving-to-the-public-cloud/#39272d1261f9 (8.6.2019). URL: https://en.wikipedia.org/wiki/Vendor_lock-in (8.6.2019).

obljubljajo, da bo oblak prilagodljiv za uporabo in integracijo, je zamenjava oblačnega ponudnika nekaj, kar še ni popolnoma razvilo. Gostovanje in integracija trenutnih aplikacij v oblaku na drugi platformi lahko povzroči neskladje pri uporabi in težave pri podpori. Na primer aplikacije, razvite v Microsoftovem razvojnem okviru (.Net), morda ne bodo delovale pravilno na platformi Linux.

3. FENOMEN RAČUNALNIŠTVA V OBLAKU KOT IZZIV KAZENSKEMU PREGONU IN PREISKOVANJU

Z do sedaj opisanimi karakteristikami računalništva v oblaku je jasno, da le-ta spada v t.i. virtualni oziroma kibernetski prostor. Ta z uporabo moderne tehnologije omogoča uporabnikom številne prednosti, hkrati pa odpira storilcem[40] kibernetskih kaznivih dejanj (v nad. KKD) nove priložnosti za kibernetsko kriminaliteto, pojav novih KKD in uporabo novih tehnik za izvršitev KD, ki so nam že poznana.

Pregon in preiskovanje KD, ki jih uvrščamo v skupino kibernetske kriminalitete je vse prej kot enostaven, saj so elementi kibernetskega sveta v katerem domuje oblak popolnoma drugačni od fizičnega sveta, kar posledično vpliva na definiranje novih pojavnih oblik kaznivih dejanj, uporabo novih vrst dokazov na sodišču, vprašanja jurisdikcije itd.

Na kakšen način računalništvo v oblaku predstavlja izziv pregonu in preiskovanju kaznivih dejanj je sestavljeno iz več vidikov, ki se med seboj prepletajo in dopolnjujejo. Za lažje razumevanje izzivov, ki vplivajo na pregon in preiskovanje moramo najprej opredeliti pojem kibernetske kriminalitete.

3.1. KIBERNETSKA KRIMINALITETA

Pojem »kibernetska kriminaliteta«[41] (ang. *cybercrime*) se je uveljavil pod vplivom Konvencije Sveta Evrope o kibernetski kriminaliteti iz leta 2001 (Budimpeška konvencija, v nadaljevanju Konvencija)[42], ki kot prvi mednarodni akt obravnava področje kibernetske kriminalitete, pred tem pa teorija glede poimenovanja ni bila enotna. V slovenskem prostoru Jakulin zagovarja poimenovanje »kriminaliteta v zvezi z računalniki« in s tem zavrača poimenovanje »računalniške kriminalitete« kot preozko, saj naj bi se to opiralo zgolj na dejanja, pri katerih računalnik nastopa kot sredstvo storitve[43]. Kazenskopravna teorija je predlagala uporabo pojma kriminaliteta, povezana z računalniki (angl. *computer-related* crime)[44]. Brvar zagovarja opredelitev, ki zajema

---

[40] Storilci običajno izvajajo kibernetska KD s pomočjo škodljivih računalniških programov, tipično z računalniškimi črvi, virusi, vohunskimi programi itd. URL: https://www.pomagalnik.com/izobrazevanje/virusi-skodljivi-programi/ (21.9.2019). Storilce kibernetske kriminalitete pogosto imenujemo »heker« (angl. *hacker*), t.j. posameznik, ki ga SSKJ slovar definira kot (1) nekoga, ki vdira v tuje računalniške sisteme ali (2) kdor z navdušenjem spreminja programsko opremo. Poenostavljeno bi lahko to dejavnost opisali kot nekakšno reševanje tehničnega problema na drugačen, samosvoj način, saj oseba na podlagi znanja izvaja izvirne modifikacije sistema ter programov. Repinc opozarja, da se je pojavom kibernetske kriminalitete za osebe, ki kriminalno vdirajo v računalniške sisteme in izrabijo varnostne sisteme brez pooblastil in/ali uporabljajo IKT za vlamljanje in izvajanje nelegalnih ali kriminalnih dejanj idp. uveljavil izraz »kreker« (angl. *cracker*) ali po slovensko »vdiralec«. J. Repinc, Odprto pismo medijem glede zlorabe termina »heker«, URL: http://www.lugos.si/novice/odprto-pismo-medijem-glede-zlorabe-termina (10.6. 2019). Več o razliki med hekerji in krekerji: A. Završnik, Kibernetska kriminaliteta (2015), str 16, prav tam.

[41] URL: https://www.techopedia.com/definition/2387/cybercrime (13.6.2019)

[42] Konvencija o kibernetski kriminaliteti (angl. *Convention on Cybercrime*) je stopila v veljavo 1. julija 2004, v Sloveniji velja od 1. januarja 2005. Konvencija o kibernetski kriminaliteti, Uradni list RS – Mednarodne pogodbe, št. 17/04.

[43] V. Jakulin, Kazenskopravni vidiki, v: Podjetje in delo, 22 (1996) 5/6, str. 823-824.

[44] A. Završnik, Kibernetska kriminaliteta (2015), str. 11, prav tam.

kazniva dejanja, pri katerih računalnik bodisi nastopa kot sredstvo (orodje) izvršitve ali pa kot predmet (cilj oziroma tarčo) napada, pri čemer mora imeti storilec posebna znanja, ki mu to omogočajo[45].

Enotne opredelitve za kibernetsko kriminaliteto ni[46], zelo poenostavljeno pa bi jo lahko opisala kot kriminaliteto, ki se izvaja preko spleta s pomočjo elektronskih nosilcev podatkov, bodisi za izvrševanje nam že poznanih kaznivih dejanj ali pa novih kaznivih dejanj na prikrit in zelo pretkan način.

V teoriji se je na podlagi Konvencije uveljavila naslednja delitev kibernetske kriminalitete (v širšem smislu)[47]:

1. kriminaliteta, povezana s celovitostjo informacijskega sistema in podatkov (kibernetska kriminaliteta v ožjem smislu); IKT je pri tem tarča napada v obliki ogrožanja bodisi zaupnosti računalniških podatkov ali informacijskega sistema bodisi njihove integritete ali dostopnosti;
2. kriminaliteta, povezana z vsebino (spolno in nasilno vsebino in kršitvami pravic intelektualne lastnine);
3. kriminaliteta, povezana z računalniki: IKT je orodje za izvršitev konvencionalne kriminalitete.

3.1.1. Objekt kazenskopravnega varstva

Konvencija opredeljuje termina »računalniški sistem« in »računalniški podatek«[48], kasnejša Direktiva o napadih na informacijske sisteme[49] iz 2013 nadgrajuje Konvencijo, saj širi[50] termin »računalniški sistem« na »informacijski sistem«. Z razširitvijo pojma Direktiva varuje vse računalniške podatke, ki so shranjeni, obdelani, pridobljeni ali se prenašajo po napravi ali skupini naprav zaradi njenega ali njihovega delovanja, uporabe, varovanja in vzdrževanja naprav za samodejno obdelovanje podatkov s pomočjo programa[51], tako da kazenskopravno varstvo po tej opredelitvi obsega večji spekter podatkov kot tudi nosilcev podatkov (osebni računalnik, pametni telefon, računalniška tablica, ipd.) preko katerih se ti prenašajo.

Objekt kazenskopravnega varstva kibernetske kriminalitete so tako: informacijski (komunikacijski) sistem, elektronska komunikacijska omrežja in podatki, ki so shranjeni ali posredovani z njimi. Varuje se integriteta, tj. dostop, zaupnost in celovitost (prepoved prenosa, poškodovanja, izbrisa, poslabšanja, spreminjanja, oviranja) računalniških podatkov in informacijskega sistema.[52]

---

[45] B. Brvar, Pojavne oblike zlorabe računalnika, v:Revija za kriminalistiko in kriminologijo, (1982), str. 94.
[46] A. Završnik, Kibernetska kriminaliteta (2015), str 13.
[47] Prav tam, str. 25.
[48] 1.a tč. 1.člena Konvencije.
[49] Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa 2005/222/HJA. L 218/8. V nadaljevanju Direktiva. URL: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32013L0040&from=SL (12.9.2019).
[50] Direktiva v svoji definiciji za razliko od Konvencije, ki se nanaša le na podatke, katere obdeluje naprava ali skupina naprav, zajema tudi vse podatke, ki niso na samem računalniku na vse tiste, ki so shranjeni, obdelani, pridobljeni in se tudi prenašajo preko te naprave.
[51] 2. člen Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa 2005/222/HJA. V nadaljevanju Direktiva. URL: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32013L0040&from=SL (13.9.2019).
[52] A. Završnik, Kibernetska kriminaliteta, (2015), str. 26.

Računalništvo v oblaku je po tej definiciji objekt kazenskopravnega varstva, saj gre za informacijski sistem, ki omogoča shranjevanje in prenos podatkov preko elektronskih komunikacijskih omrežij in spletnih aplikacij (npr. deljenje datotek v skupno rabo, uporaba elektronske pošte, aplikacij za internetno telefonijo itd).

3.2. KAZNIVA DEJANJA V KIBERNETSKEM PROSTORU

Konvencija deli kibernetska KD v naslednje kategorije (2. do 6. člen)[53]:

1. Kazniva dejanja zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov (kibernetska kriminaliteta v ožjem smislu):
- protipravni dostop/vstop/vdor/napad na informacijski sistem (npr. dostop do podatkov, ki so shranjeni v oblaku),
- protipravno prestrezanje telekomunikacij, ki se lahko odvijajo v obliki internetnega klepeta v realnem času ali v obliki internetne,
- motenje podatkov, sistemov in zloraba naprav;
2. Kazniva dejanja, povezana z računalnikom: računalništvo ponarejanja in računalniška goljufija;
3. Kazniva dejanja, povezana z vsebino: različne oblike kaznivih dejanja, povezanih z otroško pornografijo;
4. Kazniva dejanja, povezana s kršitvijo avtorske in sorodnih pravic.

Po definiciji informacijskega sistema iz Direktive, pojem opredeljuje tudi slovenski Kazenski zakonik (KZ-1)[54] in upoštevajoč sistematiko kaznivih dejanj iz Direktive, umešča med kibernetska kazniva dejanja tri tipe kaznivih dejanj, in sicer (1) dejanja, povezana z računalniki (angl. *computer-related crime*), (2) dejanja posredovanja prepovedanih vsebin s pomočjo informacijske tehnologije (angl. *content-related crime*) in (3) dejanja ogrožanja celovitosti informacijskih sistemov (angl. *integrity-related crime*)[55].

KZ-1 opredeljuje kazniva dejanja, pri katerih je predmet napada informacijski sistem v 221. členu (napad na informacijski sistem), 237. členu (zloraba informacijskega sistema) ter v tretjem odstavku 306. člena (izdelovanja in pridobivanje orožje in pripomočkov, namenjenih za kaznivo dejanja).

Direktiva o napadih na informacijske sisteme prišteva h KD zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov še naslednja dejanja (3.-8. člen):

1. Nezakonit dostop do informacijskih sistemov,
2. Nezakonito poseganje v sistem,
3. Nezakonito poseganje v podatke,
4. Nezakonito prestrezanje,
5. Kazniva dejanja v zvezi s pripomočki, ki se uporabijo za izvršitev dejanj, in
6. Spodbujanje, pomoč in podpiranje ter pomoč pri izvrševanju dejanj.

---

[53] A. Završnik, Kibernetska kriminaliteta, (2015), str. 13-14.
[54] Kazenski zakonik (Ur. l. RS, št. 50/12, 6/16, 54/15, 38/16, 27/17).
[55] K. Šugman Stubbs, P. Gorkič, Dokazovanje v kazenskem postopku, (2011), str. 182.

Preiskovanje in pregon kaznivih dejanj v povezavi z računalnikom v oblaku je tako lahko vezano na kazniva dejanja, ki jih KZ-1 določa v 143. členu (zloraba osebnih podatkov) (1) vdor v računalniško vodeno zbirko podatkov, krajo identitete, v 221. členu (2) napad na informacijski sistem, v 247. členu (3) zlorabo informacijskega sistema in v tretjem odstavku 306. člena (4) izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za storitev kaznivega dejanja.[56]

3.3. DIGITALNA FORENZIKA

Pri preiskovanju kaznivih dejanj, storjenih v virtualnem svetu ali s pomočjo elektronskih naprav se uporabljajo klasični preiskovalni pristopi, ki morajo vsebovati moderne pristope in orodja.[57] Digitalna forenzika je veda, ki zajema vrsto dejanj (zaznavanje, zavarovanje, analiziranje in predstavljanje dokazov v elektronski obliki) z uporabo preiskovalnih in tehničnih tehnik, z namenom pridobiti in zaščititi podatke ter ostalo gradivo, ki nam bo kasneje služilo kot dokazno gradivo.[58] Dimc in Dobovšek pri tem opozarjata, da se pri tem velikokrat ne upoštevata pojma kriminalistične metodike in kriminalistične taktike, s pomočjo katerih lahko sploh izluščimo ustrezno zbrane podatke, ki nam bodo služili kot podlaga za digitalno preiskovanje.[59]

Nadalje Dimc in Dobovšek delita dejavnosti z vpletenostjo elektronskih naprav s kriminalističnega vidika na dva zelo groba dela in sicer na (1) preiskovanje kibernetske kriminalitete, kjer z modernimi pristopi in orodji raziskujejo kibernetska kazniva dejanja in na (2) preiskovanja klasičnih kaznivih dejanj, pri katerih elektronske naprave vsebujejo elektronske sledi ali so uporabljeni kot orodje za storitev KD.[60]

Kot že rečeno, je sam forenzični proces sestavljen iz več dejanj in tako obsega (1) pridobivanje, (2) ohranitev, (3) forenzični pregled, (4) preiskovalno analizo in (5) predstavitev obravnavanih podatkov[61].

Enotne definicije za *cloud forensic* (slov. »oblačno forenziko«) še ni, tako da bom uporabila široko definicijo preučevalcev s tega področja, ki po mojem mnenju ustreza obravnavani temi. Oblačno forenziko preučevalci opredeljujejo kot uporabo digitalne forenzike v oblaku IT okolja, ki je tehnično sestavljena iz hibrida forenzičnih pristopov (npr. oddaljeni, virtualni, omrežni dostop, spremljanje pridobivanja podatkov v realnem času idr., za ustvarjanje digitalnih dokazov[62]

---

[56] A. Završnik, Kibernetska kriminaliteta, 2015, str. 27, op. 33.
[57] M. Dimc, B. Dobovšek, Kriminaliteta v informacijski družbi, Pravne podlage, preiskovanje in zaseg: Preiskovanje kibernetske kriminalitete, (2012), str.169.
[58] Prav tam.
[59] Prav tam.
[60] Prav tam, str.170.
[61] L. Selinšek, Digitalni dokazi in računalniška forenzika, v:Kriminaliteta in tehnologija: kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon?, (2012), str. 98.
[62] K. Ruan, J. Carthy, T. Kechadi, I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results", Digital Investigation, (2013) Vol. 10-1, , pp. 34-43, 2013. URL: https://www.researchgate.net/publication/271603639_Cloud_forensics_definitions_and_critical_criteria_for_cloud_forensic_capability_An_overview_of_survey_results (19.9.2019).

Za potrebe te naloge se bom osredotočila zgolj na prvo dejanje forenzičnega procesa, tj. pridobivanje podatkov oziroma elektronskih dokazov, katere pridobivajo organi pregona za namene preiskovanja in dokazovanja kibernetskih kaznivih dejanj oblaka z uporabo preiskovalnih dejanj in ukrepov.

3.3.1. Elektronski dokazi

Z vsemi naloženimi elektronskimi podatki na nosilcu podatkov ali v pa oblaku, je ta postal nekakšna neomejena shramba raznih podatkov, ki se odraža v obliki pomembnih dokumentov, slik, zvočnih posnetkov ipd. V postopku preiskovanja in dokazovanja kibernetskih kaznivih dejanj lahko organi do njih pridejo na različne načine, posledično se lahko kasneje ti podatki uporabijo na sodišču kot dokazi. Ker so podatki digitalizirani, govorimo v kontekstu preiskovanja kaznivih dejanj o elektronskih (tudi digitalnih) dokazih, katere preiskuje t.i. digitalna forenzika[63].

Digitalni dokazi so vrsta elektronskih dokazov, brez katerih praviloma ni mogoče preiskovati kibernetske kriminalitete[64]. S pravnega vidika so elektronski dokazi proizvod analogne naprave ali podatek v digitalni obliki, ki je ustvarjen, spremenjen, shranjen ali povezan s kakršnokoli napravo, računalnikom ali računalniškim sistemom oz. se prenaša po komunikacijskem sistemu in je relevanten za proces razsojanja. Elektronski dokazi vsebujejo tako analogne kot tudi digitalne dokaze, kot sopomenka pa se pogosto uporablja izraz digitalni dokaz.[65]

Za digitalni dokaz veljajo enaka splošna pravila kot za druga dokazna sredstva. Da se bo lahko dokaz uporabil na sodišču, mora v splošnem izpolnjevati dva pogoja, in sicer (1) mora biti pravo dopusten in (2) imeti mora ustrezno dokazno vrednost, kar velja tudi za digitalni dokaze. [66] Zaradi možnosti, ki nam jih omogoča moderna tehnologija se glede svoje pravne dopustnosti in dokazne vrednosti digitalni vseeno razlikujejo od klasičnih dokazov.[67]

3.3.2. Pridobivanje elektronskih dokazov

Kot že omenjeno, se elektronski podatki, ki bodo kasneje služili v postopku kot dokazi, lahko nahajajo na elektronskem nosilcu podatkov ali pa v samem oblaku.

Elektronske naprave oziroma nosilce podatkov, ki jih storilci uporabljajo, je mogoče pridobiti na tri načine[68]:

1. Lahko se zasežejo na nek način samostojno, npr. so najdeni na kraju KD (lahko jih predajo oškodovanci, priče ali osumljenci),

---

[63] URL: https://sl.wikipedia.org/wiki/Digitalna_forenzika (20.9.2019).
[64] A. Završnik, Kibernetska kriminaliteta, (2015), str. 64.
[65] L. Selinšek, Digitalni dokazi in računalniška forenzika, v:Kriminaliteta in tehnologija: kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon?, (2012), str. 97.
[66] L. Selinšek, 2010, Digitalni dokazi v kazenskem postopku: pogledi na aktualna vprašanja, str. 100.
[67] Več: L. Selinšek, 2010, Digitalni dokazi v kazenskem postopku: pogledi na aktualna vprašanja, str. 100-101.
[68] M. Dimc, B. Dobovšek, Kriminaliteta v informacijski družbi, Pravne podlage, preiskovanje in zaseg: Preiskovanje kibernetske kriminalitete, (2012), str.174.

2. Zasežejo se lahko pri osebnem pregledu, pregledu vozila ali pregledu prostorov (pri tem ne gre za preiskavo), in

3. Lahko se jih pa zaseže pri hišni preiskavi, osebni preiskavi ali preiskavi vozila.

Za preiskovalno dejanje preiskave se zahteva obstoj utemeljenih razlogov za sum in obstoj verjetnost, da bo mogoče pri preiskavi prostorov obdolženca prijeti ali da se bodo odkrili sledovi KD ali predmeti, ki so pomembni za kazenski postopek. Zadnja dva razloga verjetnosti sta nujen pogoj tudi pri osebni preiskavi.[69] Sama preiskava elektronske naprave se lahko opravi tako, da se (1) napravo oziroma celoten sistem zaseže in preišče v prostorih organa, lahko se (2) preišče naprava na lokaciji, (3) zaseže se le del naprave, tj. samo iskane podatke, ki se preišče na lokaciji ali pa se (4) del zaseženih iskanih podatkov preišče v prostorih organa.[70]

V postopku preiskovanja oblačnih kibernetskih KD lahko organi pregona pridobivajo elektronske dokaze z uporabo preiskovalnih dejanj in ukrepov, ki se nanašajo bodisi na samo elektronsko napravo, ki vsebuje elektronske dokaze ali pa te relevantne podatke pridobijo neposredno od ponudnikov storitev v oblaku.

Metode preiskovanja kibernetskih forenzičnih podatkov so[71]:

1. pridobivanje podatkov od osumljenca s prikritim (kibernetskim) nadzorom,
2. pridobivanje podatkov od ponudnikov storitev in
3. prisilno pridobivanje podatkov od osumljenca s preiskavami in zasegi (npr. pri hišni in osebni preiskavi, preiskavi vozila).

Obstajata dva tipa računalniških podatkov, ki jih lahko pridobivajo računalniški forenziki[72]:

1. Podatki, ki so shranjeni na nekem nosilcu podatkov v digitalnem zapisu (angl. *data at rest*, slov. *shranjeni podatki*) in
2. Podatki, ki se prenašajo z enega nosilca podatkov na drugega, na primer po telekomunikacijskem omrežju ali internetu t.i. *tranzitni podatki* (angl. *data in motion, data in transmission, data in transit*).

Shranjeni podatki se pridobivajo z zasegom in preiskovanjem elektronske naprave, tranzitni podatki pa z drugimi metodami, npr. s prisluškovanjem oziroma nadzorovanju strežnika, več o preiskovanju tranzitnih podatkov v poglavju varstva komunikacijske zasebnosti. Z novelo ZKP-J[73] sta bila v ZKP vnesena člena 219. a in 223. a, ki vsebujeta določbe in smernice o zasegu elektronskih naprav, zavarovanju podatkov v njih in o njihovi preiskavi.

Pridobivanje teh digitalnih dokazov pri preiskovanju kibernetskih kaznivih dejanj oblaka pa je vse prej kot enostavno ob upoštevanju elementov kibernetskega sveta, splošno uveljavljenih materialno in procesno pravnih teorij, saj so te ves čas prisiljene se adaptirati digitalizaciji izvrševanju novodobnih virtualnih kaznivih dejanj.

---

[69] 214. ZKP-N.
[70] M. Dimc, B. Dobovšek, Kriminaliteta v informacijski družbi, Pravne podlage, preiskovanje in zaseg: Preiskovanje kibernetske kriminalitete, (2012), str.175.
[71] A. Završnik, Kibernetska kriminaliteta, (2015), str. 65.
[72] K. Šugman Stubbs, Nove tehnologije in njihov vpliv na pojavnost in pregon kriminalitete, v: Zbornik znanstvenih razprav – LXXIII. letnik, (2013), str 197.
[73]Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku, Ur. L. RS št. 77/2009.

3.4. ZAKAJ JE PREISKOVANJE KAZNIVIH DEJANJ IZ OBLAKA ŠE TOLIKO VEČJI IZZIV KAZENSKEMU PREGONU?

S prednostmi, kot so prihranek stroškov, enostavna dostopnost in odsotnost vzdrževanja je uporaba oblaka kot storitve nadvse priročna in ekonomična. Hkrati pa fenomen oblaka spremljajo številni izzivi, ki so jih prepoznali preučevalci RO, predvsem zaradi načina hrambe in narave podatkov, na katere pa sodobno (kazensko) pravo še nima odgovorov. Preiskovanje in dokazovanje kibernetske kriminalitete predstavlja za organe kazenskega pregona poseben izziv[74], saj na zapletenost preiskovanja vpliva veliko dejavnikov, glede katerih nam sodna praksa še ni ponudnika jasnih odgovorov.

Elementi kibernetskega sveta, ki so pomembni za razumevanje izzivov pri pregonu kibernetske kriminalitete računalništva v oblaku[75]:

1. Praviloma (ne pa nujno) kibernetska KD predstavljajo tipični primer t.i. *cross-border* kriminala oziroma čezmejne kriminalitete.[76] V takem primeru gre za kazniva dejanja z mednarodnim elementom, ki je za *vprašanje jurisdikcije* takih KD ključnega pomena.[77] Sodna praksa nam še ne more ponuditi točnih pravil in vpogleda glede uporabe jurisdikcije za kazniva dejanja, ki spremljajo kibernetsko kriminaliteto iz oblaka[78]. Oblak temelji na razpršenosti podatkov po celem svetu in v tem smislu se jurisdikcijska pravila uporabljajo bodisi preširoko ali preozko. Gorkič[79] pri odgovoru na vprašanje glede določanja jurisdikcije izpostavlja dva problema: (1) preširoka uporaba kazenskega zakona lahko privede do konkurence jurisdikcij za kibernetsko kriminaliteto[80], (2) preozka uporaba teh pravil pa lahko privede do izogibanja pregonu storilca[81]. Rešitev na ta dva problema vidi v ožjem tolmačenju teritorialnega načela krajevne veljavnosti kazenskega zakona, saj zgolj potencialni dostop do podatkov (*kraj prikljicljivosti*)[82] širi kraj nastanka posledice, kar občutno povečuje nevarnost za konkurenco jurisdikcij. Kot drugo rešitev vidi v tesnejšem in aktivnejšem mednarodnem sodelovanju v okviru mednarodne pravne pomoči v kazenskih zadevah[83].
2. Dejstvo je, da zakonodaja vedno zaostaja za hitrim tehnološkim napredkom in novimi pojavnimi oblikami kaznivih dejanj;

---

[74] K. Šugman Stubbs, P. Gorkič: Dokazovanje v kazenskem postopku, (2011), str. 182.
[75] K. Šugman Stubbs, Nove tehnologije in njihov vpliv na pojavnost in pregon kriminalitete, v: Zbornik znanstvenih raprav – LXXIII. letnik, (2013), str 195.
[76] Gorkič, Nekatera vprašanja jurisdikcije za kazniva dejanja kibernetične kriminalitete, v:Zbornik znanstvenih razprav – LXVII. letnik, (2007), str. 74.
[77] Prav tam.
[78] M. Kržišnik, Legal challenges of Cloud computing. URL: https://www.linkedin.com/pulse/cloud-computing-mina-kr%C5%BEi%C5%A1nik-fintech-lawyer/ (18.9.2019).
[79] Gorkič, Nekatera vprašanja jurisdikcije za kazniva dejanja kibernetične kriminalitete, v:Zbornik znanstvenih razprav – LXVII. letnik, (2007), str. 73 – 93.
[80] Tj. v primeru, da več držav uveljavlja svojo pristojnost. V tem primeru gre lahko kršitev temeljnega načela *ne bis in idem*.
[81] Tj. kadar nobena država ne uveljavlja svoje pristojnosti.
[82] P. Gorkič, Nekatera vprašanja jurisdikcije za kazniva dejanja kibernetične kriminalitete, v:Zbornik znanstvenih razprav – LXVII. letnik, (2007), str. 83.
[83] Že 5. odstavek 22. člena Konvencije o kibernetski kriminaliteti opredeljuje medsebojno posvetovanje, v primeru da več držav uveljavlja sodno pristojnost glede domnevnega KD.

3. Klasični pravni koncepti in pravila dokazovanja so se izoblikovali na podlagi realnosti fizičnega sveta in ne virtualnega, kar se najbolj vidi pri dokazovanju z elektronskimi dokazi;
4. Standardizacija programske opreme omogoča nastanek veliko večjega obsega posledic kibernetskih KD in je neprimerljivo večji kot pri klasični kriminaliteti;
5. Vprašanje identitete oziroma anonimnost storilca/žrtve in odsotnost fizičnega stika med storilcem in žrtvijo. Pri preiskovanju in dokazovanju moramo vzpostaviti povezavo med podatki, ki jih zberemo s preiskovalnimi dejanji (navadno bo šlo za virtualno identiteto, saj storilci uporabljajo tehnike, ki jim omogočajo večje možnosti za prikrivanje kriminalitete) in o njegovi dejanski identiteti, ki omogoča preiskovalcem, da določijo in identificirajo obdolženca KD[84]. Storilci lahko preusmerijo svoj IP naslov[85] na več lokacij po celem svetu, uporabljajo ukradene identitete, za onemogočeno sledljivost transakcij uporabljajo anonimne plačilne sistemov (npr. z metodo kriptovalut);
6. Vprašanja glede lokacije podatkov, ki jih preiskovalci potrebujejo v postopku preiskave in dokazovanja. Organi morajo najprej ugotoviti, kje se sploh nahajajo ti podatki;
7. Vprašanja glede uporabe in apliciranja prava v postopku mednarodnega sodelovanja, predvsem glede prikritih preiskovalnih ukrepov;
8. Vprašanja glede narave, integritete, trajnosti in količine podatkov, ki jih pridobivamo v postopku preiskovanja in dokazovanja[86]. Strokovnjaki digitalni forenziki morajo biti poglobljeno podkovani ne le s tehničnem znanjem, vendar tudi glede poznavanja pravnih vidikov preiskave, uporabniškimi pogoji ponudnikov storitev in njihovo politiko, ki se nanaša na varstvo zasebnosti uporabnikov oblačnih storitev ter ostalih odjemalcev (predvsem, če model RO temelji na *multi-tenant* principu[87]);
9. Uporaba in metode enkripcije so oteževalni faktor pri delu forenzičnega preiskovanja, nanašajo se tudi na vprašanje subjektivnega pričakovanja zasebnosti pri varovanju podatkov v oblaku;
10. Pomembne so metode zasegov podatkov za namene kasnejše uporabe v kazenskem postopku.

NIST-ovo poročilo *Cloud Computing Forensic Science Challenges*[88] iz leta 2014 navaja izzive, s katerimi se soočamo pri forenziki oziroma pridobivanju podatkov v oblaku:

1. izziv predstavljajo Pogodbe o ravni storitve s ponudnikom storitev, ki vsebujejo manjkajoče izraze, ki so potrebni za razrešitev forenzičnega preiskovanja podatkov iz oblaka,
2. vprašanja, ki se nanašajo na določanje in reševanje vprašanj pristojnosti in uporabe ustrezne zakonodaje za zakonit dostop do podatkov iz oblaka, zaplembe oblaka in zasega virov, preko katerega se nalagajo potrebni podatki v oblak, pri tem pa lahko zaseg oblaka in zaseg virov v oblaku prekine kontinuiteto poslovanja drugih najemnikov, in
3. pomanjkanje učinkovitih kanalov za mednarodno sodelovanje, kot tudi pomanjkanje komunikacije in sodelovanja med preiskavo;

---

[84] K. Šugman Stubbs, P. Gorkič, Dokazovanje v kazenskem postopku, (2011), str. 182.
[85] IP naslov je številka, ki locira računalnik v omrežju interneta. Podobno kot določa naslov ulice in hišna št. v realnem svetu našo lokacijo.
[86] Več o tem: K. Šugman Stubbs, P. Gorkič, Dokazovanje v kazenskem postopku, (2011), str. 182-183.
[87] Tj. model oblaka z več najemniki, ki omogoča več strankam skupno rabo računalniških virov v javnem ali zasebnem oblaku. Podatki vsakega najemnika so izolirani in ostajajo nevidni drugim najemnikom. URL: https://searchcloudcomputing.techtarget.com/definition/multi-tenant-cloud (18.9.2019).
[88] URL: https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf (18.9.2019).

4. izzivi pri pridobivanju podatkov, ki temelji na sodelovanju ponudnikov storitev oblaka ter njihova usposobljenost in zanesljivost;
5. izdajanje sodnih pozivov brez poznavanja fizične lokacije podatkov[89]; in
6. izzivi, ki se nanašajo na zasebnost (neučinkovito upravljanje s ključi za šifriranje olajša izgubo sposobnosti za dešifriranje forenzičnih podatkov, shranjenih v oblaku).

[89] K. Šugman Stubbs, P. Gorkič, P., Dokazovanje v kazenskem postopku, (2011), str. 182.

4. VARSTVO ZASEBNOSTI PRI SHRANJEVANJU IN PRIDOBIVANJU PODATKOV V OBLAKU

»Eden ključnih konceptov, ki državi preprečujejo, da posega v posameznikove pravice, je zasebnost.«[90] Pridružujem se mnenju Kovačiča, ki meni, da »tehnološke spremembe prinašajo nove oblike in načine posegov v zasebnost, pravo pa je na te spremembe prisiljeno reagirati.«[91] Poseg v ustavno varovano človekovo pravico do zasebnosti predstavlja občuten poseg v človekove pravice in temeljne svoboščine, ki je dopusten samo ob izpolnjevanju strogih pogojev. Zato mora biti kazensko procesna zakonodaja (tako nacionalna kot mednarodna) urejena na način, da imajo organi pregona možnost učinkovitega preiskovanja kibernetskih kaznivih dejanj, hkrati pa se mora ohranjati načelo sorazmernosti in zagotavljati ustrezen standard varovanja pravice do zasebnosti. Ob iskanju pravega ravnotežja pravo trči ob tehtanje interesov, in sicer ob dolžnost in pravico države po preiskovanju kriminalitete ter varovanja posameznikove ustavne pravice do zasebnosti[92].

V prvem delu naloge sem opredelila pojem računalništva v oblaku, nadalje opredelila kibernetsko kriminaliteto, digitalno forenziko, načinom pridobivanja elektronskih nosilcev podatkov in elektronskih dokazov, in nenazadnje pomembnim elementom ter izzivom, ki otežujejo pregon in preiskovanje kibernetskih kaznivih dejanj. V nadaljevanju naloge bom obravnavala pravico do zasebnosti z različnih vidikov in skušala najti vzporednice z RO ter opravila pregled mehanizmov mednarodne pravne pomoči, ki so na voljo organom pregona pri preiskovanju in dokazovanju v kazenskem postopku kibernetskih kaznivih dejanj.

4.1. PRAVICA DO ZASEBNOSTI

Pravica do zasebnosti se je skozi čas in različne historične dogodke vseskozi oblikovala, njeno dojemanje je izrazito subjektivno, saj je pogojeno s posameznim okoljem in navadami posamezne družbe. Kot navajata B. in A. Lobnikar, se je »skozi zgodovino zasebna sfera premaknila iz življenjske nujnosti na področje svobode ter s tem postala vrednota.«[93]

Ob besedi zasebnost navadno pomislimo na nekaj kar je omejeno zgolj na sfero samega posameznika, kar je samo njegovo in nad čimer ima on oblast. Eden od možnih pristopov poudarja, da pomeni zasebnost pravico posameznika, da se ga pusti pri miru, t.i. *pravica biti sam*[94] (angl. *right to be let alone*). Pravica učinkuje *erga omnes*, kar pomeni, da deluje proti tretjim in tako varuje posameznika pred državno oblastjo, javnostjo ter drugimi posamezniki.

---

[90] K. Šugman Stubbs, Nove tehnologije in njihov vpliv na pojavnost in pregon kriminalitete, v: Zbornik znanstvenih razprav, 73, (2013), str 192.
[91] M. Kovačič, 2006, Nadzor in zasebnost v informacijski družbi, str. 46.
[92] K. Šugman Stubbs, Nove tehnologije in njihov vpliv na pojavnost in pregon kriminalitete, v: Zbornik znanstvenih razprav, 73, (2013), str 192.
[93] B. Lobnikar, A. Lobnika, Pravica do zasebnosti pri izvajanju policijskih pooblastil – analiza percepcije policijskih šefov, v:Revija za kriminalistiko in kriminologijo, 62 (2011), št. 4, str. 333-343.
[94] Leta 1980 sta odvetnika Warren in Brandies v reviji Harvard Law Review objavila članek Pravica do zasebnosti: pravica biti sam. Od tod izvira »moderna« definicija zasebnosti.

Po mnenju Ustavnega sodišča je človekovo zasebnost razumeti kot »... bolj ali manj sklenjeno celoto njegovih ravnanj in ukvarjanj, občutij in razmerij, za katere je značilno in konstitutivno, da so jo človek oblikuje in vzdržuje sam ali skupaj z najbližjimi, s katerimi je v intimni skupnosti, in da tako v njej biva z občutkom varnosti pred vdorom javnosti ali kogar koli drugega nezaželenega.«[95]

URS varuje tri vidike zasebnosti. Splošna definicija zasebnosti je varovana znotraj 35. člena, ki zagotavlja nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic. S tem členom pravo varuje ljudi oziroma odnose med njimi. Nadalje 36. člen varuje prostorski vidik zasebnosti, ki se nanaša na nedotakljivost stanovanja. Prvi odstavek 37. člena pa zagotavlja tajnost pisem in drugih občil v okviru komunikacijske zasebnosti, ki je v današnji dobi modernih tehnologij še najbolj deležna diskusij in pozornosti javnosti ter sodne prakse.

Pravno varstvo pravice do zasebnosti se konča, ko se mora varovati širši javni interes ali ko pravica trči ob izkazani močnejši interes drugega posameznika[96]. Omejitve pravice morajo biti določene v zakonodaji, ob upoštevanju, da omejitev sledi ustavno dopustnemu cilju[97] in če je ta omejitev skladna s splošnim načelom sorazmernosti.[98]

Šugman Stubbs navaja dva koncepta pri poseganju v zasebnost in sicer, da je potrebno ločevati posege, ki (1) jih izvaja država prek svojih organov pregona za potrebe kazenskega postopka in (2) vidik poseganja v zasebnost preko nadzora, ki ga izvajajo zasebniki.[99] Po mnenju Šugman Stubbs je v dobi sodobnih komunikacijskih omrežij še toliko bolj nujno potrebno pazljivo pretehtati, do katere meje je še dovoljena učinkovitost pregona državnih organov in kje se začne čezmerno poseganje v človekove pravice. Nujna je tudi skrbna presoja sodne veje oblasti v smislu uporabe tehnološko podprtih preventivnih metod nadzora in uporabnost dokazov, ki jih organi pridobivajo z uporabo novih tehnologij.[100]

4.2. PROSTORSKI VIDIK ZASEBNOSTI

4.2.1. Nedotakljivost stanovanja in drugih prostorov (36. člen URS)

Prostorsko zasebnost kot teritorialni koncept zasebnosti varuje 36. člen Ustave RS, ki določa, da je stanovanje nedotakljivo in izključuje pravico vseh tretjih oseb do vstopa in preiskovanja stanovanja, razen z odločbo sodišča ali s privolitvijo imetnika prostora. Določa, da ima pravico biti navzoč tisti, čigar stanovanje ali prostori se preiskujejo ali njegov zastopnik. V zadnjem odstavku pa opredeljuje izjemni primer vstopa v stanovanje brez

---

95 Up-32/94 z dne 13.4.1995.

96 U-I-25/95 z dne 27.11.1997.

97 Tretji odstavek 15. čl. Ustave RS.

98 2. čl. Ustave RS.

99 K. Šugman Stubbs: Nove tehnologije in njihov vpliv na pojavnost in pregon kriminalitete, v: Zbornik znanstvenih razprav, 73 (2013), str 192.

100 Prav tam.

sodne odredbe, če je to neizogibno potrebno, da lahko neposredno primejo storilca KD ali da se zavaruje ljudi in premoženje.

Pravica zagotavlja občutek varnosti pred vdorom javnosti ali kogarkoli nezaželenega.[101] Pravica do nedotakljivosti stanovanja dvojno varovana: kot posebna ustavna pravica do varstva nedotakljivosti stanovanja po 36. členu Ustave Republike Slovenije in v sklopu ustavnega varstva človekove zasebnosti po 35. členu Ustave.[102]

Pri preiskovanju (kibernetskih) kaznivih dejanj policija v postopku pridobitve dokazov uporablja preiskovalna dejanja, ki so navedena v XVIII. poglavju Zakona o kazenskem postopku.[103] Med preiskovalna dejanja zakon uvršča hišno in osebno preiskavo, zaseg predmetov, ravnanje s sumljivimi stvarmi, zaslišanje obdolženca, zaslišanje prič, ogled in izvedenstvo. V tem poglavju bo za nas relevantna hišna in osebna preiskava, zaseg predmetov ter preiskovanje elektronskih naprav, ki (lahko) vsebujejo elektronske dokaze.

S hišno preiskavo se posega v ustavno varovano človekovo pravico do nedotakljivosti stanovanja oziroma zasebnosti, zato mora biti mogoč preizkus zakonitosti tega posega[104]. Preiskava stanovanja in drugih prostorov obdolženca ali drugih oseb se tako sme opraviti, če so podani utemeljeni razlogi za sum, da je določena oseba storila kaznivo dejanje in je verjetno, da bo mogoče pri preiskavi obdolženca prijeti ali da se bodo odkrili sledovi kaznivega dejanja ali predmeti, ki so pomembni za kazenski postopek. Zadnja dva razloga verjetnosti sta nujen pogoj tudi pri osebni preiskavi[105].

V pisni odredbi za hišno preiskavo mora biti točno navedena lokacija, kjer se bo hišna preiskava izvajala (t.i. točka dostopa) in kateri predmeti se lahko zasežejo. Na tej točki pa trčimo ob nekatere elemente[106], ki otežujejo pregon in preiskovanje kibernetskih kaznivih dejanj. Prvi element, ki predstavlja tudi na splošno enega največjih problemov pregona kibernetskih KD, je problem identifikacije storilcev in določanja njihove lokacije, ko se storilci izdajajo pod lažnimi identitetami. Pri izvrševanju kibernetskih KD storilci uporabljajo mnoge lažne internetne povezave, ki so lahko povezami med številnimi svetovnimi strežniki. Zelo težko je odkriti storilca dejanja, ki uporablja lažno identiteto in hkrati prikriva ali potvarja IP naslov[107] naprave, ki jo uporablja. Lahko rečemo, da tu uporaba sodne odredbe za »klasično« hišno preiskavo na podlagi točne lokacije kaj dosti več ne koristi.

---

[101] I Ips 169/97.

[102] U-I-25/95.

[103] ZKP-N, Uradni list RS, št. 63/94, 25/96 - odl. US, 39/96 - odl. US, 5/98 - odl. US, 49/98 - ZPol, 72/98, 6/99, 66/00, 111/01, 32/02 - odl. US, 44/03 - odl. US, 56/03, 43/04, 68/04 - odl. US, 101/05, 14/07, 40/07 - odl. US, 102/07 - ZSKZDČEU, 21/08 - odl. US, 23/08 - ZBPP-B, 65/08 - odl. US, 68/08, 89/08 - odl. US, 77/09, 88/09 - odl. US, 29/10 - odl. US, 58/11 - ZDT-1, 91/11, 47/13, 87/14, 8/16 - odl. US, 64/16 - odl. US, 65/16 - odl. US, 16/17 - odl. US, 59/17 - odl. US, 66/17 - ORZKP153,154, 1/19 - odl. US, 22/19, 48/19 - odl. US.

[104] Vrhovno sodišče – Pravna mnenja 1/2012, str. 7, obr. Z dne 6.4.2012. URL: http://www.sodnapraksa.si/?q=id:41039&database[SOSC]=SOSC&database[SOPM]=SOPM&_submit=i%C5%A1%C4%8Di&page=0&id=41039 (19.9.2019).

[105] 214. čl. ZKP-N.

[106] Elementi, ki otežujejo pregon in preiskovanje kibernetskih KD so opisani v tretjem poglavju.

[107] IP-naslov določa lokacijo računalnika v omrežju, podobno kot naslovi ulice v mestu.

Drugi element, ki se lahko pojavi pri hišni preiskavi in zasegu pri preiskovanju kibernetskih KD, je identificiranje predmetov, ki so pomembni za kazenski postopek. Pri klasičnih kaznivih dejanjih je lahko predmet zasega storilčevo orožje, ki je v otipljivi obliki in velikosti, npr. pištola, ki je shranjena v sefu omare. Pri kibernetskih kaznivih dejanjih je fizični predmet zasega nosilec podatkov t.j. elektronska naprava, kot npr. računalnik, ki se vedno zaseže kot celota. Problem pa je, da je računalnik sestavljen iz veliko delov in vsebuje ogromno podatkov in ne samo tistih, za katere imamo sodno odredbo. Kot da bi pri klasičnem zasegu zasegli celotno omaro s sefom pištol, med katerimi bi bila tudi storilčeva. Šugman Stubbs opozarja, da sta zaseg in kopija vsega trdega diska računalnika po klasični doktrini preširoko pooblastilo ter da bi morali to povsem prilagoditi preiskavi elektronskih naprav, kjer bi bili kriteriji preiskave in zasega strožje določeni.[108]

S hišno preiskavo sta povezana tudi zaseg in preiskava elektronske naprave. V primeru zasega elektronske naprave se ravna po 223.a členu ZKP-N v povezavi s prvim odstavkom 219.a člena ZKP-N. Elektronske naprave, ki se nahajajo v prostoru, kjer se izvaja hišna preiskava lahko zasežemo bodisi na podlagi (1) soglasja uporabnika elektronske naprave ali na podlagi (2) sodne odredbe, če uporabnik odkloni zaseg[109]. V tem primeru soglasje uporabnika ni potrebno. Preiskavo elektronske naprave je mogoče zakonito odrediti že v sami odredbi za hišno preiskavo[110]. Kot že omenjeno, se pri zasegu računalnika kot nosilca podatkov vedno zaseže celega kot takega, kasneje pa se v okviru sodne odredbe za preiskovanje pri forenzičnem pregledu podatkov uporabi programe[111] in orodja, ki omogočajo selektivno izbiranje podatkov. V primeru hišne preiskave je potrebno zaseg elektronske naprave opraviti v najkrajšem možnem času, da se lahko najbolj efektivno zavaruje dokaze na elektronskem nosilcu podatkov.

Zaradi omenjenih nekaterih težav, s katerimi se soočamo pri hišni preiskavi, tj. identifikacija storilcev in predmetov, ki naj bodo predmet zasega, je takorekoč preiskovalna vrednost hišne preiskave pri praktično dokaj omejena. Kasneje se pri analiziranju zaseženih predmetov preiskovalci še dodatno srečajo s težavami, saj so ti nosilci podatkov lahko zelo dobro zaščiteni

Poleg tega, da imamo težave z identifikacijo storilcev in predmetov, pomembnih za kazenski postopek pa vidim še eno oviro pri preiskovanju KKD v oblaku s hišno preiskavo. Četudi odmislimo omenjeni težavi glede identifikacije in zasežemo pravilni elektronski nosilec, pa še ni rečeno, da bodo digitalni forenziki do podatkov na njem dostopali brez problema. Ti nosilci podatkov, ki vsebujejo sledi KD, so lahko zelo dobro zaščiteni z enkripcijskimi programi ali pa močnimi gesli, kar pomeni več dela za forenzike, predvsem pa to pomeni daljši odzivni čas na KD.

---

[108] K. Šugman Stubbs, Nove tehnologije in njihov vpliv na pojavnost in pregon kriminalitete, v: Zbornik znanstvenih razprav, 73 (2013), str 199.
[109] Drugi odstavek 219.a ZKP-N.
[110] VSL Sodba II Kp 50685/2012.
[111] Npr. Autospy, CAINE itd. M. Zbrog, A Guide to Digital Forensics and Cybersecurity tools, URL: https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools. (28.8.2019).

4.2.2. Četrti amandma - v koraku z modernimi tehnologijami?

Četrti amandma (angl. *The Fourth Amendment)* Ustave ZDA je del Listine temeljnih pravic[112] (angl. *Bill of Rights)*, ki ščiti ljudi pred nerazumnimi (neupravičenimi) preiskavami in zasegi. To pomeni, da policija ne more preiskati posameznika ali njegove hiše brez naloga, izdanega s strani sodnika, ali ob obstoju utemeljenega suma[113], da je obdolženec storil kaznivo dejanje, ki se mu očita. Dodatna zahteva se nanaša na podroben opis lokacije, ki bo predmet preiskave in oseb ter stvari, na katere se ta odredba nanaša.

Ameriško Vrhovno sodišče je v primeru *Silverman v. ZDA* razširilo dojemanje človekovega doma kot njegovega osebnega prostora na »pravico posameznika se umakniti v svoj dom in biti tam prost pred nerazumnim vdorom državnih organov«*[114]*. Primer je pomemben zato, ker je izoblikoval t.i. »ustavno zaščiteno področje« človekovega doma v primerih preiskave kaznivih dejanj. [115] Izmed najpomembnejših precedensov ameriškega Vrhovnega sodišča, ki je postavil nadaljnji pomemben mejnik v razvoju pravice do zasebnosti pa je primer *Katz vs. ZDA[116]* iz leta 1967. Ameriško Vrhovno sodišče je v sodbi postavilo pomemben standard ločevanja lastninske pravice od zasebnosti[117] in pojmovanje »pričakovane zasebnosti«. Sodišče je razsodilo, da pravo ščiti zasebnost posameznika v vseh prostorih, v katerih lahko posameznik pričakuje zasebnost[118], da je "tisto, kar [oseba] želi ohraniti kot zasebno, tudi na javno dostopnem območju, ustavno zaščiteno."[119] Sodišče je s tem sprejelo odločitev, da pomeni jedro varstva zasebnosti varstvo posameznika, in ne varstvo posesti oziroma lastnine stvari. V sodbi je tako navedeno, da četrti amandma ščiti *osebe* in ne prostore.

Pojem »razumnega« oziroma »upravičenega« pričakovanja zasebnosti je izoblikoval sodnik Harlan v svojem ločenem, a vplivnem mnenju k sodbi, v katerem je obrazložil kako naj se tolmači večinsko mnenje razsodbe in tako ustvaril test razumnega pričakovanja zasebnosti.[120] Po tolmačenju Harlana[121] je pri vprašanjih zasebnosti

---

[112] Listina zajema prvih deset amandmajev Ustave ZDA, je kot nek dodatek k Ustavi ZDA, specifično opredeljen glede osebnostnih pravic in svoboščin, s točno določenimi omejitvami glede moči oblasti v sodnih in drugih postopkih, z jasno deklaracijo, da vsa moč ni dodeljena ameriškemu Kongresu, ampak je preko Ustave vsa moč podeljena zveznim državam in ljudstvu.

[113] V ZDA je izraz *probable cause* še najbljižje slovenskemu dokaznemu standardu utemeljenega suma. "*Probable cause is a legal standard wherein the officer has in his or her possession facts and circumstances within the police officer's knowledge that provide a "reasonably trustworthy basis for a man of reasonable caution to believe that a criminal offense has been committed or is about to take place*." (*Carroll v. United States*, 267 U.S. 132) URL: https://www.legalmatch.com/law-library/article/search-warrants.html (18.4.2019).

[114] *Silverman v. United States, 365 U.S. 505 (1961).*

[115] R. Lampe, Mednarodnopravni vidiki pravice do zasebnosti – jurisprudenca 8. Člena Evropske konvencije o človekovih pravicah in temeljnih svoboščinah, v:Pravnik: revija za pravno teorijo in prakso, 59 (2004), št. 4/6, str. 225.

[116] *Katz v. United States, 389 U.S. 347, 361 (1967).* V primeru je šlo za prisluškovanje FBI Katzu, ki je v telefonski govorilnici na javno dostopnem mestu sporočal nedovoljene informacije glede stav. Prisluškovalna naprava je bila pri tem nameščena zunaj govorilnice. Sodišče je v razsodbi napisalo, da je bistveno za kršitev s strani FBI »sporno uho«, saj je Katz govoril po telefonu iz zaprte govorilnice, v kateri je imel pravico pričakovati, da bo njegova vsebina pogovora ostala zasebne narave. M. Kovačič, 2006, Nadzor in zasebnost v informacijski družbi, str. 53.

[117] Prav tam, str. 52.

[118] Prav tam, str. 53.

[119] *Katz. v. United States, 389 U.S. 347, 361 (1967).*

[120] URL: https://www.law.cornell.edu/wex/expectation_of_privacy (19.9.2019).

[121] URL: https://en.wikipedia.org/wiki/Katz_v._United_States (19.9.2019).

potrebno imeti ves čas v mislih dejstvo, da pravo varuje prav samega posameznika, in ne zgolj prostorov, lastnine ali lastnikov, ki v določenem prostoru ali določenem ravnanju upravičeno pričakuje zasebnost.[122] Pri testu imamo dva pogoja, ki morata biti izpolnjena in sicer (1) da posameznik v nekem prostoru razumno pričakuje zasebnost in (2) da je tako pričakovanje zasebnosti s strani družbe objektivno priznano.[123] Klemenčič k temu dodaja še, da mora biti tako pričakovanje utemeljeno in to ne zgolj samo subjektivno, kar pomeni da v poštev ne bo prišlo presojanje po subjektivnem testu, vendar po testu povprečnega uporabnika, ki uporablja komunikacijsko storitev.[124] Kot povzema Lampe, je bistvo primera *Katz* sprememba pojmovanja nerazumne (neupravičene) preiskave in zasegov iz četrtega amandmaja, da je za preiskavo potreben fizični vdor v »ustavno zaščiteno območje« (t.i. Silverman standard) s testom razumnega pričakovanja zasebnosti[125].

Leta 1997 je test prvič sprejela tudi sodna praksa ESČP v primeru *Halford vs. Združeno kraljestvo*, v katerem je šlo za vprašanje o razumno pričakovani zasebnosti«policistke, ki je telefonirala s službenega telefona. *Katz* je transformiral način razlage in uporabnost četrtega amandmaja v praksi, saj je sodišče pred tem gledalo ali je bil storjen dejansko fizični vdor (ang. *trespassing*). Pogled je bil deležen mnogo kritik, da je zastarel in neprimeren za uporabo sodobne tehnologije, kot je bilo tedaj telefonsko prisluškovanje, ki pa ni zahteval fizičnega vdora v dom.

Test »razumnega pričakovanja zasebnosti« je sodišče pri *Katzu* razširilo spekter uporabe amandmaja tudi na neoprijemljive (angl. *intangible*) komunikacije. Ne glede na to, da se test razumnega pričakovanja zasebnosti uporablja tako pri oprijemljivih, kot tudi neoprijemljivih predmetih, pa v primeru, da je ta prostovoljno izročen tretji osebi, oseba s tem izgubi razumno pričakovanje zasebnosti.[126]

V primeru *Riley v. California* je šlo za vprašanje apliciranja četrtega amandmaja na preiskavo oziroma zaseg prenosnega telefona ob aretaciji osumljenca. Ob aretaciji lahko navadno osumljenca organi pregona preiščejo in zasežejo relevantne predmete. Gre za prvo odločitev Vrhovnega sodišča ZDA o iskanju in zasegu elektronskega nosilca. Sodišče je razsodilo, da velja drugače za zaseg elektronskih nosilcev (kot sta računalnik in mobilni telefon) pri osebni preiskavi, kot pri zasegu drugih predmetov, saj lahko vsebuje toliko osebnih podatkov in informacij, da je za to potrebno pridobiti najprej preiskovalni nalog sodnika[127]. Tako lahko, upoštevajoč četrti amandma, policija zaseže in preišče nosilec podatkov, če imajo za-to ustrezen veljavni preiskovalni nalog[128].

---

[122] B. Lobnikar, A. Lobnika, Pravica do zasebnosti pri izvajanju policijskih pooblastil – analiza percepcije policijskih šefov, v:Revija za kriminalistiko in kriminologijo, 62 (2011), št. 4, str. 333-343.

[123] *Katz. V United States, 389 U.S. 347, 361 (1967)*

[124] G. Klemenčič, Ustavnosodni test utemeljenega pričakovanja zasebnosti, v:Komentar Ustave RS. URL: https://e-kurs.si/komentar/ustavnosodni-test-utemeljenega-pricakovanja-zasebnosti/ (10.9.2019)

[125] R. Lampe, Mednarodnopravni vidiki pravice do zasebnosti – jurisprudenca 8. Člena Evropske konvencije o človekovih pravicah in temeljnih svoboščinah, v:Pravnik: revija za pravno teorijo in prakso – Letnik 59, št.4/6 (2004), str. 225.

[126] Glej npr. *United States v Miller, 425 U.S. 435, 442-42 (1976).*

[127] *Riley v. California.* URL: https://en.wikipedia.org/wiki/Riley_v._California (15.9.2019).

[128] Preiskovalni nalog je pravni standard v obliki naročila sodnika, ki daje policiji pooblastilo oziroma pravico, da preiščejo specifičen prostor za iskanje specifičnih (torej točno določenih v nalogu) predmetov ali materialov. Da sodnik izda preiskovalni nalog je potrebno, da obstaja utemeljen sum. URL: https://dictionary.cambridge.org/dictionary/english/warrant (15.9.2019).

V primeru *US v. Crist* je zvezno sodišče Pennsilvanije določilo, da je razlika med preiskavo računalnika in ostalimi oprijemljivimi predmeti namreč pri tem, da so z odstranitvijo trdega diska iz računalnika in prepisom podatkov, ki so na njem izpolnjeni pogoji za preiskavo v skladu z četrtim amandmajem, pa čeprav je pomanjkljivo dejstvo glede fizičnega vdora (sodišče je bilo mnenja, da je računalnik sestavljen iz več ločenih delov, in vsak del je zase oprijemljiva stvar, ki je lahko predmet preiskave).

Sodna praksa se je od *Katza* z razvojem tehnologije nadgrajevala in dopolnjevala, vendar točnih pravil in smernic, ki bi se nanašale prav na sam oblak še vedno ni izoblikovala.

Primer *Carpenter v. Združene države Amerike*[129] iz leta 2018 je zelo pomemben, v katerem je Vrhovno sodišče ZDA razsodilo, da se brez veljavnega preiskovalnega naloga tudi ne more dostopati do zgodovinskih zapiskov od telekomunikacijskega ponudnika storilca, ki vsebujejo fizične lokacije mobilnih telefonov ter da gre v takšnem primeru za nasprotje s četrtim amandmajem. Pred tem so preiskovalni organi lahko pridobivali te podatke brez naloga.

Po mnenju Couillarda[130] si podatki, shranjeni v oblaku zaslužijo tudi določeno stopnjo varstva zasebnosti iz četrtega amandmaja, kjer se sam koncept oblaka uporablja in dojema drugače, sodišča pa morajo priznati razumno pričakovanje zasebnosti v oblaku, kar pod četrtim amandmajem zajema tudi subjektivno razumno pričakovanje zasebnosti. Couillard zagovarja stališče, da razumnega pričakovanja zasebnosti ni deležen tisti uporabnik spletnih storitev, ki daje informacije zasebne narave na splet brez kakršnih koli ukrepov za zaščito informacij.

Couillard predstavi test razumno pričakovane zasebnosti v zvezi z RO po zgledu ameriške sodne prakse kot nek »virtualni zabojnik«, na oziroma v katerem uporabniki pričakujemo zasebnost. Kot pri prostorskem vidiku zasebnosti pričakujemo zasebnost v zaprtem prostoru, pri oblaku pričakujemo apliciranje zasebnosti v virtualnem smislu. Seveda pa razumnega pričakovanja zasebnosti ni deležen tisti uporabnik spletnih storitev, ki daje informacije zasebne narave na medmrežje brez kakršnih koli varnosti ukrepov. S tem, ko bo posameznik poskrbel za zaščito svojih podatkov v oblaku z ustreznimi metodami (uporaba zaščitnih gesel, varnostnih kod, enkripcije[131]), bo v zadostni meri dal vedeti, da želi na zaščitenih podatkih imeti zasebnost in s tem bo izpolnjen bo pogoj iz testa o razumno pričakovani zasebnosti. Posameznik se mora potruditi in vpeljati zadostne varnostne ukrepe, v kolikor ne želi, da je vsebina njegovih podatkov izpostavljena širši javnosti.

---

129 S. McCubbin, Summary: The Supreme Court Rules in Carpenter v. United States, (2018). URL: https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states (16.9.2019).

130 D. A. Couillard, Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing (June 1, 2009). Minnesota Law Review, Vol. 93, p. 2205, 2009; URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1832982 (30.5.2019) in URL: http://www.minnesotalawreview.org/wp-content/uploads/2012/01/Couillard_MLR.pdf (15.6.2019).

131 Strokovnjaki za zaščito svetujejo, da je najboljša opcija za zaščito enkripcija ali uporaba močnega gesla (z uporabo številk, simbolov, velikih in malih začetnic).

4.2.3. Varstvo prostorskega vidika zasebnosti v 8. členu EKČP

Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin[132] (EKČP) združuje več vidikov zasebnosti in v prvem odstavku 8. člena določa med drugim tudi varstvo prostorskega vidika zasebnosti, saj določa, da ima »vsakdo pravico do spoštovanja zasebnega in družinskega življenja, doma in dopisovanja.«[133] Nadalje določa vrsto izjem oziroma primerov, v katerih lahko javna oblast poseže v izvrševanje te pravice.

Kot navaja Lampe, »se lahko javna oblast vmešava v izvrševanje pravice do zasebnosti posameznika (na podlagi zakona in kadar je to nujno v demokratični družbi) le v primeru dveh upravičenih javnih interesov: (1) javne in državne varnosti in (2) ekonomske blaginje, s tem da sledi trem legitimnim ciljem: preprečitev nereda ali zločina, varovanje zdravja ali morale in varovanje pravice in svoboščin drugih ljudi.«[134]
Ravno zaradi zaščite prostorske zasebnosti so prostori kot so dom, bivališče in stanovanje posebej varovani ne le v Ustavi RS in Kazenskemu zakoniku[135], temveč tudi v mednarodno pravnih aktih, kot je 8. člen EKČP. Konvencija je osnova, na podlagi katere odloča in deluje Evropsko sodišče za človekove pravice (ESČP). V precedenčnem primeru *Camenzind v. Švica*[136] je, kot navaja Lampe, je ESČP *inter alia in abstracto* postavilo kriterije, po katerih je mogoče presojati ustreznost in učinkovitost posamezne zakonodaje, ali ta nudi dovolj visoko zaščito pred zlorabami javne oblasti pri odreditvi in izvajanju preiskave in zasegov.[137] Sodni primeri ESČP, ki se nanašajo na ukrepe, preiskave in zasege[138]: ukrepi, ki vključujejo vstop v zasebne domove, morajo biti »v skladu z zakonom« (*L.M. v. Italy [139])*, morajo biti v skladu s kazenskim postopkom (*Panteleyenko v. Ukrajina[140])*, morajo zasledovati enega od legitimnih ciljev (*Smirnov v. Rusija[141])* in morajo biti »nujno potrebni v demokratični družbi« za dosego tega cilja (*Camenzind v. Švica[142])*. Čeprav judikatura ESČP v povezavi z RO in varstvom prostorskega vidika zasebnosti še ne more ponuditi nič konkretnega, bi prišla v poštev merila in pogoji za prostorsko zasebnost

---

[132] Evropska konvencija o človekovih pravicah in temeljnih svoboščinah, Uradni list RS – Mednarodne pogodbe, št. 7/94.
[133] 8.a člen Konvencije.
[134] R. Lampe, Pravo človekovih pravic: sistem človekovih pravic v mednarodnem, evropskem in ustavnem pravu. (2010), str. 308.
[135] 152. člen KZ-1.
[136] *Camenzind v. Švica* Odločba z dne 16. 12. 1997.
[137] R. Lampe, Mednarodnopravni vidiki pravice do zasebnosti – jurisprudenca 8. Člena Evropske konvencije o človekovih pravicah in temeljnih svoboščinah, v:Pravnik: revija za pravno teorijo in prakso – Letnik 59, št.4/6 (2004), str. 221.
[138] Povzeto po: Guide on Article 8 of the European Convention on Human Rights 290. točka. URL: https://www.refworld.org/pdfid/5a016ebe4.pdf (21.9.2019).
[139] *L.M. v. Italy* Odločba z dne 8.2.2005.
[140] *Panteleyenko v. Ukrajina* Odločba z dne 29.6.2006.
[141] *Smirnov v. Rusija* Odločba z dne 7.6.2007.
[142] *Camenzind v. Švica* Odločba z dne 16.12.1997.

4.3. KOMUNIKACIJSKA ZASEBNOST

4.3.1. Varstvo tajnosti pisem in drugih občil (37. člen URS)

Drugi vidik zasebnosti, v katerega posegamo pri pridobivanju dokazov iz oblaka opredeljuje 37. člen Ustave RS, ki določa, da je zagotovljena tajnost pisem in drugih občil. Nadalje v drugem odstavku člen vsebuje pogoje za omejitev pravice do tajnosti pisem in drugih občil. Poseg v svobodo komuniciranja je dopusten pod določenimi pogoji, in sicer: (1) da je poseg določen v zakonu, (2) da poseg v pravico pred tem odredi sodišče, (3) da je izvajanje takšnega posega časovno omejeno in (4) da je tak poseg nujen za uvedbo ali potek kazenskega postopka ali varnost države[143].

Klemenčič v komentarju tajnosti komunikacije in svobode komuniciranja komentira ustavno določbo glede »tajnost« komunikacije kot omejujočo, saj »večina mednarodnih in tujih ustavnih dokumentov na tej točki govori o spoštovanju dopisovanja, o svobodi in zasebnosti komuniciranja ipd.« [144] Ustavni člen na opisan način po mnenju Klemenčiča prepoveduje zgolj nadzorovane komunikacije, večji problem pa vidi v dejstvu, da člen ne omenja pozitivne pravice[145] do svobode komuniciranja.

Ustavni člen zagotavlja zasebnost vsebine komunikacije posameznika in prometnih podatkov, povezanih z njo, tako da se brez njegove privolitve nihče ne seznani z vsebino sporočila, ki ga posreduje prek sredstva, ki omogoča izmenjavo oziroma posredovanje informacij (preko spleta, na daljavo), pri tem pa se zasleduje interes posameznika, da se svobodno odloča o tem, komu, v kakšnem obsegu, na kakšen način in pod kakšnimi pogoji bo posredoval določeno sporočilo.[146]

Sodišče je pri presojanju področja varstva komunikacijske zasebnosti poudarilo, da komunikacijska zasebnost zajema vse podatke, ki se nanašajo na (1) vsebino komunikacije, kot tudi na (2) vse podatke, povezane s to komunikacijo (tj. prometnih podatkov[147]). Pridobitev teh podatkov pomeni vpogled v vsebino in okoliščine komunikacije ter s tem poseg v pravico posameznika iz prvega odstavka 37. člena Ustave.[148]

---

[143] Up-106/05.

[144] G. Klemenčič, Ustavnosodni test utemeljenega pričakovanja zasebnosti, v:Komentar Ustave RS. URL: https://e-kurs.si/komentar/ustavnosodni-test-utemeljenega-pricakovanja-zasebnosti/ (13.6.2019).

[145] T.i. pozitivna pravica do komunikacijske zasebnosti vsebuje tako pravico do varovanja zaupnosti komunikacije, kot tudi svobodo do komuniciranja. Ibidem.

[146] Gl. 20. Točko U-I-45/08.

[147] To so tisti podatki, ki nam povedo s kom je klic potekal, ali je sploh potekal, koliko časa je komunikacija potekala.

[148] L. Selinšek, Digitalni dokazi in računalniška forenzika, v:Kriminaliteta in tehnologija: kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon?, (2012), str. 105.

Za poseg v komunikacijsko zasebnost gre takrat, kadar dostopamo do podatkov, ki se že nahajajo na napravi, uporabljeni za komunikacijsko sredstvo, če gre za podatke, ki pomenijo tako vsebino komunikacije ali t.i. prometne podatke[149].

4.3.2. Posegi in varstvo komunikacijske zasebnosti v ZKP

S preiskovalnimi dejanji, ki so odgovor na že opisane[150] elemente in izzive kibernetskega sveta, za potrebe preiskovanja in dokazovanja kibernetskih kaznivih dejanj posegamo v posameznikovo komunikacijsko zasebnost in svobodo. Kot že omenjeno v poglavju[151] o pridobivanju elektronskih podatkov, jih lahko pridobivamo od samega osumljenca s prikritim kibernetskim nadzorom, od ponudnika storitev ali prisilno od osebe s preiskovanji in zasegi.

Preiskovalna dejanja, ki pridejo v poštev pri pridobivanju tranzitnih podatkov (kateri bodo kasneje v postopku lahko služili kot elektronski dokazi) so lahko[152]: (1) preiskovalna dejanja usmerjena na podatke s katerimi razpolaga ponudnik komunikacijskih storitev, ponudnik storitev oblaka ali so v posesti tretje osebe, lahko pa z njimi razpolaga domnevni storilec. V zadnjem primeru, ko se bodo ti podatki nahajali pri domnevnemu storilcu, bo to zahtevalo njegovo aktivno sodelovanje, tako da bo merila za dovoljenosti teh dokazov določal privilegij zoper samoobtožbo[153]. (2) Za razliko od ukrepov[154], ki so usmerjeni k pridobivanju shranjenih podatkov, pa gre pri komunikacijskem vidiku zasebnosti za tranzitne podatke[155], zato bodo prišli v poštev ukrepi, ki zahtevajo posebno obliko pridobivanja podatkov v realnem času, t.j. prestrezanje podatkov, kot tudi njihovo shranjevanje in zavarovanje. (3) Z uporabo preiskovalnih dejanj lahko pridobivamo podatke o prometu (ti vsebujejo tudi lokacijske podatke) ali o vsebini komunikacije[156].

Za potrebe preiskovanja in dokazovanja kibernetskih kaznivih dejanj (v oblaku) je potrebna hitra reakcija organov pregona, kot tudi prikritost njihovega delovanja. Drugače od klasičnih preiskovalnih dejanj, ki so namenjena zbiranju dokaznega gradiva kot odziv na že izvršeno KD, pa je uporaba prikritih preiskovalnih dejanj (PPU) pri kibernetskih kaznivih dejanjih veliko bolj primerna. PPU so namenjeni odzivanju na kriminaliteto že v najzgodnejših fazah izvršitve KD in so za preiskovano osebo prikriti, tako da ta ne ve, da je nadzorovana[157]. So procesna dejanja, s pomočjo katerih si zagotovimo dokazno gradivo. Izvajajo se izključno v predkazenskem postopku in pomenijo zelo invazivni poseg v pravico do zasebnosti.

---

[149] Odločba Ustavnega sodišča RS, št. Up-106/05 z dne 2.10.2008.
[150] Gl. točko 3.2.2.
[151] Gl. točko 3.2.1.
[152] K. Šugman Stubbs; P. Gorkič, Dokazovanje v kazenskem postopku, (2011), str. 184-185.
[153] Bistvo privilegija zoper samoobtožbo je, da ni dovoljeno nikogar siliti, da izpove, oziroma da osumljeni ne čuti nobenega pritiska, da se izpove. Privilegij izvira iz *common law* sistema, razteza se tudi na pesronalne dokaze širše narave (npr. dnevniki in dokumenti). K. Šugman Stubbs; P. Gorkič Šugman, Dokazovanje v kazenskem postopku, (2011), str. 249.
[154] Kot že opisano v poglavju o nedotakljivosti stanovanja gre za preiskovalna dejanja hišna preiskava, zasega predmetov ter preiskovanja elektronskih naprav, ki vsebujejo elektronske dokaze.
[155] Gre za vrsto podatkov, ki potujejo z enega elektronskega nosilca na drugega preko telekomunikacijskega ali spletnega omrežja.
[156] Kot že omenjeno v prejšnjem odstavku, sta obe kategoriji podatkov varovani v okviru 37. člena Ustave RS.
[157] K. Šugman Stubbs; P. Gorkič: Dokazovanje v kazenskem postopku, (2011), str. 144 – 146.

Glede na dobrino, v katero se s PPU-jem posega, lahko te razdelimo v naslednje skupine[158]:

- ukrepi, ki pomenijo predvsem posege v pravico do samostojnega odločanja v lastnih zadevah,
- ukrepi, ki pomenijo predvsem posege v svobodo komuniciranja (pomenijo poseg v pravico po 37. členu URS), in
- ukrepi, ki pomenijo predvsem prikrite posege v varstvo osebnih podatkov.

Na zakonodajnopravnem področju, ki ureja slovensko ureditev kazenskega postopka je prišlo v letošnjem letu do pomembnih sprememb z uvedbo ZKP-N[159]. Koncept novele je predvsem v tem, da morajo tudi organi pregona slediti tehnološkemu razvoju, ki ga spretno izkoriščajo storilci kibernetskega kriminala. Nekateri relevantni PPU, ki bi lahko prišli v poštev po noveli pri preiskovanju kibernetskih KD iz oblaka[160] so[161]:

1. PPU tajnega opazovanja po 149. a členu ZKP-N[162] v povezavi s četrtim odstavkom istega člena, kjer so taksativno našteti primeri za uvedbo tega ukrepa[163]. S tem posegom posamezniku prikrivamo dejstvo, da policija osredotočeno in dalj časa pridobiva podatke o njegovem gibanju in aktivnostih, kar vpliva na njeno odločitev kako ravnati v stiku z drugimi.[164] Gre za neprekinjeno ali ponavljajoče se opazovanje ali sledenje, osredotočeno na spreminjanje položaja, gibanja ali aktivnosti osebe. Tajno opazovanje se sme izvajati na zakonsko predpisanih prostorih – tam, kjer opazovana oseba zasebnosti ne pričakuje[165]. Za KKD, povezana z oblakom bi ta PPU lahko prišel v poštev npr. za KD napada na informacijski sistem po drugem, tretjem in četrtem odst. 221. člena KZ-1.
2. PPU pridobivanja prometnih podatkov[166] po ZKP-N[167] - je ukrep, ki preiskovalnemu sodniku omogoča pridobiti podatke od operaterjev oziroma ponudnikov storitev podatke, o okoliščinah komunikacije, ne pa o sami vsebini. Ukrep je poseben primer zahteve za posredovanje podatkov, govorimo o posebni vrsti edicijske dolžnosti[168]; in sicer:
   a. prenovljeni 149.b člen omogoča pridobivanje podatkov o prometu za nazaj (npr. pridobivanje shranjenih podatkov od ponudnikov storitev/operaterjev, ki jih že zakonito hranijo). Dosedanja ureditev je urejala le pridobivanje podatkov za nazaj, novela pa omogoča sprotno spremljanje prometa komunikacij, ob zvišanem dokaznem standardu (utemeljeni razlogi za sum) in le za omejena KD, ki so enaka kot pri ukrepu tajnega opazovanja. Novela tu dodaja še natančnejšo opredelitev komunikacijskega sredstva, za katero naj bi se pridobili prometni podatki[169]. V del določbe, ki se

[158] K. Šugman Stubbs; P. Gorkič: Dokazovanje v kazenskem postopku, (2011), str. 147.
[159] Novela je začela veljati 20. aprila letos, uporabljati pa se bo začela 20. oktobra. Določbe za prikrite preiskovalne ukrepe veljajo že od 20. julija.
[160] Pri tem se osredotočam na pridobivanje tranzitnih podatkov s PPU, ki pomenijo poseg v komunikacijsko zasebnost.
[161] Zgaga Markelj, Zakon o kazenskem postopku (ZKP): z novelo ZKP-N, Uvodna pojasnila, (2019), str. 43-63.
[162] Ukrep, ki pomeni predvsem poseg v pravico do samostojnega odločanja v lastnih zadevah (35. člen US RS).
[163] Zgaga Markelj, Zakon o kazenskem postopku (ZKP): z novelo ZKP-N, Uvodna pojasnila, (2019), str. 44.
[164] K. Šugman Stubbs; P. Gorkič: Dokazovanje v kazenskem postopku, (2011), str. 149.
[165] Prav tam, str. 150.
[166] Dosedaj je bil ta ukrep urejen le v 149.b čl., zdaj je nadomeščen v petih členih.
[167] Zgaga Markelj, Zakon o kazenskem postopku (ZKP): z novelo ZKP-N, Uvodna pojasnila, (2019), str. 44–51.
[168] K. Šugman Stubbs; P. Gorkič: Dokazovanje v kazenskem postopku, (2011), str. 165.
[169] Predlog zakona o spremembah in dopolnitvah zakona o kazenskem postopku (ZKP-N; EVA: 2016-2030-0033 Predlog ZKP-N. URL: https://euprava.gov.si/.download/edemokracija/datotekaVsebina/372912?disposition=inline (19.9.2019)

nanaša na izvajanje ukrepa sprotnega spremljanja prometa komunikacij bi lahko umestili nadzor vsebine podatkov, kot tudi prometnih podatkov, ki bi se prenašali v/iz oblaka.

b. Povsem nov 149. c člen se nanaša na »ukrep zamrznitve in posredovanja podatkov o prometu za naprej«, t.i. spremljanje podatkov v realnem času. Člen je pomemben, ker omogoča organom preiskovanja večjo osredotočenost ukrepa, ki se izvaja naprej, zato je tu večji nabor KD, za katere se lahko ukrep uporabi. Drugi odstavek pa vsebuje pomembno omejitev za sam postopek, saj je potrebno še vnaprej določiti omejen in določljiv seznam oseb, za katere se bo ukrep izvajal (zato se ne more ukrep izvajati zoper nedoločenega števila oseb). Če apliciramo določbo na preiskovanja KD iz oblaka, kjer storilci uporabljajo lažne identitete, nam ta ukrep ravne ne more kaj dosti pomagati.

c. Nadalje je v 149. č členu podrobneje urejen dostop do naročniških podatkov (brez sodne odredbe in brez privolitve posameznika, na katerega se ti podatki nanašajo) za policijo, državnega tožilca in sodišče. Glede oblaka bi lahko prišel v poštev, za lažje identificiranje IP naslova z morebitnim osumljencem.

d. In nenazadnje, novi 149. e člen pa določa začasno hrambo elektronskih dokazov. Gre pravzaprav za implementacijo 16. in 17. člena Konvencije o kibernetski kriminaliteti, ki se nanašata na institut takojšnjega zavarovanja shranjenih računalniških podatkov pri posamezni osebi, ki poseduje ali upravlja take podatke, oziroma takojšnje zavarovanje in delno razkritje podatkov o prometu. Ker se določba nanaša na ponudnike storitev informacijske družbe, se lahko ta določba nanaša na ponudnike oblačnih storitev in bi prišla prav v primeru preiskovanja kibernetskih KD iz oblaka.

3. Člena, ki urejata pravno podlago za uporabo v javnosti kar spornega IMSI-lovilca sta 150.a in 150.b člen. IMSI-lovilec ali tudi »lažna postaja« je posebno tehnično sredstvo, ki zna simulirati nekatere funkcije bazne postaje mobilne telefonije ter na ta način opraviti določena preiskovalna dejanja na bližnjih mobilnih telefonih[170]. Novela omejuje namene uporabe lovilca omejuje zgolj na identifikacijo telefonskega priključka oziroma lokacijo le-tega.[171] Z IMSI-lovilcem je mogoče pridobivati podatke, katere potrebujemo, da bomo lahko nadalje identificirali številke komunikacijskega sredstva (mobilnega telefona) in samih številk. Policija pa lovilca ne sme uporabljati za dešifriranje tekočega prometa, niti že obstoječega, prav tako pa ne sme uporabljati naprednih preiskovalnih dejanj[172]. Ukrep nam lahko pomaga kot priprava za nadaljnje ukrepe iz točke 2 zgoraj[173], v tem primeru je potrebno izpolnjevati še toliko višje pogoje za odreditev.[174] Ker se določbe nanašajo v pretežni meri na komunikacijskega sredstvo mobilnega telefona, povezave z oblakom tukaj ne moremo ravno izpostaviti. Morda bi prišla določba lahko prav v tistih primerih, ko bi že identificirali imetnika oblaka kot tudi njegovo številko mobilnega telefona, a ne bi poznali njegove lokacije, tako da bi nam IMSI-lovilec pri tem prišel v pomoč.

---

[170] Predlog zakona o spremembah in dopolnitvah zakona o kazenskem postopku (ZKP-N; EVA: 2016-2030-0033 Predlog ZKP-N, str. 33. URL: https://euprava.gov.si/.download/edemokracija/datotekaVsebina/372912?disposition=inline (21.9.2019)

[171] Prav tam.

[172] Prav tam.

[173] Za 149.b člen, prvi ostavek 149.c člena ali ukrepa iz 1.točke prvega odstavka 150.člena ZKP-N.

[174] Zgaga Markelj, Zakon o kazenskem postopku (ZKP): z novelo ZKP-N, Uvodna pojasnila, (2019), str. 54.

Do možnih rešitev pri preiskovanju KD v oblaku bi prišli lahko s pomočjo prekritih preiskovalnih ukrepov z uporabo forenzičnih računalniških programov (FRP), ki vsebujejo kodo, namenjeno oddaljeni in prikriti uporabi tuje elektronske naprave[175]. Ena od možnih rešitev glede RO ponuja »*zajem pri samem viru komunikacije*[176]« in ne več preko operaterja telekomunikacijskih storitev. Šlo bi za nadzorovanje komunikacije, še preden bi se lahko ta zašifrirala. Z odsotnostjo zahteve po prisotnosti samega operaterja, bi policija prihranila veliko dragocenega časa. Vendar, prvič, izvrševanje tega ukrepa ne bi prišlo v poštev v primeru že šifriranih komunikacij, ko bi le-te bile zaščitene z močnimi šifrirnimi gesli, saj nimamo ustrezne zakonske podlage za izvajanje uporabe tujih tehničnih sredstev za nadziranje elektronskih komunikacij, tako da policiji ni omogočeno izvajanje tega ukrepa. Drugič, prikriti preiskovalni ukrepi rešujejo le del problematike, saj delujejo le pri t.i. *tekočih* podatkih, ne pa tudi pri shranjenih podatkih. Problem je v šifriranju podatkov in odsotnosti pravne podlage, ki je nujno potrebna, da bi zadovoljili zakonske določbe glede načela zakonitosti in zakonski podlagi za ukrepe, ki posegajo v zakonitost.

Za potrebe preiskovanja kibernetskih kaznivih dejanj iz oblaka sem se v tem delu naloge omejila zgolj na prikrita preiskovalna dejanja, s katerimi se lahko rešujejo nekateri pravni izzivi, ki spremljajo preiskovalce pri pregonu takih kaznivih dejanj. Glede na zapisano lahko povzamem, da bi za preiskovanje kaznivih dejanj iz oblaka lahko prišlo v poštev večina PPU, se boljša rešitev pa bi bila uvedba forenzičnih računalniških programov.

Potrebno je še omeniti preiskave elektronske naprave, ki bo po novem vključevala tudi preiskavo s prek omrežja povezanimi in dosegljivimi informacijskimi sistemi, kjer so shranjeni podatki (t. i. podatki v oblakih). S primerjavo od prej, kjer je bilo bolj precizirano, na katere naprave se nanašajo zakonske določbe, je to zdaj malo manj jasno, tako da bo policija lahko nadzorovala tudi druge informacijske poti. Zato se mnogi sprašujemo, ali ne gre morda tukaj za uvajanje novih prikritih preiskovalnih ukrepov? Saj pri uvedbi tega mehanizma, fizična navzočnost imetnika elektronskega nosilca ne bo potrebna (kot je to npr. pri hišni preiskavi, pri prostorskem vidiku zasebnosti). Zakonodajalec se vidno zaveda, da tehnologija napreduje in da se več in več podatkov hrani v oblakih – kot pravi zakonodajalec ne gre za uvedbo prikritega preiskovalnega ukrepa, ampak za pridobivanje dokazov.

4.3.3. Varstvo komunikacijske zasebnosti in 8. člen EKČP

Vsebina 8. člena EKČP je opisana že v poglavju prostorskega vidika, na varstvo komunikacijske zasebnosti se le-ta nanaša v delu, da vsakomur priznava tajnost pisem in drugih občil. Ti se razlagajo zelo široko in zajemajo telefonske komunikacije, elektronsko pošto, SMS sporočila itd.[177] Pogoji za omejevanje pravice do komunikacijske zasebnosti so isti kot za varstvo prostorskega vidika zasebnosti. Da pravica do komunikacijske zasebnosti ni absolutna je razsodilo ESČP v zadevi *Klass in drugi proti Nemčiji*[178] (1978). V tem primeru se je pet nemških odvetnikov pritožilo na ESČP zaradi takratne pravne ureditve, ki je pooblaščala organe, da so lahko spremljali njihove telefonske komunikacije in medsebojne komunikacije, brez vnaprejšnjega opozorila s strani

---

175 P. Gorkič, Sodobni prikriti preiskovalni ukrepi, drugič: forenzični računalniški programi, 2014, str. 2.

176 Prav tam.

177 M. Kovačič, 2006, Nadzor in zasebnost v informacijski družbi, str. 81.

178 Klaas et. Al. V. ZR Nemčija, odločba z dne 6.9.1978.

organov, da so pod njihovim nadzorom. ESČP je presodilo, da pri tem ni šlo za nobeno kršitev glede 8. člena EKČP, saj so bili organi po takratni zakonodaji upravičeni se vmešati in upravljati s tem pooblastilom, kot je tajni nadzor nujno potreben za »nujno v demokratični družbi v interesu javne in državne varnosti in za preprečevanje neredov in zločinov«.[179] V tem primeru je šlo za prisluškovanje za posameznih linijah, saj tehnologije za masovno prisluškovanje takrat še niso uporabljali. V primeru *Zakharov proti Rusiji*[180] pa je šlo za masovno prisluškovanje, saj je varnostno-obveščevalna služba Zvezna varnostna služba (angl. FSB - *federal security service*) namestila svojo prisluškovalno opremo v prostore vseh ruskih mobilnih operaterjev in tako prisluškovala kateremu koli telefonskemu pogovoru v državi, brez vedenja ali pomoči mobilnega operaterja. Ruski novinar Zahkarov se je pritožil na ESČP, saj je menil, da je FSB s tem nedopustno posegla v pravico do zasebnosti državljanov. Sodišče je s svojo razsodbo postavilo t.i. »evropski standard za masovni nadzor telekomunikacij za obveščanje in državnovarstvene namene«, ki zdaj zahteva, da države oblikujejo svojo zakonodajo tako, da bodo njihove varnostno obveščevalne službe morale izrecno navesti na katere osebe, prostore oziroma priključke naj se prisluhi nanašajo. Potrebna bo tudi vsebinska kot dejanska presoja zaprosila[181]. Za podobno situacijo je šlo v primeru *Big Brother Watch in drugi proti Združenemu kraljestvu*[182], kjer se je skupina pritožnikov pritožila na ESČP zaradi obsega in razsežnosti programa za elektronski nadzor, s katerim je upravljala vlada ZK. Z njihovim mnenjem, da je bilo njihovo nadzorstvo usmerjeno v prestrezanje in pridobivanje komunikacij njihovih in tujih obveščevalnih služb ter posredovanje komunikacij od ponudnikov komunikacijskih storitev, se je strinjalo tudi ESČP. Razsodilo je, da so britanske oblasti, s tem, ko niso omogočile in integrirale ustreznih zaščitnih ukrepov za izbiro, zajemanje in filtriranja informacij, kršile 8. člen ESČP[183].

Omeniti je potrebno še primer *Benedik proti Sloveniji*[184], ki je zahteval med drugim tudi mednarodno sodelovanje v kazenskih zadevah držav članic. Nanaša se na potrebo po sodnem nalogu za pridobitev informacij o naročnikih, povezanih z dinamičnim IP naslovom. Več uporabnikov si je v različnih državah izmenjevalo in posedovalo slikovno in video gradivo s podobami spolnih zlorab otrok, med njimi tudi slovenski IP naslov, kar je odkrila švicarska policija leta 2006 in to tudi sporočila slovenskim organom. Slovenska policija je na podlagi takratnega 149b(3) člena ZKP zahtevala od ponudnika storitev, da ji ta razkrije na podlagi pisne zahteve podatke o uporabniku, ki ima ta IP naslov. Ponudnik je policiji ugodil, kasneje pa so pridobili še osebne in prometne podatke na podlagi 149b(1).člena ZKP. Gospod Benedik se je pritožil na ESČP in zatrjeval poseg v zasebno življenje in komunikacijo. ESČP je razsodilo, da se uporabnik z uporabo omrežja, ki ni omejil vidnosti in dosegljivosti IP drugim udeležencem v omrežju, ni prostovoljno odrekel legitimnemu pričakovanju zasebnosti in da mu je bila res kršena pravica do komunikacijske zasebnosti in zasebnega življenja. Pravici sta ustavni pravici,

---

[179] URL: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf (21.9.2019).
[180] Zakharov proti Rusiji, št. 47143/06 z dne 4.12.2015.
[181] Informacijski pooblaščenec, povzetki sodb Evropskega sodišča za človekove pravice. URL: https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/sodbe-mednarodnih-sodisc/povzetki-sodb/ (21.9.2019).
[182] BIG BROTHER WATCH in drugi proti ZDRUŽENEMU KRALJESTVU, št. 58170/13, 62322/14 in 24960/15 z dne 13. 9. 2018.
[183] Prav tam.
[184] Benedik proti Sloveniji, št. 62357/14 z dne 24. 4. 2018.

zato je podatek o identiteti posameznika v komunikacijskem prostoru mogoče pridobiti le na podlagi sodne odločbe[185].

Na podlagi opisanega lahko apliciram ugotovitve tudi na računalništvo v oblaku. Kljub odsotnosti posebne obravnave oblaka med »drugimi občili« menim, da bi prišla v poštev merila in pogoji poseganja v komunikacijsko zasebnost po 8. členu EKČP.

[185] Informacijski pooblaščenec, povzetki sodb Evropskega sodišča za človekove pravice. URL: https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/sodbe-mednarodnih-sodisc/povzetki-sodb/ (21.9.2019).

5. KAKO SE ODZIVAJO MEDNARODNI IN PRAVNI MEHANIZMI NA POSEGE V ZASEBNOST?

Razpršenost interneta je eden tistih ključnih elementov, ki spremljajo kibernetski kriminal in predstavlja velik izziv, s katerim se soočamo pri preiskovanju kibernetskih KD. Ta postane še toliko bolj kompleksen, v kolikor niso vpeljani pravi mehanizmi, ki bi olajšali delo pri pridobivanju digitalnih dokazov in preiskovalnih kibernetskih kaznivih dejanj. Brezmejnost medmrežja in s podatki v oblaku, predvsem pomeni nujno potrebno sodelovanje med državami, ki se odraža v medsebojni mednarodni pravni pomoči (MPP) in uporabi učinkovitih mehanizmov, ki olajšuje preiskovanje brezmejnih kibernetskih KD.

5.1. MEDNARODNA PRAVNA POMOČ

Oblak v prostoru interneta ne pozna nacionalnih meja[186]. Kazniva kibernetska dejanja, kot so hekanje v računalnike ali v oblak in tatvine osebnih podatkov iz oblaka, niso več geografsko omejena dejanja, medtem ko je klasično kazensko pravo omejeno na fizično območje države, zato je izjemnega pomena mednarodna pravna pomoč držav v procesu kazenskega postopka in uskladitev nacionalnih jurisdikcij, ustrezna komunikacija in sodelovanje.

Državna suverenost se navzven kaže prav v izvajanju kazenskega pravosodja. Če ni prisotnega elementa čezmejnosti, potem lahko država to stori popolnoma sama. V kolikor pa je prisoten mednarodni element, pa je potrebno sodelovanje tudi druge države in tedaj govorimo o mednarodni pravni pomoči, v našem primeru v kazenskih zadevah[187].

MPP je eden izmed mehanizmov, ki olajšujejo pregon kibernetskih KD in pomeni izvedbo procesnih dejanj, ki ga pristojni organi ene države (tj. zaprošena država) opravi na zaprosilo pristojnega organa druge države (tj. država prosilka) na podlagi in v skladu z veljavnimi mednarodnimi pogodbami, ki zavezujejo obe državi, ali evropskega pravnega reda ter notranjega reda zaprošene države.[188]

Z uporabo oblaka in novih tehnologij je učinkovita MPP še toliko bolj pomembna, saj je potreben hiter in učinkovit pregon storilcev. Razpršenost interneta je eden tistih ključnih elementov, ki spremljajo kibernetski kriminal, to je dejstvo. Mednarodni element se lahko pokaže v primeru, da je storilec v tujini ali izven območja suverenosti države, katera bi želela uresničiti pravico po kaznovanju[189]. Drugič, lahko gre za (elektronske) dokaze, ki se nahajajo v tujini in so potrebni za potrebe dokončanja kazenskega postopka v državi postopka[190].

---

[186] M. Ambrož, L. Bavcon, Z. Fišer, D. Korošec, V. Sancin, L. Selinšek, M. Škrk, Mednarodno kazensko pravo, (2012) str. 393.
[187] Prav tam.
[188] RS, Ministrstvo za pravosodje; spletni vir: http://www.mp.gov.si/si/delovna_podrocja/urad_za_mednarodno_sodelovanje_in_mednarodno_pravno_pomoc/mednarodna_pravna_pomoc/ (13.5.2019).
[189] M. Ambrož, L. Bavcon, Z. Fišer, D. Korošec, V. Sancin, L. Selinšek, M. Škrk, Mednarodno kazensko pravo, (2012) str. 393
[190] Prav tam.

Prav gotovo je, da je uvedba učinkovitih pravnih mednarodnih mehanizmov, ki se nanašajo na pridobivanje čezmejnih (elektronskih) dokazov ključnega pomena.

Države članice sodelovale sprva v obliki mednarodno pravne pomoči prav na dokaznopravnem področju, in tako sta bili sklenjeni dve konvenciji. Prva leta 1959, o medsebojni pravni pomoči v kazenskih zadevah z dvema dodatnima protokoloma in kasneje Konvencija iz leta 2000. Obe konvenciji temeljita na načelu reciprocitete[191].

Podlaga za izvajanje MPP so številne mednarodne pogodbe (bilateralne in multilateralne), pravni red EU in domača zakonodaja. Države EU so sprejele številne pravne akte s tega področja, ki se bodisi uporabljajo neposredno bodisi jih morajo DČ prenesti v notranjo zakonodajo.Zakonodaja na področju izročitve s strani podatkov ponudnikov storitev pristojnim organom v DČ EU se je v zadnjih letih tudi spremenila, predvsem v zvezi s ponudniki storitev iz ZDA.

Nadvse pomembno je, da v tehnološko napredni dobi zakonodajalci vpeljejo učinkovite pravne in mednarodna mehanizme, s katerimi bodo uspešno sodelovali v primeru preiskovanja mednarodnih kaznivih dejanj.

5.1.1. MPP in prostorski vidik zasebnosti

Prostorski vidik zasebnosti je pomemben takrat, kadar želimo zaseči nosilce, na katerih so shranjeni relevantni elektronski dokaz, in jih želimo zaseči, tipično ob hišni preiskavi. Pri tem gre za *shranjene podatke*, ki se nahajajo na elektronskem nosilcu, katerega organi pregona zasežejo pri hišni preiskavi. Ko je za potrebe kazenskega postopka potrebno pridobiti dokaze oziroma relevantna, obremenilna dejstva iz države, v kateri ne poteka kazenski postopek, »država prosilka« na podlagi svojega prava zaprosi drugi državo, tj. »zaprošeno državo« za pridobitev, izročitev dokazov ali opravo preiskovalnega dejanja za potrebe preiskovanega kazenskega postopka.

Pri tem imamo dva »varnostna filtra«, saj mora zaprosilo oziroma zahtevek najprej odobriti sodnik države prosilke, potem pa še sodnik zaprošene države, tako da gre ta zahteva čez dve različni jurisdikciji – torej na podlagi svojega prava država prosilka izda zahtevek, na drugi strani pa organi zaprošene države na podlagi svojega nacionalnega prava zahtevek preučijo ter ga spremenijo v nalog za pridobitev dokazov.

Z dvofaznim postopkom odobritve naloga oz. zahtevka ni problema glede jurisdikcije, varstvo glede postopka in temeljnih pravic je v zadostni meri zavarovano, vendar je postopek nadvse dolgotrajen in težaven, predvsem zaradi uporabe tujega jezika ter različnih pravnih sistemov držav.

5.1.2. MPP in komunikacijska zasebnost

Pri komunikacijski zasebnosti pa imamo *tranzitne podatke*, ki jih lahko prestrezamo, nadzorujemo strežnike in

---

[191] Recipročno načelo je načelo, po katerem priznava država drugi državi ali njenim državljanom določene pravice, ugodnosti s pogojem, da jih tudi druga država priznava njej oziroma njenim državljanom.

promet komunikacij. Pri pridobivanju elektronskih dokazov komunikacij ni potrebnega dvojnega pravnega filtra za potrebe mednarodne pravne pomoči, saj gre za neposredno pridobivanje podatkov od ponudnika storitev. Na podlagi zahteve policije države A ponudniku spletnih storitev v državi B, ta ponudnik izroči zahtevane podatke policiji iz države A. Odsotnost dvojnega filtra pomeni hitrejše odzivanje na kriminaliteto, vendar moramo biti pri tem veliko bolj pozorni glede prikritosti izvajanja ukrepov.

5.2. ODZIVANJE V OKVIRU KONVENCIJE O KIBERNETSKI KRIMINALITETI

Po "enajstem septembru" v ZDA se je nekako dejansko okrepil in povečal občutek za boj proti terorizmu, tudi na področju kibernetskega prostora. Konvencija o kibernetski kriminaliteti[192] je bila oblikovana in sprejeta z zavedanjem po oblikovanju skupne kriminalitetne politike, katere cilj je varovanje družbe pred kibernetskimi kaznivimi dejanji.

Kot navaja Rupnik[193] v svojem povzetku o Konvenciji, so »redke konvencije doživele tako široko podporo kot jo je Konvencija o kibernetski kriminaliteti« ali tudi »Budimpeštanska konvencija«. Konvencija Sveta Evrope, sprejeta leta 2002[194] je bila podpisana v zelo kratkem času po zaključku strokovno opravljenega dela, dve leti kasneje pa so države članice podpisale še Dodaten protokol h Konvenciji, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v računalniških sistemih[195]. Konvencija je pomembna tudi zato, ker določa[196] splošen okvir mednarodnega sodelovanja preiskovalcev, saj vemo, da kibernetski kriminal večinoma ne pozna nacionalnih meja.

Kot prvi mednarodni dokument obravnava sodobno kibernetsko kriminaliteto z vidika *priporočil*, katere podpisnice upoštevalo pri implementaciji in preoblikovanju[197] notranjih pravil kazenskega in procesnega prava ter jurisdikcije na področju kibernetske kriminalitete.

Za nas pomemben del, ki se nanaša na kazensko procesni del, je opisan v II. poglavju Konvencije skupaj s kazensko materialnim delom. Seveda Konvencija ne omenja specifično definicije oblaka in njegovih storitev, vendar si lahko kljub temu posredno predstavljamo apliciranje definicij oziroma ukrepov iz Konvencije na preiskovanje KD iz oblaka. Konvencija je tedaj uvedla institut »takojšnjega zavarovanja in shranitve računalniških podatkov in delno razkritje podatkov o prometu«. Že tedaj so se zavedali kakšnega velikega pomena je ukrep zavarovanja podatkov, da je nujen in racionalen. Uvede se institut odredbe za pripravo ter

---

192 Ur. l. RS št. 62/2004 z dne 7.6.2004.

193 A. Rupnik, Konvencija o kibernetski kriminaliteti »Budimpeštanska konvencija«, URL: http://uploadi.www.ris.org/editor/1132054990Kiber_kriminaliteta.pdf (12.5.2019).

194 V veljavo je stopila 1. julija 2004.

195 V veljavo stopil 1. marca 2006. Sama Konvencija ne vsebuje določb o rasizmu in ksenofobiji v kibernetskem prostoru, saj je bila glavna nasprotnica sprejema teh določb prav ZDA zaradi svoje tradicionalne ureditve svobode govora in izražanja. Da so pridobili ZDA kot podpisnico Konvencije, je zato Svet Evrope leta 2001 formiral novo skupino, ki je pripravila ta dodaten protokol h Konvenciji, ki jo smiselno dopolnjuje.

196 V tretjem poglavju o mednarodnem sodelovanju.

197 V drugem poglavju definira ukrepe, ki jih je potrebno sprejeti na državni ravni.

zbiranje računalniških zavarovanih podatkov (18. člen), katerega uporabijo organi pregona, ponudniki omrežnih storitev ali skrbniki sistemov izvršiti odredbo ter organom tako izročiti zahtevane podatke.

III. del se nanaša na mednarodno sodelovanje, kjer opredeljuje splošna načela, načela za izročitev ter posebne določbe, kamor spada mednarodno sodelovanje pri preiskovanju ali izvedbi postopkov v zvezi s kaznivimi dejanji, poveznimi z računalniškimi sistemi in podatki, ter o zbiranju elektronskih dokazov o KD. Posebne določbe se nanašajo med drugim tudi na začasne ukrepe, medsebojno pomoč pri preiskovalnih pooblastilih ter na omrežje 24/7[198]. Že 5. odstavek 22. člena Konvencije o kibernetski kriminaliteti opredeljuje medsebojno posvetovanje, v primeru da več držav uveljavlja sodno pristojnost glede domnevnega KD.

Konvencija temelji na ustaljenem »dvofaznem« postopku MPP, razen v primeru 32. člena, kjer določa čezmejni dostop do shranjenih računalniških podatkov s soglasjem pooblaščene osebe ali kadar so podatki javno dostopni.

5.3. EU KONVENCIJA O MEDSEBOJNI PRAVNI POMOČI V KAZENSKIH ZADEVAH MED DRŽAVAMI ČLANICAMI EVROPSKE UNIJE (2000)

Ena izmed pomembnejših Konvencij, ki se nanaša na medsebojno pravno pomoč v kazenskih zadevah je bila sprejeta leta 2000, v Sloveniji je začela veljati leta 2005 z Zakonom o ratifikaciji Konvencije o mednarodni pravni pomoči v kazenskih zadevah med državami članicami Evropske unije, ki jo je Svet pripravil na podlagi 34. člena Pogodbe o Evropski uniji (MKPPKZ).[199]

Države članice so podpisale Konvencijo v želji po izboljšanju pravosodnega sodelovanja v kazenskih zadevah med državami članicami in upoštevanju, da se zavedajo pomembnosti krepitve pravosodnega sodelovanja ob upoštevanju načela sorazmernosti.

Ureja medsebojno pravno pomoč v postopkih »v zvezi s kaznivimi dejanji, za katera je kaznovanje v trenutku zaprosila za pravno pomoč v pristojnosti pravosodnih organov pogodbenice prosilke.«[200] Uporablja se na področjih pridobivanja dokazov s preiskavo in zasegom, telekomunikacij, sprejemanja izjav osumljencev in prič in uporabo videokonferenc.

V postopku organ prosilec lahko zaprosilo za mednarodno pomoč direktno naslovi na organa izdajatelja. V koliko izvršitveni organ nima nobenih zadržkov za zavrnitev zaprosila, mora zaprosilo izvršiti čim prej in v roku,

---

[198] Omrežje 24/7 je točka za stike, dosegljiva štiriindvajset ur na dan in sedem dni na teden, za zagotavljanje takojšnje pomoči za preiskave ali postopke v zvezi s kaznivimi dejanji, povezanimi z računalniškimi sistemi in podatki, ali za zbiranje dokazov o kaznivem dejanju v elektronski obliki.

[199] Zakon o ratifikaciji Konvencije o medsebojni pravni pomoči v kazenskih zadevah med državami članicami Evropske unije, ki jo je Svet pripravil na podlagi 34. člena Pogodbe o Evropski uniji (MKPPKZ), (Uradni list RS – Mednarodne pogodbe, št. 7/05).

[200] 1. člen Konvencije o medsebojni pravni pomoči v kazenskih zadevah med državami članicami Evropske unije, C 197/3.

ki ga določi zaprosilec. Poseben poudarek iz preambule opozarja na 20. člen Konvencije, ki se nanaša na prestrezanje telekomunikacij *brez* tehnične pomoči druge države članice. Obveznosti po tem členu se nanašajo na »odredbe za prestrezanje, ki jih izda ali odobri pristojni organ *ene* države članice med preiskavami kaznivih dejanj, … , da bi bila ugotovljena istovetnost storilcev, …«[201] Dejstvo, da odredbo izda ali jo odobri organ zgolj *ene* države (»država, ki prestreza«) nam ilustrira zgolj en filter skozi katerega gre preverjanje pogojev in utemeljenost zahteve po odredbi, to pa odpira vprašanje jurisdikcije ter prikritosti oz. nadzora nad izvršitvijo. V kolikor ta država ne potrebuje dodatne tehnične pomoči države, v kateri nadzoruje naslov komunikacijskega priključka osebe, jo zgolj seznani s prestrezanjem. V četrti točki člena je naveden kar precej hiter reakcijski čas obveščene države, t.j. da v najkasneje 96 urah pristojni organ obveščene države odgovori na informacije, ki jih je prejel.

Konvencija uveljavlja pravilo lat. *Forum regit actum*, ki narekuje organom zaprošene države, da morajo postopati v skladu z navodili države prosilke, kar je še toliko bolj pomembno pri pridobivanju in zavarovanju dokazov. Seveda ti postopki ne smejo biti v nasprotju s temeljnimi načeli in pravili države izvršiteljice.

5.4. EVROPSKI PREISKOVALNI NALOG V KAZENSKIH ZADEVAH

Leta 2008 je bil v želji po uvedbi uniformiranega mehanizma, s katerim bi organi pridobivali dokaze, sprejet Okvirni sklep Sveta 2008/978/PNZ o evropskem dokaznem nalogu (v nad. EDN) za namene pridobitve predmetov, dokumentov in podatkov za uporabo v kazenskih postopkih[202], ki pa nikoli ni prav zaživel, saj je imel veliko pomanjkljivosti. Zato so organi še naprej iskali način, kako bi odpravili slabosti EDN in tako so predlagali idejo o evropskem preiskovalnem nalogu (v nadaljevanju EPN), ki nadomešča vse do tedaj veljavne mehanizme na dokaznopravnem področju.

EPN je sodna odločba, ki pravosodnim organom (vključno s sodišči, preiskovanimi sodniki in javnimi tožilci) poenostavlja delo pri pridobivanju dokazov, ki so v drugi državi članici. Luč je ugledal maja 2017 z Direktivo Evropskega parlamenta in Sveta 2014/41/EU o evropskem preiskovalnem nalogu v kazenskih zadevah[203]. Ena izmed sedmih pobudnic pri pobudi za EPN je bila tudi Slovenija. Veljati je začel 5. maja 2018 Zakonom o spremembah in dopolnitvah zakona o sodelovanju v kazenskih zadevah z državami članicami Evropske unije (ZSKZDČEU-1B)[204], s katerim je bila implementirana Direktiva. Med drugimi določbami ta nadomešča tudi Konvencijo o medsebojni pravni pomoči iz leta 2000[205].

---

[201] 20 čl. Zakon o ratifikaciji Konvencije o medsebojni pravni pomoči v kazenskih zadevah med državami članicami Evropske unije, ki jo je Svet pripravil na podlagi 34. člena Pogodbe o Evropski uniji (Uradni list RS – Mednarodne pogodbe, št. 7/05).

[202] OKVIRNI SKLEP SVETA 2008/978/PNZ z dne 18. decembra 2008 o evropskem dokaznem nalogu za namene pridobitve predmetov, dokumentov in podatkov za uporabo v kazenskih postopkih, L 350/72.

[203] DIREKTIVA EVROPSKEGA PARLAMENTA IN SVETA 2014/41/EU z dne 3. aprila 2014 o evropskem preiskovalnem nalogu v kazenskih zadevah, L 130/1.

[204] Zakon o sodelovanju v kazenskih zadevah z državami članicami Evropske unije (Uradni list RS, št. 48/13, 37/15 in 22/18).

[205] Sporočilo za medije Evropske komisije o evropskem preiskovalnem nalogu. URL: https://europa.eu/rapid/press-release_IP-17-1388_sl.htm (13.6.2019).

Omogoča, da so čezmejne kazenske preiskave enostavnejše in hitrejše, kar je še toliko bolj pomembno pri preiskovanju KD iz oblaka. »Država izdajateljica[206]« od »države izvršiteljice« zahteva, da zbira dokaze v kazenskih postopkih, kar vključuje tudi med drugim izvajanje preiskav. Velja med državami članicami EU in temelji na vzajemnem priznavanju med državami članicami[207] ter vključuje vse preiskovalne ukrepe[208] (razen ustanovitve skupne preiskovalne skupine). Vsebuje tudi določbe za čezmejni nadzor telekomunikacij.

Nekatere pomembne prednosti, ki jih omogoča evropski preiskovalni nalog v kazenskih zadevah[209]:

- Konstruira celovito in enotno orodje z obsežnim področjem uporabe – z EPN se nadomešča razdrobljen pravni okvir za pridobivanje dokazov. Postopek zajema vse od zasega dokazov do posredovanja obstoječih dokazov.
- Predpisuje stroge roke za zbiranje zahtevanih dokazov – DČ predpisuje 30-dnevni rok za odločitev o priznanju. Ob sprejetju imajo nato države še 90-dnevni rok za dejansko izvršitev zahtevanih preiskovalnih ukrepov.
- Zavrnitev naloga le v določenih izjemnih primerih – omejuje organa prejemnika glede zavrnitve izvršitve naloga, to lahko stori le, če je zahtevek v nasprotju s temeljnimi pravnimi načeli ali če škodi interesom nacionalne varnosti.
- Standardizirani obrazec in manj birokracije – obrazec v uradnem jeziku države izvršiteljice omogoča lažje razumevanje organom pri postopanju v postopku.
- Varovana je temeljna pravica do obrambe – ob izdaji naloga mora organ oceniti nujnost in sorazmernost[210] preiskovalnega ukrepa. Dodatni varnosti filter je sodni organ, ki mora izdati ali potrditi EPN, kar omogoča varovanje pravice do obrambe.

»Reševanje čezmejnega kriminala zunaj nacionalnih meja zahteva prilagoditev pravnih okvirjev držav, v katerih se izvajajo preiskave in tudi preiskovalnih pooblastil, ki jih imajo pravosodni organi DČ«, kot je še posebej poudaril generalni pravobranilec Yvesa Bota v sklepnih predlogih, predstavljenih aprila letos v povezavi z zadevo zadevi *C-324/1- kazenski postopek zoper Ivana Gavanozova*[211]. Navaja, da se z Direktivo 2014/41 poenostavlja pravni okvir za zbiranje dokazov v preiskovalnih postopkih in izboljšuje njihova učinkovitost. V sklepnih predlogih pa predvsem poudarja, da je dotični primer prva možnost sodišča za razlago Direktive 2014/41 v smislu, da se opredeli in najde »pravo ravnovesje med učinkovitostjo in hitrostjo preiskovalnih ukrepov na eni strani ter varstvom pravic oseb, na katere se nanašajo ti preiskovalni ukrepi, na drugi.«[212]

---

[206] 1. člen Direktive.

[207] Načelo vzajemnega priznavanja je splošno uveljavljeno načelo in pomeni, da mora vsaka država EU poznati in izvesti zahtevo druge države na enak način, kot če bi obravnavala odločitev domačih organov.

[208] Kot so tajne preiskave in prestrezanje telekomunikacij, ukrepe za zavarovanje dokazov, začasno premestitev pridržanih oseb za namene zbiranja dokazov, itd.

[209] Povzeto po: Sporočilo za medije Evropske komisije o evropskem preiskovalnem nalogu. Vir: https://europa.eu/rapid/press-release_IP-17-1388_sl.htm (13.6.2019).

[210] Odreditveni organ lahko izda EPN le, če je preiskovalni ukrep nujen, sorazmeren in dovoljen tudi v državi izvršiteljici primerih.

[211] Skupni predlogi generalnega pravobranileca Yvesa Bota, v zadevi C-324/1- kazenski postopek zoper Ivana Gavanozova.URL:http://curia.europa.eu/juris/document/document.jsf?text=&docid=212923&pageIndex=0&doclang=sl&mode=req&dir=&occ=first&part=1&cid=8464029 (22.9.2019).

[212] Prav tam, tč. 6.

Menim, da je evropski preiskovalni nalog dober mehanizem tudi za pridobivanje elektronskih dokazov iz oblaka, predvsem ker predpisuje strožje pogoje za zbiranje dokazov in točno določa izrecne pogoje, pod katerimi se lahko zavrne nalog.

5.5. E-EVIDENCE ALI BOLJŠI DOSTOP DO ELEKTRONSKIH DOKAZOV

"Trenutno 85% vseh kazenskih preiskav vključuje elektronske podatke!"[213]

Evropska unija se zaveda, da tradicionalna preiskovalna orodja niso vedno prilagojena digitalnemu okolju, zato išče nove in primernejše možnosti, ki bi preiskovalnim organom omogočalo enostavnejše dostopanje do dokazov, shranjenih v oblaku v drugi državi članici ali drugje po svetu. Potrebno je uvesti moderna preiskovalna orodja, ki bodo omogočila enostavnejši, hitrejši in učinkovitejši dostop do elektronskih dokazov.

Kot že opisano v poglavju o elektronski dokazih, so ti digitalni podatki v elektronski obliki (kot so npr. IP naslov, elektronska pošta, besedilna sporočila ali vsebina iz aplikacij za pošiljanje sporočil, digitalne slike ipd.), in se kot taki lahko uporabijo za preiskovanje in pregon kaznivih dejanj. Shranjeni so na nosilcih podatkov, večinoma so se ti podatki nahajajo v oblaku strežnikov ponudnikov komunikacijskih storitev, ti pa se lahko nahaja v državi, kjer se preiskuje kaznivo dejanje ali v kakšni drugi državi. "Čezmejna zahteva za pridobitev e-dokazov se vloži v več kot 50% vseh kazenskih preiskav!"[214] Vprašanje pa je, kako in na kakšen način lahko organi pregona pridejo do teh podatkov.

Komisija EU je aprila 2018 predlagala zakonodajna predloga o e-dokazih, in sicer:

- Uredbo o evropskem nalogu za predložitev in evropskem nalogu za zavarovanje elektronskih dokazov v kazenskih zadevah[215] in
- Direktivo o določitvi harmoniziranih pravil o imenovanju pravnih zastopnikov[216] za namene zbiranja dokazov v kazenskih postopkih.

Oba zakonodajna predloga predstavljata najnovejši skupni pravni okvir o elektronskih dokazih, v okviru katerega si EU prizadeva za izboljšanje čezmejnega dostopa do e-dokazov, ki bo omogočal, da se sodni nalogi naslovijo neposredno na ponudnika storitev ali njihovega pravnega zastopnika v drugi državi članici.

Predlagana uredba bo organom kazenskega pregona omogočila dostop hitrejši dostop do e-dokazov, ki so shranjeni pri ponudniku storitev, ne glede na to, kje točno se nahajajo. Uvaja dva naloga in sicer:

---

213 URL: https://www.consilium.europa.eu/sl/policies/e-evidence/ (13.6.2019).

214 Prav tam.

215 Predlog uredbe EVROPSKEGA PARLAMENTA IN SVETA o evropskem nalogu za predložitev in evropskem nalogu za zavarovanje elektronskih dokazov v kazenskih zadevah (17.4.2018, COM(2018) 225 final). URL: https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0012.02/DOC_1&format=PDF (16.9. 2019).

216 V nadaljevanju PZ.

- Nalog za predložitev dokazov bo omogočal sodnim organom države članice (v kateri se preiskuje kaznivo dejanje), da zahtevo do dostopa do e-dokazov naslovijo neposredno na ponudnika storitev v drugi državi članici. Uredba določa rok za odgovor ponudnika storitev na zahtevo, ki je 10 dni, v nekaterih izjemnih in zadostno utemeljenih primerih pa se še ta rok skrajša na 6 ur,
- Nalog za zavarovanje je zelo pomembnega pomena, saj bo ponudniku storitev onemogočal, da izbriše e-dokaze v vmesnem času, ko bo nalog za predložitev še v obdelavi.

Navedena direktiva bo poglavitni okvir za uporabo predlagane uredbe, saj določa pravila za imenovanje PZ ponudnikov storitev, kateri bo odgovoren za prejem odločb in nalogov ter za njihovo izvajanje. Vsi ponudniki storitev bodo morali imenovati PZ v EU. Marca letos je Svet dosegel kompromis o stališču glede pravil za imenovanje PZ, iz sporočila za javnost Sveta EU z dne 8.3.2019[217] pa lahko izluščimo nekatere najbolj glavne elemente tega kompromisa, ki so:

- Glede meril za določitev lokacije PZ: ti so v eni izmed DČ, kjer imajo ponudniki storitev svojo poslovno enoto ali kjer ponujajo svoje storitve;
- Solidarna odgovornost v primeru neizpolnjevanja obveznosti se deli med ponudnike storitev in PZ;
- Potrebno je PZ zagotoviti zadostne vire ter pooblastila za opravljanje svojih nalog;
- PZ se lahko uporabijo tudi za zbiranje drugih vrst dokazov, kakor pa samo e-dokazov. Lahko prejemajo tudi druge zahtevke v zvezi s kazenskim postopkom, kot npr. EPN (gl. točko 4.3.);
- Sankcije naj bodo »učinkovite, sorazmerne in odvračilne«;
- Cel seznam PZ bo javno dostopen, predvsem zato, da bo za organe kazenskega pregona dostop preprost, predvsem prek Evropske pravosodne mreže na področju kazenskih zadev.

5.6. CLOUD ACT (ZDA)

V želji po posodobitvi zakonov, ki se nanašajo na nadzor in zasebnost podatkov v oblaku, je bil 23. marca 2018 sprejet Cloud Act. Uveden je bil pravzaprav po težavah, ki jih je imel Zvezni urad za preiskave (v nadaljevanju angl. *FBI*) s pridobivanjem oddaljenih podatkov od ponudnikov storitev z uporabo Zakona o shranjenih komunikacijah (angl. SCA - *Stored Communications Act*[218]), kateri pa je bil napisan leta prej, natančneje leta 1986, kakor se je pa RO uveljavilo v tolikšni meri, kot ga poznamo danes. SCA v današnjem času, ko za potrebe kazenskega postopka potrebno pridobivati ključne podatke iz oblaka od ponudnikov storitev, zakon deluje kot »zakon o blokiranju«.[219] Vsebuje zakonsko izjemo, ki izrecno prepoveduje ameriških ponudnikom storitev s sedežem v ZDA, da razkrivajo tujim vladam komunikacijske vsebine – razen, če med to državo obstaja bilateralni sporazum na podlagi CLOUD Act-a. SCA velja tudi v primeru, če je tuja država (*non-US government*) pridobila odredbo o razkritju v skladu s svojimi nacionalnimi zakoni.[220]

---

[217] Vir: https://www.consilium.europa.eu/sl/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/ (maj 2019)

[218] URL: https://en.wikipedia.org/wiki/Stored_Communications_Act#Microsoft_Corporation_v._United_States_of_America (21.9.2019).

[219] P. Swire, J. Daskal, Frequently asked questions about the U.S. Cloud Act (16.4.2019). URL: https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act/ (22.9.2019).

[220] Prav tam.

Vzrok za sprejetje Cloud Acta je bil primer *Microsoft vs. U.S.*[221], ki je povzročal Zveznemu uradu za preiskave kar nekaj preglavic[222]. Šlo je za primer preiskovanja trgovine z drogami leta 2013. Ameriški državljan je imel v svojem oblaku obremenjujoče podatke, ki so bili potrebni za preiskavo, na Microsoftovih oddaljenih strežnikih na Irskem. FBI je trdil, da ima Microsoft popoln nadzor nad podatki in tako pozval Microsoft na izročitev teh podatkov na podlagi SCA, vendar je Microsoft zavrnil zahtevo, saj naj bi se SCA nanašal samo na izročitev podatkov, ki so na ameriškem ozemlju. FBI je sicer ugotovil, da bi lahko zahtevane podatke pridobil s pomočjo pogodbe o medsebojni pravni pomoči za pomoč pri odkrivanju podatkov med čezmejnim kazenskim pregonom, vendar tega ni začel, saj je lahko ta postopek zelo počasen in bi tako postal ovira za nadaljnje prizadevanje sprejetja nove zakonodaje. Medtem ko je bila obravnavana zadeva na Vrhovnem sodišču ZDA, je sodišče po soglasju vlade in Microsofta sprejelo Cloud Act.

Cloud act (angl. *The Clarifying Lawful Overseas Use od Data Act*) je sestavljen iz dveh ključnih delov. En del odgovarja na zaskrbljenost tujih vlad glede ameriških zakonov, ki omejujejo dostop tujih organov do komunikacijskih vsebin, ki jih hranijo ameriški ponudniki storitev. Ti zakoni vsebujejo omejitve, ki veljajo tudi v primeru, ko tuje vlade iščejo dostop do podatkov o svojih državljanih pri preiskovanju lokalnega kriminala. Ta del CLOUD Act-a dovoljuje oblikovanje bilateralnih izvršilnih sporazumov, ki bi odpravili te omejitve in s tem omogočili tujim vladam dostop do komunikacijskih vsebin neposredno od ameriških ponudnikov storitev, pod določenimi pogoji. Drugi del pa pojasnjuje pravila, ki urejajo dostop ameriških organov kazenskega pregona do podatkov, ki jih hranijo ameriški ponudniki storitev. Če povzamemo, Cloud Act omogoča ameriškim organom kazenskega pregona, da jim ponudniki storitev neposredno posredujejo zahtevane podatke, shranjene na strežnikih, ne glede na to, ali so podatki shranjeni v ZDA ali zunaj njenega ozemlja in dovoljuje oblikovanje bilateralnih sporazumov z državami zunaj Amerike, da lahko njihovi organi pregona prav tako neposredno pridobijo zahtevane podatke za postopek kazenskega pregona.

Kot navedeno zgoraj, bi lahko organi pregona pridobili v primeru *Microsoft* potrebne podatke tudi na podlagi Pogodbe o medsebojni pravni pomoči pri odkrivanju podatkov med čezmejnem kazenskim pregonom[223] (angl. MLAT – Mutual Legal Assistace Treaty), ki je pogodba med dvema ali več državami za potrebe zbiranja in izmenjevanja informacij za potrebe javnih in kriminalnih zadev. Ker pa je v tem primeru postopek »dveh varnostnih filtrov«[224] je to zelo dolgotrajen in kompliciran proces, ki pa v današnji moderni dobi, vsaj za pridobivanje podatkov iz oblaka, ni več primeren.

Cloud Act je odlična podlaga za pridobivanje podatkov od ameriških ponudnikov storitev, tako za ameriške organe pregona, kot za organe tujih držav. Omogoča neposredno pridobivanje podatkov od ponudnikov storitev, tako ameriških kot ne-ameriških organov pregona, seveda pod določenimi pogoji, kar je bolje od določil po SCA zakonu.

221

222 Povzeto po: https://en.wikipedia.org/wiki/Microsoft_Corp._v._United_States (16.7.2019).

223 Pogodba je bila podpisana 25.6.2003.

224 Postopek opisan v poglavju MPP in prostorskega vidika zasebnosti, gl. tč. 5.1.2.

5.7. (NE)USTREZNOST OBSTOJEČIH MEHANIZMOV MEDNARODNE PRAVNE POMOČI

Skozi pregled obstoječih in preteklih mehanizmov v tem poglavju nam da jasno vedeti, da se morajo pravni okvirji, ki določajo pogoje za pridobitev elektronskih dokazov vseskozi prilagajati tehnološkemu razvoju. Mednarodna pravna pomoč v kazenskih zadevah je pri tem ključnega pomena. V okviru EU je cilj poenotenega pravnega okvirja v okviru mednarodne pravne pomoči v kazenskih zadevah, predvsem pri pridobivanju dokazov iz oblaka. Zakon o spremembah in dopolnitvah zakona o sodelovanju v kazenskih zadevah z državami članicami Evropske unije (ZSKZDČEU-1B) nadomešča Konvencijo o medsebojni pravni pomoči iz leta 2000 in s tem sledi potrebam tehnološkega razvoja.

Z Uredbo o evropskem nalogu za predložitev in evropskem nalogu za zavarovanje elektronskih dokazov v kazenskih zadevah in Direktivo o določitvi harmoniziranih pravil o imenovanju pravnih zastopnikov za namene zbiranja dokazov v kazenskih postopkih se sledi cilju k enotnosti pravnih okvirjev o elektronskih dokazih, v okviru katerega si EU prizadeva za izboljšanje čezmejnega dostopa do e-dokazov, ki bo omogočal, da se sodni nalogi naslovijo neposredno na ponudnika storitev ali njihovega pravnega zastopnika v drugi državi članici.

6. SKLEP

Čezmejnost interneta predstavlja storilcem kibernetskih kaznivih dejanj velike prednosti, saj lahko pri svojem izvrševanju delujejo prikrito, se nahajajo pod lažnimi lokacijami, kar preiskovalcem teh kaznivih dejanj povzroča ogromne preglavice. Pri pregonu kibernetskih kaznivih dejanj morajo organi pregona pridobiti ustrezne relevantne podatke o osumljencu, o njegovih aktivnostih, in elementi, kot so čezmejnost interneta, identifikacija storilec, uporaba novih elektronskih dokazov, predstavljajo preiskovalcem kibernetske kriminalitete zelo velike preglavice. Pri pridobivanju relevantnih podatkov, ki bodo služili kot elektronski dokazi v postopkih pregona kibernetske kriminalitete morajo organi zakona upoštevati standarde in omejitve pri posegih v pravico do zasebnosti obravnavanih posameznikov kot obdolžencev.

V poglavju o zasebnosti, sem obravnavala vprašanje kako in na kakšen način lahko organi pregona dostopajo do relevantnih podatkov, ki jih potrebujejo za kazenski pregon. Dejstvo je, da je pravica do zasebnosti ustavno varovana pravica in kot taka uživa zaščito v mednarodnem okolju, zato poseg vanjo predstavlja občuten poseg v človekove pravice in temeljne svoboščine, ki je dopusten samo ob izpolnjevanju strogih pogojev. Nad svojo zasebnostjo ima človek sam oblast, pa naj se ta nanaša na prostor, v katerem zadovoljuje svoje potrebe in interese ali na vsebino komunikacij, katere ima z zunanjim svetom. Pravica ni absolutna, saj se njeno pravno varstvo konča, ko se mora varovati širši javni interes ali ob izkazani močnejši interes drugega posameznika. Od *Silverman standarda*, ki velja za opredelitev »ustavno zaščitenega območja« glede nerazumnih preiskav in zasegov iz četrtega amandmaja se je preko *Katza* uveljavil standard »utemeljenega pričakovanja zasebnosti«, kateri omogoča posamezniku pričakovanje zasebnosti v nekem prostoru, kjer je tako pričakovanje lahko objektivno priznano. S *Katzom* se je razširil spekter apliciranja nerazumnih preiskav in zasegov tudi na neoprijemljive komunikacije. Novejša sodna praksa se že nanaša na nosilce podatkov in na vprašanja, kako lahko z njimi ravnajo organi kazenskega pregona. Z *Riley v. California* primerom je jasno, da mora imeti policija za zaseg elektronskih nosilcev imeti za to ustrezni preiskovalni nalog, saj ti nosilci vsebujejo toliko osebnih podatkov in informacij. Ista zahteva za preiskovalni nalog velja tudi glede pridobitve dostopa do zgodovinskih izpiskov od telekomunikacijskega ponudnika, ki vsebujejo fizično lokacijo mobilnih telefonov, kot je razsodilo Vrhovno sodišče Amerike leta 2018 v primeru *Carpenter v. Združene države Amerike*. Obravnavana relevantna sodna praksa v nalogi, glede posegov organov v komuniakcijsko zasebnost se nanaša večinoma na množično nadzorovanje komunikacij s strani varnostno-obveščevalnih služb in organov pregona (*Klass in drugi proti Nemčiji, Zakharov proti Rusiji, Big Brother Watch in drugi proti Združenemu kraljestvu*), kot tudi na vprašanje zaščite pravice do komunikacijske zasebnosti in zasebnega življanja, s potrebo po imetju ustrezne sodne odločbe, kot je bilo razsojeno v primeru *Benedik proti Sloveniji.* Dotični primer je zahteval mednarodno sodelovanje več držav, ki je ključnega pomena za pregon kibernetskih kaznivih dejanj.

Kljub prenovljenem Zakonu o kazenskem postopku z novelo N, pa je rešitev urejanja pravnih okvirjev za učinkovitejši in hitrejši postopek pregona kibernetskih kaznivih dejanj v mednarodnem sodelovanju in ne v nacionalnih zakonodajah. Potrebujemo usklajenem odziv na kibernetsko kriminaliteto, saj se pri pregonu odpirajo mnogi izzivi kibernetskega sveta, ki so jih prepoznali preučevalci prava, na katere pa zakonodaja in sodna praksa še ne more ponuditi ustreznih odgovorov. V okviru EU je cilj poenotenega pravnega okvirja v

okviru mednarodne pravne pomoči v kazenskih zadevah, predvsem pri pridobivanju dokazov iz oblaka, tako da se mora izboljšati in pospešiti čezmejni dostop do elektronskih dokazov.

V prihodnje bo potrebna uskladitev preiskovalnih dejanj in nova posodobljena procesna pravila. Potrebno bo nujno zagotoviti ustrezne pravne okvirje, da bodo imeli vsi ponudniki storitev (s tem mislim predvsem na ponudnike oblačnih storitev), bodisi s sedežem v EU ali Ameriki, enake obveznosti s posredovanjem elektronskih dokazov za potrebe kazenskih postopkov. Prvi korak k temu je bil storjen s Cloud Actom, na ravni EU pa je Evropska Komisija februarja letos naredila še večji napredek, saj je predlagala začetek pogajanj o čezmejnem dostopu do elektronskih dokazov, potrebnih za izsleditev nevarnih kriminalcev in teroristov.[225] Na podlagi dveh sklepov Evropskega sveta iz oktobra 2018[226] Komisija predstavlja dva sklopa pogajalskih direktiv. En sklop glede pogajanj z ZDA in drug sklop za dodatni protokol h Konvenciji o kibernetski kriminaliteti. Obe pogajalski direktivi, ki ju mora še odobriti Svet, vključujeta močna varnostna merila glede zasebnosti zahtevanih podatkov, varstva teh podatkov in varovanja zasebnosti posameznikov.[227]

[225] URL: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en (22.9.2019).
[226] URL: https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf (22.9.2019).
[227] Povzeto po: URL: https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf (22.9.2019).

7. VIRI

7.1. MONOGRAFIJE

Kovačič Matej, Nadzor in zasebnost v informacijski družbi: Filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu, Fakulteta za družbene medije, Ljubljana, 2007.
Lampe Rok, Pravo človekovih pravic: sistem človekovih pravic v mednarodnem, evropskem in ustavnem pravu, Uradni list Republike Slovenije, Ljubljana, 2010.
Završnik Aleš, Kibernetska kriminaliteta, GV založba: Inštitut za kriminologijo pri Pravni fakulteti, Ljubljana, 2015.

7.2. KNJIGE VEČ AVTORJEV

Ambrož Matjaž, Bavcon Ljubo, Fišer Zvonko, Korošec Damjan, Sancin Vasilka, Selinšek Liljana, Škrk Mirjam, stvarno kazalo Sabina Zgaga; Mednarodno kazensko pravo, Uradni list Republike Slovenije, Ljubljana, 2012.

Dimc Maja, Dobovšek Bojan; Kriminaliteta v informacijski družbi: Pravne podlage, preiskovanje in zaseg: Preiskovanje kibernetske kriminalitete; Fakulteta za varnostne vede, Ljubljana, 2012.

Šugman Stubbs Katja, Gorkič Primož; Dokazovanje v kazenskem postopku, GV založba, Ljubljana, 2011.

7.3. POGLAVJA IZ ZBORNIKOV

Gorkič Primož, Nekatera vprašanja jurisdikcije za kazniva dejanja kibernetične kriminalitete, v:Zbornik znanstvenih razprav – LXVII. letnik, (2007), str. 73-93.

Selinšek Liljana, Digitalni dokazi in računalniška forenzika, Digitalni dokazi v kazenskem postopku: pogledi na aktualna vprašanja, v: Završnik Aleš (ur.) Kriminaliteta in tehnologija: kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon?, Inštitut za kriminologijo pri Pravni fakulteti, Ljubljana, 2010, str. 97-121.

Šugman Stubbs Katja, Nove tehnologije in njihov vpliv na pojavnost in pregon kriminalitete, v: Zbornik znanstvenih razprav – LXXIII. letnik, (2013), str 197-217.

Zgaga Markelj, Zakon o kazenskem postopku (ZKP): z novelo ZKP-N, Uvodna pojasnila, (2019), str. 43-63.

7.4. ČLANKI

Branko Lobnikar, Lobnikar Alenka, Pravica do zasebnosti pri izvajanju policijskih pooblastil – analiza percepcije policijskih šefov, v:Revija za kriminalistiko in kriminologijo, 62 (2011), št. 4, str. 333-343.

Brvar B., Pojavne oblike zlorabe računalnika, v:Revija za kriminalistiko in kriminologijo, (1982), str. 94.

Gorkič Primož, Sodobni prikriti preiskovalni ukrepi, drugič: forenzični računalniški programi, 2014.

Jakulin Vid, Kazenskopravni vidiki, v: Podjetje in delo, 22 (1996) 5/6, str. 823-824.

Lampe Rok, Mednarodnopravni vidiki pravice do zasebnosti – jurisprudenca 8. Člena Evropske konvencije o človekovih pravicah in temeljnih svoboščinah, v:Pravnik: revija za pravno teorijo in prakso, 59 (2004), št. 4/6, str. 225.

7.5. SODNE ODLOČBE

Benedik proti Sloveniji (ESČP, št. 62357/14 z dne 24. 4. 2018).
Big brother watch in drugi proti Združenemu kraljestvu, (ESČP, št. 58170/13, 62322/14 in 24960/15 z dne 13. 9. 2018).

Camenzind v. Švica (ESČP, št. 21353/93 z dne 16.12.1997).

Carroll v. United States, (U. S. Supreme Court, 267 U.S. 132, 1925).
I Ips 169/97.
Katz v. United States, 389 (U.S. Supreme Court 347, 361 1967).
Klaas et. Al. V. ZR Nemčija (ESČP, št. 5029/71 z dne 6.9.1978).
L.M. v. Italy (št. 60033/00 z dne 8.2.2005).
Microsoft v. U.S. (253 F.3d 34 (D.C. Cir. 2001 z dne 9.9.2015).

Panteleyenko v. Ukrajina (ESČP, št. 11901/02 z dne 29.6.2006).

Riley v. California (U.S. Supreme Court 134 S. Ct. 2473, 2014).
Silverman v. United States, (U.S. Supreme Court 365 U.S. 505, 1961).
Smirnov v. Rusija (ESČP, št. 71362/01 z dne 7.6.2007).

United States v Miller (U.S. Supreme Court 307 U.S. 174, 1939).
U-I-45/08.

U-I-25/95.
U-I-25/95.
Up-32/94.
Up-106/05.
Up-106/05.
U.S. v. Microsoft (253 F.3d 34 (D.C. Cir. 2001)
VSL Sodba II Kp 50685/2012.

Zakharov proti Rusiji (ESČP št. 47143/06 z dne 4.12.2015).

7.6. PRAVNI VIRI

Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa 2005/222/HJA. L 218/8

Direktiva 2014/41/EU Evropskega parlamenta in Sveta z dne 3. aprila 2014 o evropskem preiskovalnem nalogu v kazenskih zadevah, L 130/1.

Evropska konvencija o človekovih pravicah in temeljnih svoboščinah, Uradni list RS – Mednarodne pogodbe, št. 7/94.

Evropska konvencija o kibernetski kriminaliteti, Uradni list RS – Mednarodne pogodbe, št. 17/04.

Kazenski zakonik (Ur. l. RS, št. 50/12, 6/16, 54/15, 38/16, 27/17).

OKVIRNI SKLEP SVETA 2008/978/PNZ z dne 18. decembra 2008 o evropskem dokaznem nalogu za namene pridobitve predmetov, dokumentov in podatkov za uporabo v kazenskih postopkih, L 350/72

Predlog uredbe EVROPSKEGA PARLAMENTA IN SVETA o evropskem nalogu za predložitev in evropskem nalogu za zavarovanje elektronskih dokazov v kazenskih zadevah (17.4.2018, COM(2018) 225 final).
Ur. l. RS št. 62/2004 z dne 7.6.2004.

Vrhovno sodišče – Pravna mnenja 1/2012, str. 7, obr. Z dne 6.4.2012.

Zakon o ratifikaciji Konvencije o medsebojni pravni pomoči v kazenskih zadevah med državami članicami Evropske unije, ki jo je Svet pripravil na podlagi 34. člena Pogodbe o Evropski uniji (MKPPKZ), (Uradni list RS – Mednarodne pogodbe, št. 7/05).

ZKP-N, Uradni list RS, št. 63/94, 25/96 - odl. US, 39/96 - odl. US, 5/98 - odl. US, 49/98 - ZPol, 72/98, 6/99, 66/00, 111/01, 32/02 - odl. US, 44/03 - odl. US, 56/03, 43/04, 68/04 - odl. US, 101/05, 14/07, 40/07 - odl. US, 102/07 - ZSKZDČEU, 21/08 - odl. US, 23/08 - ZBPP-B, 65/08 - odl. US, 68/08, 89/08 - odl. US, 77/09, 88/09 - odl. US, 29/10 - odl. US, 58/11 - ZDT-1, 91/11, 47/13, 87/14, 8/16 - odl. US, 64/16 - odl. US, 65/16 - odl. US, 16/17 - odl. US, 59/17 - odl. US, 66/17 - ORZKP153,154, 1/19 - odl. US, 22/19, 48/19 - odl. US.

7.7. INTERNETNI VIRI

A. Rupnik, Konvencija o kibernetski kriminaliteti »Budimpeštanska konvencija«, URL: http://uploadi.www.ris.org/editor/1132054990Kiber_kriminaliteta.pdf (12.5.2019).

B. Darrow, Yes, the cloud computing category can grow (almost) forever, 2018. Spletni vir: https://www.cio.com/article/3268684/budget/yes-the-cloud-computing-category-can-grow-almost-forever.html. (februar 2019)

B. Schafer, How far can Cloud Computing go?, URL: https://marketbrothersmedia.com/how-far-can-cloud-computing-go/ (3.6. 2019).

G. Klemenčič, Ustavnosodni test utemeljenega pričakovanja zasebnosti, v:Komentar Ustave RS. URL: https://e-kurs.si/komentar/ustavnosodni-test-utemeljenega-pricakovanja-zasebnosti/ (10.9.2019)

Informacijski pooblaščenec, povzetki sodb Evropskega sodišča za človekove pravice. URL: https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/sodbe-mednarodnih-sodisc/povzetki-sodb/ (21.9.2019).

Guide on Article 8 of the European Convention on Human Rights 290. točka. URL: https://www.refworld.org/pdfid/5a016ebe4.pdf (21.9.2019).

J. Repinc, Odprto pismo medijem glede zlorabe termina »heker«, URL: http://www.lugos.si/novice/odprto-pismo-medijem-glede-zlorabe-termina (10.6. 2019).

M. Kržišnik, Legal challenges of Cloud computing. URL: https://www.linkedin.com/pulse/cloud-computing-mina-kr%C5%BEi%C5%A1nik-fintech-lawyer/ (18.9.2019).

K. Ruan, J. Carthy, T. Kechadi, I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results", Digital Investigation, (2013) Vol. 10-1, , pp. 34-43, 2013. URL: https://www.researchgate.net/publication/271603639_Cloud_forensics_definitions_and_critical_criteria_for_cloud_forensic_capability_An_overview_of_survey_results (19.9.2019).

P. Mell, J. Grance, The NIST Definition of Cloud Computing, URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (12.2.2019).
URL: https://searchitchannel.techtarget.com/definition/cloud-service-provider-cloud-provider (12.2.2019).

P. Swire, J. Daskal, Frequently asked questions about the U.S. Cloud Act (16.4.2019). URL: https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act/ (22.9.2019).

Predlog zakona o spremembah in dopolnitvah zakona o kazenskem postopku (ZKP-N; EVA: 2016-2030-0033 Predlog ZKP-N. URL: https://e-uprava.gov.si/.download/edemokracija/datotekaVsebina/372912?disposition=inline (19.9.2019)

RS, Ministrstvo za pravosodje; spletni vir: http://www.mp.gov.si/si/delovna_podrocja/urad_za_mednarodno_sodelovanje_in_mednarodno_pravno_pomoc/mednarodna_pravna_pomoc/ (13.5.2019).

Varstvo osebnih podatkov in računalništvo v oblaku, smernice Informacijskega pooblaščenca, 2012, str. 5, strav tam. URL: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_rac_v_oblaku.pdf (12.2.2019)
Sporočilo za medije Evropske komisije o evropskem preiskovalnem nalogu. URL: https://europa.eu/rapid/press-release_IP-17-1388_sl.htm (13.6.2019).

Skupni predlogi generalnega pravobranileca Yvesa Bota, v zadevi C-324/1- kazenski postopek zoper Ivana Gavanozova.URL:http://curia.europa.eu/juris/document/document.jsf?text=&docid=212923&pageIndex=0&doclang=sl&mode=req&dir=&occ=first&part=1&cid=8464029 (22.9.2019).

URL: https://en.wikipedia.org/wiki/Microsoft_Corp._v._United_States (16.7.2019).
URL: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en (22.9.2019).
URL: https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf (22.9.2019).
URL: https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf (22.9.2019).
URL: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf (21.9.2019).
URL: https://ii.feri.um.si/sl/studij/osnovni-pojmi-itk/ (14.1.2019).
URL: https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-salesforce-dominates-saas/ (21.9.2019).
URL: https://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/ (20.2.2019).
URL: www.cisco.com (15.1.2019).
URL: https://searchcloudcomputing.techtarget.com/definition/multi-tenant-cloud (21.9.2019).
URL: https://www.techopedia.com/definition/29545/resource-pooling (12.2.2019).
URL: http://www.islovar.org/islovar (12.2.2019)
URL: https://searchcloudcomputing.techtarget.com/definition/cloud-infrastructure (10.9.2019).
URL: https://www.consilium.europa.eu/sl/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/ (maj 2019)
URL:https://en.wikipedia.org/wiki/Stored_Communications_Act#Microsoft_Corporation_v._United_States_of_America (21.9.2019).
URL: https://www.esds.co.in/blog/the-cost-benefits-of-cloud-computing/ (10.9.2019).
URL: https://www.techopedia.com/definition/9550/storage-server (10.9.2019).
URL: https://www.ibm.com/cloud/learn/benefits-of-cloud-computing. (10.9.2019).
URL: https://cloud.oracle.com/sl_SI/iaas/sla
URL: https://www.networkworld.com/article/3394341/when-it-comes-to-uptime-not-all-cloud-providers-are-created-equal.html (september 2019).

URL: https://www.forbes.com/sites/forbestechcouncil/2017/12/14/four-ways-to-avoid-vendor-lock-in-when-moving-to-the-public-cloud/#39272d1261f9 (8.6.2019). URL: https://en.wikipedia.org/wiki/Vendor_lock-in (8.6.2019).

URL: https://www.techopedia.com/definition/2387/cybercrime (13.6.2019)

URL: https://sl.wikipedia.org/wiki/Digitalna_forenzika (20.9.2019).

URL: https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf (18.9.2019).

URL: https://searchcloudcomputing.techtarget.com/definition/multi-tenant-cloud (18.9.2019).

URL: https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools. (28.8.2019).

URL: https://www.law.cornell.edu/wex/expectation_of_privacy (19.9.2019).

URL: https://en.wikipedia.org/wiki/Katz_v._United_States (19.9.2019).

URL:https://www.consilium.europa.eu/sl/policies/e-evidence/ (13.6.2019).

URL: https://dictionary.cambridge.org/dictionary/english/warrant (15.9.2019).