UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

POMEN KRIPTOGRAFIJE PRI ZAGOTAVLJANJU VARNOSTI OSEBNIH PODATKOV NA INTERNETU

Ljubljana, 28. september 2018 JORG KARAS

IZJAVA O AVTORSTVU

Podpisani Jorg Karas, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Pomen kriptografije pri zagotavljanju varnosti osebnih podatkov na internetu, pripravljenega v sodelovanju s svetovalcem prof. dr. Alešem Popovičem

I Z J A V L J A M

1. da sem predloženo delo pripravil samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____ Podpis študenta: _____

KAZALO

KAZALO TABEL

KAZALO SLIK

KAZALO PRILOG

SLOVAR IZRAZOV

Asimetrična enkripcija - Način enkripcije, ki za svoje delovanje uporablja dva različna šifrirna ključa – javnega in zasebnega.

Biometrična enkripcija – Način enkripcije, ki za šifriranje uporablja individualne biološke lastnosti posameznika, kot na primer prstne odtise ali očesno mreno.
CIO – Angleško Chief Information Officer – vodilna oseba znotraj organizacije, zadolžena za informacijsko tehnologijo, njeno nemoteno delovanje in varnost.
DPA – Data Protection Act
EDPS – European Data Protection Supervisor
»End-to-end« enkripcija – Način enkripcije, s pomočjo katerega je sporočilo šifrirano od začetka do konca komunikacijske poti.
ENISA – European Union Agency for Network and Information Security
Enkripcija – Proces kriptografije, ki zajema šifriranje podatkov.
E-veščine – Veščine, povezane z internetom in njegovo varno uporabo.
FHE – Angleško Fully Homomorphic Encryption – popolna homomorfična enkripcija.
GDPR – General Data Protection Regulative
Homomorfična enkripcija – Način enkripcije, ki dovoljuje računske operacije na šifriranih sporočilih, in katerih rezultat se odraža na nešifiranih tako, kot da bi bile opravljene v originalni obliki.
Informacijska arhitektura – Načrt informacijskih potreb organizacije na najvišjem nivoju, ki predstavlja informacijske potrebe za izvanje poslovanja.
Informacijska infrastruktura – Fizične zmogljivosti, storitve in upravljanje, povezane z računalniškimi viri organizacije.
Informacijska varnost – S tem izrazom označujemo varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem.
Informacijski sistem – Urejen in organiziran sistem, ki uporabnike oskrbuje z vsemi potrebnimi informacijami za odločanje.
Kibernetski kriminal – Kaznivo dejanje ali prekršek, storjen s pomočjo komunikacijskih naprav v omrežju, ki vključuje računalnik in omrežje.
Kriptografija – Znanost, ki preučuje logično spremembo podatkov.
Kvantna enkripcija – Način enkripcije, ki za svoje delovanje uporablja principe kvantne mehanike in se ne zanaša na matematične predpostavke.
»Nothing to hide argument« – dobesedno »argument ničesar za skriti«, s tem izrazom označujemo stališče kadar nas nadzor tajnih služb ne moti, ker ne počnemo nič ilegalnega.
Simetrična enkripcija – Način enkripcije, ki za svoje delovanje uporablja zgolj 1 ključ, tako za šifriranje, kot tudi za dešifriranje.
Socialni inženiring – Najpogostejše tehnika v primerih zlorabe osebnih podatkov, s katero napadalec od žrtve pridobi zaupne podatke s pomočjo zlorabe zaupanja.
Trade-off izbira – Tehnika povečanja ali zmanjševanja enega ali več željenih izidov z namenom povečanja ali obdržanja drugega željenega izida, ki nam pomaga maksimizirati celotno korist.
ZVOP-1 – Zakon o Varstvu Osebnih Podatkov
Žvižgač – Zaposleni ali bivši zaposleni, ki razkriva po njegovem mnenju nepoštene, neetične in nelegalne dejavnosti in kršitve v organizaciji, ki jih izvajajo trenutni ali nekdanji člani.

UVOD

Podjetja in državne ustanove zbirajo informacije o našem početju, razmišljanju in zasebnem življenju z namenom ustvarjanja dobička in nadzora prebivalstva. Velik del poslovanja podjetij se odvija na spletu, kjer s pomočjo analiziranja naših navad in sledenja obnašanju na spletu oblikujejo produkte in načine trženja. Državne tajne službe pa na drugi strani s tovrstnim načinom nadzorujejo populacijo in odkrivajo zasebna življenja ljudi, tudi če za to nimajo razloga (Greenwald, 2014).

Zakaj bi mobilna aplikacija, ki nam ponuja program za predvajanje glasbe, potrebovala dostop do zgodovine klicev in sporočil? Kaj počnejo banke z našimi podatki in s kom jih delijo? Zakaj želijo zavarovalnice podatke o zgodovini našega zdravljenja in zdravja (Office of the Privacy Commissioner New Zealand, 2017)? Mnogo ljudi bi odgovorilo, da jim je vseeno ali se njihove podatke zbira ali ne, saj nimajo kaj skriti. Strokovno se to imenuje »argument ničesar za skriti« (angl. nothing to hide argument), katerega bistvo je, da je državni nadzor populacije upravičen in da ne ogroža zasebnosti, saj nismo zagrešili kaznivih dejanj in je potreben za odkrivanje nelegalnih aktivnosti. Takšno razmišljanje pa je napačno, saj ni bistvenega pomena kaj organizacije, ki osebne podatke zbirajo, z njimi počnejo, ampak zakaj je to zbiranje sploh potrebno. Odgovore na ta vprašanja bom podal v tej nalogi.

Svoboda je temeljna človekova pravica, ki pa je v zadnjem času pred veliko preizkušnjo. Ogroženost naše zasebnosti namreč nikoli ni bila tako visoka kot danes (Informacijski pooblaščenec Republike Slovenije, 2017). Informacijsko okolje nas sili, da organizacijam dovoljujemo uporabo osebnih podatkov brez natančnega vedenja kaj se z njimi dejansko dogaja. Večina platform, ki vključujejo računalniške programe, mobilne aplikacije, elektronsko bančništvo, zavarovalništvo, idr., zahteva dovoljenje zbiranja in uporabe mnogih podatkov, ki se jih sploh ne tičejo. Ti podatki nimajo nikakršne veze z njihovo primarno dejavnostjo, zato se upravičeno lahko vprašamo, zakaj jih sploh potrebujejo oziroma kaj počnejo z njimi.

Splošna regulativa na področju varnosti podatkov (angl. General Data Protection Regulativev nadaljevanju GDPR) prinaša veliko sprememb tako za fizične kot tudi za pravne osebe. Cilj tega zakona je urediti področje varnosti podatkov v Evropski uniji (v nadaljevanju EU), ga narediti bolj učinkovitega in zaščititi prebivalstvo pred neupravičeno uporabo njihovih podatkov (GDPR Portal, 2018). Največkrat gre za neupravičeno posredovanje osebnih podatkov drugim osebam in nezakonito uporabo le-teh z namenom trženja storitev ali produktov.

Namen magistrskega dela je pokazati posameznikom in podjetjem, da vpeljava tehnologije, ki uporablja kriptografijo, poveča varnost osebnih podatkov na internetu in podjetjem zagotavlja ustrezno raven zaščite pred krajo in zlorabami. Ker gre za zelo specifično področje, bom del naloge posvetil tudi analizi drugih tipov občutljivih in tveganih

podatkov. Veliko ljudi in podjetij namreč še vedno ne razume pomembnosti zavarovanja svojih podatkov in niso dovolj osveščeni o tveganjih kraje podatkov, zato bom skušal dokazati, da je uporaba kriptografije ključnega pomena za učinkovito zaščito podatkov in odpornost proti neželenim napadom. Poleg tehnološkega vidika bom raziskal še zakonske vidike in organe, ki delujejo na tem področju.

Cilj magistrskega dela: Raziskati, kako lahko uporaba sodobnih metod zaščite s pomočjo kriptografije in enkripcije zniža tveganja zlorabe osebnih podatkov na internetu tako za posameznike, kot tudi za podjetja.

Metoda magistrskega dela: Teoretična analiza tuje in slovenske literature s področja kriptografije in varstva osebnih podatkov. Opravil bom pisne intervjuje z dvema državnima in dvema evropskima organoma, pri čemer bom preučil praktične vidike nadzora in izvrševanja zakonodaje na področju varstva osebnih podatkov. Preučil bom izzive, s katerimi se regulatorji soočajo, in potencialne rešitve, ki jih kriptografija ponuja. V nalogo bo vključen ekonomski vidik dodane vrednosti uporabe kriptografske tehnologije in zagotavljanja konkurenčnih prednosti.

Struktura magistrskega dela: Magistrska naloga je sestavljena iz treh delov. V prvem delu se bom osredotočil na področje osebnih podatkov, kjer bom analiziral katere vrste zlorab in tipov osebnih podatkov poznamo. Preučil bom kakšne so zakonske podlage in kako se izvajajo. Zakonske podlage bodo najprej predstavljene na nacionalni, nato še na nadnacionalni-evropski ravni. Pomembno vlogo pri razumevanju pomembnosti učinkovite zaščite podatkov igrajo tudi žvižgači; največkrat bivši zaposleni v tajnih službah, ki so razkrili škodljive prakse nadzora in kontroverzne načine vdora v zasebnost (Greenwald, 2014).V drugem delu bom preučil kriptografijo kot vedo in njen namen pri zagotavljanju večje informacijske varnosti. V analizo bom vključil tehnologije in organizacije, ki uspešno uporabljajo tovrstne zaščite in predstavil koncepte uporabe v prihodnosti. V ta del bom vključil in raziskal pomanjkljivosti informacijskih sistemov, ki uporabljajo enkripcijo (Swenson, 2008). V zadnjem delu bom analiziral ali uporaba kriptografije dejansko poveča varnost in s kakšnimi tveganji se lahko ob uporabi le-te srečamo. Ugotavljal bom tudi ali uporaba kriptografije poveča dobiček podjetij, ali se podjetja tega zavedajo, kateri so najpogostejši problemi pri vpeljavi enkripcijske tehnologije in katere konkurenčne prednosti nam prinaša. Vključil bom vpliv tajnih služb na standarde enkripcije podatkov in njihova prizadevanja za spremembo delovanja sodobne informacijske družbe z namenom popolnega nadzora prebivalcev (Greenwald, 2014). Dodatek drugemu delu bo PRISM program, ki ga je razvila ameriška tajna služba (NSA). Nedavna razkritja so namreč pokazala, da je ta program osnova za največji masovni nadzor prebivalstva v zgodovini katerekoli države na svetu.

1 VARNOST OSEBNIH PODATKOV NA INTERNETU

Razne organizacije tako v fizičnem, kot tudi v virtualnem svetu, zbirajo osebne podatke, njihova analiza pa postaja pomemben del konkurenčnih prednosti podjetij, saj z njo lahko oblikujejo profile svojih potrošnikov, temu primerno prilagajo svoje delovanje in tako maksimizirajo svoj dobiček. Iz potrošniškega vidika je pri večini ljudi danes deljenje podatkov na internetu nekaj vsakdanjega. Podjetja to izkoriščajo za trženje svojih produktov in profiliranje kupcev.

Družbena omrežja, kot na primer Facebook, podjetjem ponujajo ciljano trženje, ki temelji na analizi osebnih podatkov, ki jih posamezniki vnesejo v platformo. Tako lahko podjetja prilagodijo oglaševanje ciljni skupini določenega spola, starostne skupine, ali določenih osebnostnih značilnosti. To je očitno predvsem pri mlajši populaciji. Raziskava je namreč pokazala, da mlajši ljudje nimajo ovir pri deljenju svojih podatkov, ker je njihova osveščenost o posledicah takšnega početja pomanjkljiva, trend zaskrbljenosti o tem pa gre navzdol (Ridley-Siegert, 2015).

Zavedanje širše populacije o pomembnosti varovanja svojih podatkov je relativno nizko, medtem ko je kraja le-teh vse pogostejša. Najbolj učinkovit način zaščite je trenutno enkripcija, ki temelji na različnih stopnjah varnosti ob različnih dolžinah ključev. Države, ki spletni varnosti posvečajo več pozornosti, so podjetjem privlačnejše za poslovanje. Zgrajeno imajo namreč učinkovito informacijsko infrastrukturo, ki podjetjem omogoča varno hrambo podatkov.

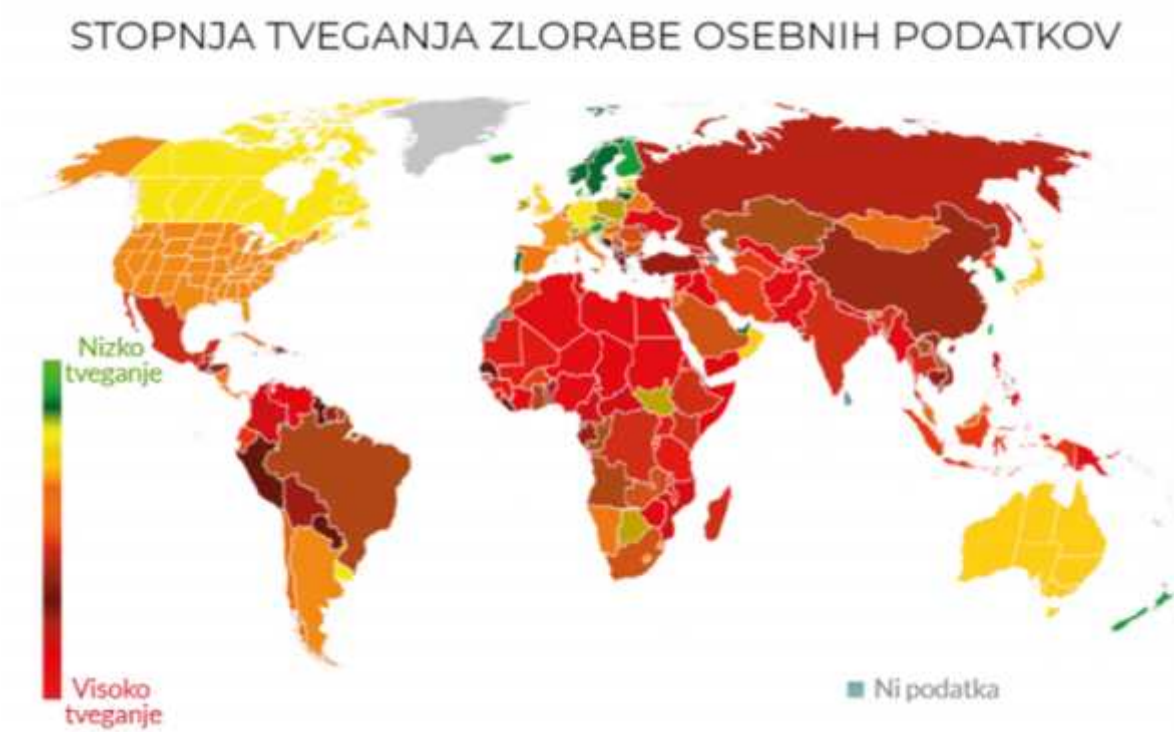
Za začetek si oglejmo, katere države imajo najslabšo raven varnosti informacij in kje je ta varnost na visokem nivoju.

1.1 Stopnja tveganja zlorabe osebnih podatkov v različnih državah

Slika 1 nam prikazuje stopnje tveganja zlorabe osebnih podatkov glede na geografsko lego. Bolj razvite države namenjajo temu problemu več uspešnosti in so s svojo informacijsko infrastrukturo bolj učinkovite in odporne proti napadom, vendar obstajajo izjeme kot je ZDA, kjer imajo sedeže največja spletna podjetja, varnostno tveganje pa je 14.2 %, kar je ne umešča niti med prvih 25 držav glede na varnost osebnih podatkov.

Metodologija ocenjevanja varnosti temelji na analizi IP naslovov v posameznih državah in na analizi naslednjih dejavnikov: korupcije, globalnih konfliktov, terorizma, naravnih nesreč, politike in stanja infrastrukture. Študija je zajemala 3.5 bilijona IP naslovov v 170 državah. Najbolj varna država je Švica, ki ima faktor tveganja 1.6 %, najbolj nevarna pa je Somalija s faktorjem 92.9 %.

Slika 1: Stopnje tveganja zlorabe osebnih podatkov



Vir: An international benchmark of the world's safest - and riskiest - data locations (2017).

Slovenija se s faktorjem tveganja 10.3% uvršča relativno visoko in sicer pred države kot so ZDA, Italija, Španija, Francija, idr. Ta faktor kaže na dobro poslovno okolje v Sloveniji za domača in mednarodna spletna podjetja in na ustrezno raven informacijske varnosti.

1.2 Načini zlorab osebnih podatkov

Za lažje razumevanje problematike potrebe po varnosti osebnih podatkov moramo najprej vedeti, kje se kraje sploh dogajajo in kakšne načine kraj poznamo. Tretje osebe so pri krajah vedno bolj inovativne, vedno pogostejša je uporaba t.i. socialnega inženiringa. Žrtve se tako prepriča, da je na drugi strani pristna oseba, kateri nato slepo zaupa gesla, številke transakcijskih računov in podobno. Preučil bom kako potekajo kraje in na kakšen način se lahko proti njim učinkovito zaščitimo.

Poznamo dva načina kraje osebnih podatkov: fizični in elektronski. Pri prvem gre za nezakonito pridobitev podatkov preko nosilcev zapisov informacij. Tretja oseba brez dovoljenja ukrade nosilec in ga uporablja za dosego različnih ciljev. Pri elektronski kraji gre za pridobitev podatkov preko socialnega inženiringa, vdora v računalniške sisteme in raznih drugih metod, s katerimi je preko spleta možno omogočiti dostop do občutljivih podatkov. Kazniva dejanja na elektronskem področju imenujemo tudi kibernetski kriminal, ki je v zadnjem desetletju postal resen problem. S pojavom kibernetskih vojn med državami in vdori tajnih državnih skupin računalniških strokovnjakov v zaupne podatke drugih držav

predstavlja elektronska kraja podatkov resno grožnjo sodobnim gospodarstvom, zato države in poslovni subjekti namenjajo vedno več sredstev za varnost njihovih sistemov. Ameriška banka JP Morgan Chase tako samo za varnost njihovega elektronskega sistema nameni več kot 250 milijonov ameriških dolarjev letno (Bankrate Corporation, 2017).

1.2.1 Fizična kraja podatkov

Kljub razširjenosti spletnih kraj je fizična kraja še vedno najbolj pogosto uporabljen način kraje podatkov. Z več pogledov je fizična kraja lažja kot spletna, saj ni potreben vdor v omrežje. Podjetja namreč namenjajo sredstva spletni varnosti in ne toliko fizični.

Razširjena uporaba prenosljivih spominskih medijev je omogočila še večjo izpostavljenost občutljivih podatkov (Miller, 2008). Problem je tudi v dostopu do informacij. V veliko primerih lahko že zaposleni na najnižjih nivojih organizacije dostopajo do dokumentov, ki se jih ne tičejo. Le-ti ob morebitnih konfliktih ali odpustitvijo prekopirajo dokumente na prenosljiv medij in jih predajo tretjim osebam z namenom oškodovanja (bivšega) delodajalca. Dovell Bonnett, ustanovitelj podjetja Access Smart Ltd., ki se ukvarja z minimiziranjem tveganj kibernetskih napadov z uporabo brezstičnih pametnih kartic, opredeljuje naslednje načine in tveganja fizične kraje podatkov:

- Posnemanje kartice (angl. skimming).
- Kraja denarnice ali torbice.
- Kraja računalnika.
- Odklenjeni kabineti podatkovnih baz.
- Podkupovanje zaposlenih z namenom pridobitve podatkov.
- Kraja pošte.

1.2.2 Spletna kraja podatkov

Ribarjenje (angl. Phishing) Izraz phishing izvira iz angleških besed »password« (geslo) in »fishing« (ribarjenje). Predstavlja način pridobivanja osebnih podatkov preko lažnih elektronskih naslovov in spletnih strani. Prevaranti žrtev želijo pripeljati do tega, da jim izda podatke katere lahko zlorabijo. Pri tem uporabljajo različne tehnike socialnega inženiringa, s katerimi vplivajo na psihologijo žrtve in dosežejo dojemanje legitimnosti prevarantov ter njihovih lažnih spletnih strani (Intuit Online Security Center, 2017). Za takšne zlorabe so posledice relativno majhne kadar gre zgolj za odtujitve elektronskih pošt ali podobnih računov, lahko so pa tudi zelo velike kadar gre za krajo denarja z osebnih računov. Po nekaterih podatkih naj bi dnevno nastalo od 100 do 200 novih strani za phishing napade.

Pharming izvira iz angleških besed »farming« (kmetovati) in »pharmacy« (farmacija). Označuje tehniko genetskega inženiringa naslovov spletnih mest (Intuit Online Security Center, 2017). Glavna razlika med phishingom in pharmingom je v tem, da phishing več ali

manj deluje na psihološki ravni z uporabo socialnega inženiringa, pri pharmingu pa gre za tehnične napade, kot na primer neposreden napad na DNS strežnike ali določene datoteke na računalniku uporabnika.

Uporabnik spletne strani je tako prepričan, da je na svoji spletni strani in samozavestno vnaša občutljive podatke, kateri so takoj po vnosu na voljo prevarantom, ki so ustvarili to lažno stran. Koncepti odprtih sistemov vzajemnega priznavanja transakcij to tveganje povsem odpravljajo, vendar so trenutno še nerazviti in v začetnih fazah.

Kraja podatkov preko virusa na računalniku. Pri kraji preko virusov gre za različne vrste neželenih programov, katere uporabnik prejme preko kontaminiranih datotek ali drugih virov. Pri tovrstnih krajah gre za različne tipe programov kot so:

- *Malware* – Malware dobesedno pomeni škodljiv program (angl. Malicious software), katerega namen je pridobiti podatke z našega računalnika ali pa onemogočanje določenih funkcij.
- *Spyware* – Gre za programe, ki nadzirajo naše aktivnosti na računalniku. Takšen program največkrat deluje v ozadju, zato uporabnik sploh ne ve, da ga ima.
- *Adware* – Reklamni programi (angl. Advertisement software), ki uporabljajo naše aktivnosti na spletu za trženje produktov. Gre za vsiljive programe, ki jih dobimo tudi z namestitvijo drugih programov.
- *Ransomware* – Gre za kombinacijo angleških besed »ransom« (odkupnina) in »malware« (škodljiv program). S tem izrazom označujemo viruse, ki se nam ob kliku na določeno povezavo namestijo na računalnik in s pomočjo enkripcijskega ključa zaklenejo naše osebne podatke in datoteke. Na ekranu se nam pojavi sporočilo, v katerem je zapisana zahtevana višina odkupnine in rok plačila. V primeru neplačila se enkripcijski ključ uniči in dostop do datotek je trajno onemogočen. To je trenutno eden najbolj dobičkonosnih načinov izsiljevanja posameznikov, saj deluje na podlagi zaznane vrednosti ukradenih informacij posameznika. Strokovna revija HelpNet Security je opravila raziskavo, v kateri je ugotovila, da je povprečna vrednost odkupnine 1400$, in da več kot 70 % ljudi plača odkupnino, če gre za informacije, povezane z njihovo zaposlitvijo.
- Trojanski konj – Najbolj razširjen tip virusa. Trojanski konj se preko metod socialnega inženiringa predstavi kot legitimen in uporaben program. Ko pridobi naše zaupanje, ga namestimo in tako upravljalcem tega programa omogočimo dostop do našega računalnika. Onemogoči nam delovanje in naš računalnik spremeni v t.i. »zombi računalnik«, preko katerega se širi veriga virusa.

Preko teh programov lahko tretja oseba pridobi praktično neomejen dostop do podatkov in tudi do ostalih fizičnih delov računalnika kot na primer spletna kamera ali mikrofon. Programi jim ne omogočijo zgolj zbiranja podatkov ampak tudi nadzor. Takšne prakse so zelo nazorno prikazane v dokumentarnem filmu Citizenfour (2014), kjer Edward Snowden

razkriva, kako je ameriška tajna služba NSA lahko pridobila dostop do celotnega računalniškega sistema kateregakoli uporabnika (Poitras, 2014).

Pomembno je poznati ukrepe, s katerimi minimiziramo tveganja kraje podatkov preko virusov. Pri tem pomembno vlogo igra enkripcija datotek, previdnost pri prenašanju datotek, močna, raznovrstna gesla, fizična zaščita spletne kamere in mikrofona, ipd. Predvsem zaklepanje datotek ali trdega diska onemogoči neposreden dostop tretjim osebam. Obstajajo tudi načini enkripcijskih zaklepov diska s preverjanjem prstnega odtisa, ki pa so relativno dragi v primerjavi z drugimi metodami.

1.2.3 Največji zabeleženi vdori v informacijske sisteme spletnih podjetij

Vdori v informacijske sisteme organizacij se dogajajo vsak dan, najbolj odmevni pa so primeri, pri katerih gre za velika spletna podjetja z ogromnimi bazami informacij, za katera predpostavljamo, da varnost dojemajo resno in imajo primerno zavarovane strežnike, ki vsebujejo občutljive podatke. Še posebej nas preseneti kadar tretjim osebam s škodljivimi nameni uspe vdreti v zdravstvene in finančne sisteme, ki vsebujejo podatke o naših računih, karticah, številkah zdravstvenega zavarovanja in zgodovini bolezni.

Tabela 1: Največji vdori v podatkovne baze spletnih podjetij

Spletno podjetje	**Leto**	**Število ukradenih računov**
AOL	2004	92 milijonov
LinkedIn	2010	117 milijonov
Dropbox	2011	67 milijonov
Yahoo	2012	1 milijarda
Ebay	2012	145 milijonov
Spambot	2015	711 milijonov
Ashley Madison	2015	33 milijonov
MySpace	2015	164 milijonov
Friend Finder Network	2016	412 milijonov

Vir: World's Biggest Data Breaches (2018).

V tabeli 1 je za razumevanje razpona problema vdorov zanimiv primer Ashley Madison, spletne strani, ki napotuje uporabnike k nezvestobi in »skokom čez plot«. Ko je leta 2015 stran bila napadena, so ukradli podatke o več kot 33 milijonih uporabnikov in jih objavili na spletu. To je povrzročilo široko razpravo o tem, ali so takšne strani sploh legalne in ali so tudi najbolj razviti varnostni koncepti sploh odporni proti napadom.

Primer Ashley Madison je pod vprašaj postavil tudi zasebnost posameznikov in razkril, kako lahko ukradene skrivnosti posameznikom uničijo življenja. Razkriti so bili primeri izsiljevanja, kjer so hekerji s podatki izsiljevali večinoma nezveste moške in jim grozili z razkritjem njihovega skrivnega življenja v primeru neplačila (Hosie, 2017).

Mnogi se ne zavedajo količine različnih podatkov, ki sploh so v obtoku, zato bom v spodnjem poglavju analiziral katere vrste osebnih podatkov sploh obstajajo in katere načine klasifikacije le-teh poznamo.

1.3 Klasifikacija osebnih podatkov

Razvrstitev osebnih podatkov v kategorije je stvar subjektivne presoje in kriterijev. Obstaja več vidikov, glede na katere jih lahko razvrstimo: raven tajnosti, faktor tveganja, področje izvora, način shranjevanja, idr.

Klasifikacija podjetja Enterprivacy Consulting Group, ki se že 15 let ukvarja z varnostjo osebnih podatkov, razporeja osebne podatke v skupine glede na področja vpliva teh podatkov. Pri tej klasifikaciji je upoštevanotako posameznikovo javno, kot tudi zasebno življenje. Osebne podatki so razčlenjeni v 6 kategorij, ki se med seboj razlikujejo glede na področje delovanja (Enterprivacy Consulting Group, 2018).

Interni podatki:

- Znanje in prepričanja posameznika (religija, filozofska prepričanja, ipd.)
- Verodostojnost (gesla, PIN kode, ipd.)
- Preference (mnenja, najljubša hrana, najljubša barva, ipd.)

Eksterni podatki:

- Unikatna identifikacija (uporabniško ime, osebna izkaznica, ipd.)
- Etnična pripadnost (rasa, narodnost, ipd.)
- Spolna usmerjenost (seksualne preference, fetiši, ipd.)
- Vedenjski podatki (zgodovina brskalnika, zgodovina telefonskih klicev, ipd.)
- Demografski podatki (starost, dohodek, ipd.)
- Zdravstveni podatki (duševno zdravje, zgodovina zdravljenja, ipd.)
- Fizične karakteristike (višina, teža, starost, ipd.)

Sociološki podatki:

- Profesionalni podatki (nazivi, zgodovina dela, ipd.)
- Kriminalni podatki (obtožbe, oprostitve, ipd.)
- Javno-življenjski podatki (socialni status, zakonski stan, ipd.)
- Družinski podatki (poroke, ločitve, sorodniki, ipd.)
- Socialno-omrežni podatki (prijatelji, znanci, ipd.)
- Komunikacijski podatki (telefonski posnetki, e-mail, ipd.)

Finančni podatki:

- Podatki o računu (številka kreditne kartice ali bančnega računa)

- Lastniški podatki (lastništvo avtomobilov, lastništvo nepremičnin, ipd.)
- Transakcijski podatki (podatki o nakupih, podatki o prodaji, ipd.)
- Kreditni podatki (podatki o kreditih, kreditni sposobnosti, ipd.)

Sledljivi podatki:

- Računalniški podatki (IP naslov, sledi brskalnika, ipd.)
- Kontaktni podatki (e-mail naslov, fizični naslov, ipd.)
- Lokacijski podatki (država, GPS koordinate, ipd.)

Zgodovinski podatki:

- Zgodovina življenja (dogodki, ki so v preteklosti zaznamovali posameznikovo življenje)

Iz zgornjega seznama lahko ugotovimo, da je osebnih podatkov relativno veliko, in da se nahajajo na različnih lokacijah. Na nekaterih lokacijah so brez učinkovite zaščite lahka tarča za kriminalna dejanja ali nepooblaščeno uporabo.

Zgornja klasifikacija podatke razvršča glede na njihovo vrsto, mnoge organizacije pa jih razvrščajo glede na stopnjo zahtevane zaščite. Kalifornijska univerza Berkeley podatke klasificira na način, ki ga prikazuje Tabela 1 (UC Berkeley, 2017):

Tabela 2: Berkeleyevski standard klasifikacije podatkov

Številka nivoja	**Stopnja zaščite**
Nivo 3	Ekstremna
Nivo 2	Visoka
Nivo 1	Zmerna
Nivo 0	Omejena ali ničelna

Vir: UC Berkeley (2017).

Nivo 3: Podatki, ki jih zaznamuje najvišja raven tveganja obojestranskih posledic zlorabe. V to kategorijo spadajo poslovni podatki organizacij, rezervne kopije sistemov, centralne sistemske konzole, ipd.

Nivo 2: Podatki, ki jih zaznamuje statutarna zahteva po obvestilu obeh strank v primeru vdora v zbirko podatkov. V to kategorijo spadajo številke zavarovalnih polic, številke vozniškega dovoljenja, podatki o kreditnih karticah, zdravstveni podatki, ipd.

Nivo 1: Podatki, izdani z namenom obveščanja. V to kategorijo spadajo osebni podatki, ki niso opredeljeni v ostalih treh nivojih in podatki, zaščiteni z pogodbami in sporazumi: podatki o študentih (tudi identifikacijska številka študenta), osebni podatki osebja (tudi identifikacijska številka zaposlenega), licenčni ključi, ipd.

Nivo 0: Podatki, namenjeni širši javnosti.

Smiselna je tudi klasifikacija podatkov, predstavljena v raziskovalni nalogi ameriškega študenta informatike, v kateri navaja naslednjo razvrstitev podatkov v kategorije glede na stopnjo tajnosti podatkov (Ajibuwa, 2009):

- **Strogo zaupni podatki:** Najbolj občutljivi dokumenti o zaupnih stvareh. V to kategorijo spadajo strateški plani in poslovne skrivnosti podjetij, morebitna kraja katerih bi utegnila pustiti nepopravljive posledice.
- **Zaupni podatki:** Podatki, razkritje katerih bi utegnilo ogroziti obstoj organizacije ali njenih operacij. V to kategorijo spadajo poslovni rezultati, zdravstveni podatki zaposlenih, ipd.
- **Zmerno zaupni podatki:** Podatki s srednjo stopnjo zaupnosti, ki so še vedno obravnavani kot zaupni. V to kategorijo spadajo podatki, ki opisujejo načine delovanja organizacije, med katere spadajo podatki o projektih, o delovnih procesih, ipd. Namenjeni so zgolj pooblaščenim osebam.
- **Podatki, namenjeni interni uporabi:** Podatki, ki niso namenjeni javnosti, vendar njihovo morebitno razkritje ne bi imelo večjih posledic. V to kategorijo spadajo podatki o trajanjih sestankov vodstva, poročila internih projektov, ipd.
- **Javni podatki:** Javno dostopni podatki brez oznake tajnosti.

1.4 Zakoni in predpisi na področju varnosti osebnih podatkov

V naslednjih točkah bom raziskal zakone, ki se navezujejo na varnost osebnih in drugih podatkov. V Republiki Sloveniji zaenkrat še ne obstaja sklop zakonov, ki bi urejali zgolj internet in kibernetsko kriminaliteto. Eden izmed razlogov za to je dejstvo, da je na internetu težko določiti meje in da je mogoče prikriti identiteto posameznika. Institucije EU se tega problema zavedajo in si prizadevajo za uzakonjenje tega prodročja, zato bom raziskal tudi delovanje evropskih agencij na področju informacijske varnosti in opredelil delo ter naloge evropskega supervizorja za varnost osebnih podatkov.

1.4.1 Zakon o varstvu osebnih podatkov – ZVOP-1

Zakon o varstvu osebnih podatkov (Ur. l. RS, št. 86/04, v nadaljevanju ZVOP-1) je temeljni zakon na področju osebnih podatkov,. S tem zakonoske določajo pravice, obveznosti, načela in ukrepi, ki preprečujejoneupravičene posege v dostojanstvo in zasebnost posameznika pri obdelavi njegovih osebnih podatkov. ZVOP-1 ureja splošno uporabo vseh vrst osebnih podatkov in ni osredotočen zgolj na spletno uporabo, z izjemo zakona o elektronskih komunikacijah, ki predstavlja napredek na področju regulacije kibernetske kriminalitete. Mnoge države namreč že razlikujejo med zakoni, ki urejajo spletno kriminaliteto, in med splošnimi zakoni. Problem takšnih zakonov je, da so zelo kompleksni, saj je težko prenesti nacionalne zakone na splet, kjer praktično ni nikakršnih meja.

Neuradno prečiščeno besedilo Zakona o varstvu osebnih podatkov obsega:

- Zakon o varstvu osebnih podatkov – ZVOP-1 (Ur. l. RS, št. 86/04, z dne 5. 8. 2004),
- Zakon o Informacijskem pooblaščencu – ZInfP (Ur. l. RS, št. 113/05, z dne 16. 12. 2005),
- Zakon o spremembah in dopolnitvah Zakona o ustavnem sodišču – ZUstS-A (Ur. l. RS, št. 51/07, z dne 8. 6. 2007),
- Zakon o spremembah in dopolnitvah Zakona o varstvu osebnih podatkov – ZVOP-1A (Ur. l. RS, št. 67/07, z dne 27. 7. 2007),
- Zakon o varstvu osebnih podatkov – uradno prečiščeno besedilo – ZVOP-1-UPB1 (Ur. l. RS, št. 94/07, z dne 16. 10. 2007).

Zakonsko stanje v Sloveniji je na področju osebnih podatkov na internetu pomanjkljivo. Posledično organi pregona, na katere so naslovljene kršitve in pritožbe, nimajo dovolj pooblastil za ukrepanje. Države bi morale stremeti k temu, da oblikujejo posebne organe pregona, ki bi bili specializirani za kibernetsko kriminaliteto, in bi svoje resurse posvečali zgolj preprečevanju kršenja zakonov na internetu.

1.4.2 GDPR – Splošna uredba Evropske Unije o varstvu osebnih podatkov

GDPR (angl. General Data Protection Regulation) je splošna uredba Evropske Unije o varstvu osebnih podatkov. V veljavo je stopila s 25.majem 2018 in predstavlja velik korak naprej pri zagotavljanju pravilne obdelave in uporabe podatkov. Namenjena je tako organizacijam znotraj EU, kot tudi organizacijam zunaj EU, katerih storitve koristijo prebivalci EU (GDPR Portal, 2018). Glavni novosti pri tej novi regulativi sta pridobivanje osebne privolitve za obdelavo osebnih podatkov in imenovanje pooblaščenca, zadolženega za varstvo osebnih podatkov (angl. Data Protection Officer – DPO). Za podjetja predstavlja nova regulativa velik izziv, saj od njih zahteva, da spremenijo način zbiranja podatkov. Pred uvedbo GDPR-ja je Evropska Komisija izdala brošure, katerih namen je bil izobraziti podjetja o novostih in jih pripraviti na spremembe še pred uvedbo regulative. Predpriprava je pri tako obširnih zakonih ključna, saj se podjetja izognejo visokim kaznim, ki sledijo, če se ne odzovejo pravočasno na zakonske zahteve.

Glavne novosti GDPR-ja:

- Soglasje za uporabo in upravljanje osebnih podatkov je obvezno, zapisano mora biti jasno in razumljivo.
- Uporabniki imajo pravico biti »pozabljeni«, njihovi podatki se morajo izbrisati iz baz njegovega upravljalca.
- Uporabniki lahko zahtevajo kopijo njihovih osebnih podatkov v prenosljivem formatu.
- Uporabniki imajo pravico izvedeti katere podatke podjetje zbira in kako jih uporablja/obdeluje.
- Za obdelavo podatkov osebe, mlajše od 16 let, je obvezno soglasje njihovih staršev.

GDPR občutno izboljšuje položaj posameznikov in spoštovanje njihove pravice do zasebnosti. Prav tako na drugi strani omogoča državnim organom ukrepanje na področju

upravljanja in deljenja osebnih podatkov, ki so prej bila slabo zakonsko opredeljena. GDPR opredeljuje tudi delovanje podjetij izven EU, ki ponujajo storitve evropskim državljanom, zato lahko trdimo da gre za zakon, ki se nanaša na celoten svet.

Zagrožene kazni ob neupoštevanju so zelo visoke. Podjetjem bodo ob kršitvi izdane kazni v višini do 4 % letnega dohodka oziroma 20 mio €, katerakoli številka bo večja. Naj poudarim, da govorimo o procentih dohodka, ne dobička. Poleg tega so posamezniki, ki so bili žrtve kršitev, upravičeni do odškodnine za nastalo škodo. Podjetja ob kazni in odškodnini izgubijo še ugled in zaupanje njihovih uporabnikov.

GDPR in kriptografija. V Uvodni izjavi številka 83 je zapisano: »Da bi ohranili varnost in preprečili kršitve vpeljave te Regulative, mora kontrolor oziroma upravljalec zbirk podatkov oceniti tveganja, povezana z obdelavo, in implementirati ukrepe, ki bodo ta tveganja zmanjšala, kot na primer enkripcija.« (I-SCOOP, 2018).

Čeprav enkripcija v veliki meri pogojuje zadovoljivo varnost naših podatkov, je v celotnem besedilu GDPR-ja, ki obsega 261 strani, omenjena zgolj štirikrat. Poleg tega pa nikjer ne piše, da je enkripcija predpisana z zakonom ali obvezna. Gre zgolj za priporočila in primere dobre prakse, zato bi lahko rekli, da je enkripcija posredno pogojena z zakonom, saj so zakonske zahteve glede zaščite podatkov takšne, da jih brez uporabe ustreznih šifer ni mogoče učinkovito zavarovati.

1.4.3 Drugi zakoni, ki se nanašajo na področje upravljanja in varstva podatkov

Zakon o elektronskih komunikacijah (ZEKom-1). Ta zakon opredeljuje pogoje za zagotovitev delovanja elektronskih omrežij in izvajanja telekomunikacijskih storitev. Pokriva področje zagotavljanja konkurence, določa pravice uporabnikov, ureja področje varnosti omrežij, prav tako pa tudi ureja področje zagotavljanja njihovega delovanja v izrednih stanjih. Na področju varnosti osebnih podatkov uzakonja pravico do zasebnosti in rešuje druga vprašanja, povezana z elektronskimi komunikacijami. Njegov namen je omogočiti hitrejši razvoj elektronskih komunikacijskih sistemov in z njimi povezanih storitev ob ustrezni ravni varnosti in spoštovanja posameznikovih pravic.

Zakon o dostopu do informacij javnega značaja (ZDIJZ). Opredeljuje postopke pridobivanja in uporabe informacij javnega značaja, s katerimi razpolagajo državni organi, lokalne skupnosti, javne agencije, skladi in druge osebe javnega prava, ki vključujejo tudi nosilce javnih pooblastil in javne službe). Namen ZDIJZ-ja je zagotavljanje transparentnosti delovanja javnih organov in omogočanje spoštovanja pravic pravnih in fizičnih oseb do pridobitve informacij javnega značaja.

Zakon o inšpekcijskem nadzoru (ZIN). ZIN ureja zadolžitve, pristojnosti, položaj, pravice in dolžnosti inšpektorjev. Vključuje postopke inšpekcijskega nadzora, inšpekcijske ukrepe in druga področja, povezana z delovanjem in nadzorov inšpektorjev.

2. člen ZIN: »Inšpekcijski nadzor je nadzor nad izvajanjem oziroma spoštovanjem zakonov in drugih predpisov. Inšpekcijski nadzor izvršujejo inšpektorice oziroma inšpektorji (v nadaljnjem besedilu: inšpektorji) kot uradne osebe s posebnimi pooblastili in odgovornostmi.«

Na področju varstva osebnih podatkov predstavlja zakonsko podlago za uporabo le-teh v različnih situacijah, kot na primer uporaba podatkov ob inšpekcijskem nadzoru, izdaja globe ob neupoštevanju posredovanja osebnih podatkov pravnih oseb in upravljanje osebnih podatkov prijavljenih kandidatov za strokovni izpit za inšpektorja.

Zakon o tajnih podatkih (ZTP-UPB2). Zakon o tajnih podatkih določa osnove enotnega sistema odločanja o varovanju in dostopu do tajnih podatkov državnih organov Republike Slovenije. Zakon velja tako za pravne kot tudi za fizične osebe in poleg ostalega opredeljuje tudi odgovornosti in dolžnosti nosilcev tajnih podatkov. V njegovem 3. členu je določeno, katere osebe imajo v okviru svojih funkcij pravico do dostopa do tajnih podatkov po pridobitvi ustreznega dovoljenja. Edina oseba, ki za dostop ne potrebuje dovoljenje je Komisija Državnega zbora Republike Slovenije za nadzor nad delom varnostnih in obveščevalnih služb.

Zakon o medijih (ZMed). ZMed je obširen zakon, ki določa dolžnosti in pravice časopisov, revij, radijskih in televizijskih programov, elektronskih publikacij ter drugih oblik dnevnega ali periodičnega objavljanja uredniško oblikovanih vsebin, ki so dostopne javnosti. Z vidika zasebnosti sta pomembna naslednja odstavka:

- 6. člen: Svoboda izražanja – ureja področje svobode izražanja, prostega pretoka informacij in odprtosti medijev za različna mnenja in vsebine.
- 45. člen: Dostop do informacij za medije – določa osnovne postopke pridobitve informacij, ki so lahko uporabljene v obveščevalne namene.

1.4.4 Opredelitev stanja in pomanjkljivosti zakonov na področju varnosti osebnih podatkov

Zakoni, ki se nanašajo na varnost podatkov v Sloveniji, so z izjemo ZVOP-1 dokaj pomanjkljivi. Le-ti so zastareli in ne vključujejo večine področji, kjer se odvijajo nove vrste kriminalnih dejanj. Napisani so bili namreč v času preden se je večina podatkov prenašala preko elektronskih medijev. Razlogov za takšno stanje zakonov je več, eden glavnih pa je zagotovo hitra rast tehnologije in interneta. Internet je, kot bomo kasneje spoznali tudi v intervjujih z različnimi institucijami, težko urediti z zakoni. Na njem namreč ni nikakršnih geografskih meja, zato sta nadzor nad njim in uveljavljanje zakonodaje, ki ga ureja, otežena.

Slovenija bi lahko postala evropski primer dobre prakse učinkovite internetne zakonodaje. Uvesti bi morala zakon, ki bi urejal zgolj varnost osebnih podatkov na internetu, ne pa splošne varnosti osebnih podatkov. Skupaj z zaintersirano javnostjo in stroko bi zakonodajno

telo moralo oblikovati nov zakon, ki bi uredil omenjeno področje, zvišal raven varnosti podatkov in poskrbel za razlikovanje med dobronamernim in zlonamernim deljenjem le-teh. Jedro zakona bi morala biti učinkovita opredelitev nelegalnega posredovanja podatkov posameznikov in kazni za njegove kršitelje. Zakon bi lahko opredeljeval tudi zakonske zahteve glede zasnove in delovanja informacijskih infrastruktur za podjetja, ki upravljajo z bazami podatkov, in preventivnih ukrepov za zaščito pred potencialnimi vdori tretjih oseb.

Potrebna bi bila ustanovitev Slovenske agencije za informacijsko varnost, ki bi imela dovolj pristojnosti za avtonomno delovanje in uveljavljanje omenjenega zakona. Ta agencija bi z izdajanjem brošur in informiranjem prebivalstva o pomembnosti te problematike pripomogla k zvišanju ravni zaščite pred potencialnimi vdori in zlorabo podatkov. Lahko bi uvedla tudi sistem anonimnih prijav krištev, kjer bi posamezniki lahko prijavili kršitve brez izdaje svoje identitete.

Potreben bo konsenz znotraj Evropske Unije o učinkoviti vpeljavi univerzalnega zakona, ki ne bi omejeval svobode govora, hkrati pa bi preprečeval kriminalnim organizacijam tajno komunikacijo in deljenje informacij.

1.5 Pristojni organi, zadolženi za izvajanje zakonodaje na področju varstva osebnih podatkov, v Republiki Sloveniji

V tem delu bom preučil vladne službe, ki izvajajo zakonodajo, povezano z varstvom osebnih podatkov, rešujejo probleme in pritožbe posameznikov in skladno z zakoni odločajo o kršitvah, povezanih s krajo in neupravičeni uporabi osebnih podatkov. V analizo bodo vključeni različni državni organi, ki so pooblaščeni za reševanje problemov na omenjenem področju.

1.5.1 Informacijski pooblaščenec

Informacijski pooblaščenec (v nadaljevanju IP) je 31. 12. 2005 ustanovljen samostojen in neodvisen državni organ, zadolžen za varstvo osebnih podatkov in pravilno uporabo le-teh. Skrbi za to, da ne prihaja do kršitev zakonov, oziroma rešuje probleme glede kršitev zakonov, ki urejajo uporabo osebnih podatkov. Trenutni vodja tega organa je Mojca Prelesnik.

IP pomaga pri presoji o ukrepanju, kadar nekdo neupravičeno poseže v naše osebne podatke, kadar nam upravljalec zbirke podatkov ne dovoli seznanitve z našimi podatki in kadar kot upravljalec takšne zbirke potrebujemo odločbo IP-ja za obdelavo osebnih podatkov (biometrija, prenos v tretje države…). Njegove pristojnosti so naslednje:

- Odločanje o pritožbah glede odločb, s katerimi je organ neupravičeno zavrnil zahtevo po dostopu do informacij javnega značaja.
- Nadzor nad izvajanjem vseh zakonov, ki urejajo varstvo in obdelavo osebnih podatkov.

- Odločanje o pritožbah posameznikov, kadar upravljalec osebnih podatkov ne ugodi zahtevi posameznika po vpogledu v podatke, izpisu le-teh, seznanitvi o njih, ipd.
- Kot prekrškovni organ je pristojen za nadzor nad izvajanjem ZinfP-ja, ZDIJZ-ja (zakon o dostopu do informacij javnega značaja) v okviru pritožbenega postopka in ZVOP-ja.

IP tudi deluje na področju mednarodnih projektov, med katerimi sta najpomembnejša:

- ARCADES (Introducing d**A**ta p**R**ote**C**tion **A**n**D** privacy issu**E**s at school**S** in the EU) in
- CRISP (Evaluation and **C**e**R**tificat**I**on Schemes for **S**ecurity **P**roducts).

ARCADES je projekt, katerega cilj je dvigniti raven zaščite osebnih podatkov in raven zasebnosti v vseh šolah Evropske Unije. Za dosego tega cilja želijo v evropskih šolah izvesti dvodnevne seminarje, vezane na omenjen cilj projekta in potrebi po zvišanju ravni osveščenosti o problematiki zaščite posameznikovih podatkov. Ob zaključku seminarjev želijo predstaviti rezultate raziskav in smernice za prihodnost (Arcades project, 2017).

Poslanstvo projekta ARCADES:

- Povišati raven zavedanja o pomembnosti zaščite osebnih podatkov in uveljavljanja pravic posameznikov.
- Povečati dostopnost gradiva o problematiki zasebnosti v šolah.
- Izdajati brošuro o rezultatih njihovega dela in smernicah za prihodnost.
- Uvesti željen oziroma optimalen model dobre prakse.
- Ne zgolj izboljšati sodelovanje med institucijami, vključenimi v ta projekt, ampak tudi povezati snovalce DPA-jev (angl. Data Protection Act – Akt o zaščiti podatkov), katerim bi ta projekt lahko koristil (Arcades project, 2017).

CRISP je triletni projekt Evropske Unije iz sedme finančne perspektive, katerega cilj je vpeljava harmoniziranih standardov na področju evropske industrije varstva podatkov. Deluje na področju ovrednotenja in certificiranja metod, ki jih podjetja na tem področju uporabljajo. Razviti želijo t.i. »CRISP shemo«, ki bi pripomogla k povišanju ravni zaupanja prebivalcev v tehnologije varstva podatkov, hkrati pa bi na učinkovit način pripomogla narediti trg varnostnih produktov bolj konkurenčen in enoten (Crisp project, 2017).

Njihove metode, uporabljane v fazi vrednotenja varnostnih produktov, uporabljajo S-T-E-Fi model štirih dimenzij:

- Security – Varnost produktov in odpornost proti grožnjam in napadom.
- Trust – Zanesljivost produktov in dojemanje uporabnikov sistemov, tako končnih uporabnikov kot tudi ostalih zaposlenih.
- Efficiency – Učinkovitost in ekonomičnost produktov (stroški življenjskega cikla produkta, implementacijski stroški, operativni stroški, ipd.).
- Freedom infringement – Vpliv na raven omejenosti svobode in pravic uporabnikov produktov.

Rezultati projekta bodo znani ob njihovem končnem poročilu, dolgoročni rezultati pa se bodo pokazali šele čez čas. Projekt predstavlja korak naprej pri zagotovitvi kakovostnih in učinkovitih varnostnih sistemov in na področju varstva podatkov. Pripomogel bo k višji ravni zaščite temeljnih človekovih pravic in skladnosti produktov z zakoni EU, predvsem z zakonom »General Data Protection Law« – GDPR 679/2016 (Crisp project, 2017).

Pisni intervju z namestnikom IP-ja, mag. Andrejem Tomšičem. Zanimalo me je, kako procesi in odločbe IP-ja potekajo v praksi, zato sem 23. 3. 2017 naslovil nekaj vprašanj na urad IP-ja. Odgovore sem prejel že naslednji dan, za kar se zahvaljujem namestniku IP-ja mag. Andreju Tomšiču.

Namestnik IP je mnenja, da ima njihova služba zadostno zakonsko podlago za opravljanje svojih nalog in pristojnosti, da pa težave nastanejo, kadar gre za upravljalca podatkovne zbirke, katera ima strežnike in podjetje v tujini. Tam IP nima nikakršnih pristojnosti za ukrepanje.

Prihodnji izzivi so opisani v letnem poročilu IP-ja, v zadnji točki tretjega dela (stran 65), kjer so strnjene naslednje ugotovitve:

- IP ugotavlja, da gre večino kršitev pripisati nepoznavanju ali nerazumevanju zakonodaje, v manjši meri pa tudi malomarnosti in namernemu kršenju. Slednje se dogaja predvsem v zasebnem sektorju zaradi ekonomskih interesov kršitelja.
- Težavo predstavljajo tudi zavezanci, ki opravljajo dejavnosti v fiktivnih poslovnih prostorih, kot odgovorne osebe pa so mnogokrat postavljene osebe, ki niso državljani Republike Slovenije.
- IP pozdravlja novelo Zakona o prekrških (ZP-1), vendar opozarja, da je na področju varstva osebnih podatkov v praksi problematično izrekanje glob in nesorazmerne višine kazni pri velikih podjetjih in samostojnih podjetnikih.
- IP sicer meni, da se je raven obveščenosti javnosti glede varstva osebnih podatkov tudi po njegovi zaslugi bistveno povišala, da pa hiter razvoj tehnologije vodi do napačnega razumevanja pravic do zasebnosti in varstva osebnih podatkov.
- IP opozarja na napačno razumevanje ljudi, ki smo ga izpostavili v uvodu: »Zakaj bi nas skrbelo varstvo osebnih podatkov, če nismo storili nič napačnega?«. IP varnost in zasebnost jemlje zelo resno in vprašanja na temu področju skuša reševati objektivno in enakopravno.
- IP je v letu 2015 izdal 5 smernic, od katerih velja omeniti smernice o zavarovanju osebnih podatkov (predlaga priporočljive standarde in procese zavarovanja) in smernice o pogodbeni obdelavi osebnih podatkov (pojasnjuje procese znotraj pogodbenih obdelav podjetij, ki nudijo tovrstne storitve).

IP izdaja brošure, opredeljuje smernice in informira prebivalstvo o pomembnosti zaščite osebnih podatkov na internetu. O tem problemu si prizadeva osvestiti posameznike že v mladih letih, ker se danes otroci z elektroniko in deljenjem svojih podatkov srečajo že zelo

zgodaj. IP je izdal brošuro z naslovom: »Samo ti odločaš – Komu lahko zaupam osebne podatke in kdaj?« Ta brošura vsebuje navodila, kako se učinkovito zaščititi pred krajo podatkov in se izogniti nepremišljenemu deljenju podatkov. Zelo nazorno nam pokaže, kaj vse se lahko zgodi, če se na internetu znajdejo naše osebne slike, posnetki ali drugi občutljivi podatki, ki lahko zelo hitro spremenijo naše življenje in javno podobo.

Na IP-jevi spletni strani ima samo varstvo osebnih podatkov na internetu svojo sekcijo, ki obsega več kot 10 strani. Vsebuje priporočila za varno uporabo interneta in opisuje pasti, načine napadov in mehanizme prijave kriminalnih dejanj. »Spletno-oko.si« je slovenska spletna prijavna točka, kjer lahko anonimno prijavimo sovražni govor in otroško pornografijo. Kot člana svetovalnega telesa pri tem projektu sodelujeta tudi Vrhovno državno tožilstvo Slovenije in Policija (Informacijski pooblaščenec Republike Slovenije, 2017).

Projekt »Safe.si« je portal namenjen osveščanju o varni rabi interneta in mobilnih naprav za otroke, najstnike, starše in učitelje. V projektu sodelujeta tako IP, kot tudi Varuh RS, in je podprt s strani mnogih institucij Republike Slovenije ter sofinanciran s strani Evropske Unije. Na portalu lahko najdemo nasvete o zaščiti podatkov na internetu, varni uporabi informacijske tehnologije, primernem obnašanju na spletu in o drugih dejavnikih, ki se navezujejo na uporabo interneta.

1.5.2 Varuh človekovih pravic

S sklepom, sprejetim dne 26.6.2001, je varuh človekovih pravic pridobil pristojnosti **neodvisne institucije za varnost osebnih podatkov** z naslednjimi nalogami (Varuh človekovih pravic Republike Slovenije, 2017):

- Neposreden nadzor spoštovanja predpisov o varstvu osebnih podatkov, tako pri upravljalcih baz, kot tudi pri uporabnikih.
- Spremljanje in nadziranje dela Inšpektorata za varstvo osebnih podatkov.
- Svetovanje na področju varstva osebnih podatkov.
- Sodelovanje v oblikovanju in sprejemanju predpisov.
- Opravljanje drugih zakonsko predpisanih nalog.

Varuh človekovih pravic je te naloge opravljal do sprejetja novele Zakona o varstvu osebnih podatkov dne 15.07.2004, z začetkom veljavnosti 01.01.2005 (Ur. l. RS, št. 94/07), ki je večino nalog varovanja osebnih podatkov prenesel na Informacijskega pooblaščenca. Ob tem pa je varuh ohranil pristojnosti, zapisane v Zakonu o varuhu človekovih pravic, vendar v veliko manjši meri kot prej. Še vedno je dolžan poročati državnem zboru o dogajanju, ugotovitvah, priporočilih in predlogih na področju varovanja osebnih podatkov.

Pisni intervju s predstavnico Varuha človekovih pravic RS, gospo Natašo Kuzmič.

Ugotovitve intervjuja so naslednje:

- Varuh RS je mnenja, da ima za svoje opravljanje nalog zadostna pooblastila.
- O problematiki varstva oseb pred posegi v osebnostne pravice, storjenimi preko interneta, je Varuh RS v letnem poročilu za leto 2014 ocenil, da veljavna ureditev ne omogoča učinkovitega pravnega varstva žrtev zlorab in da bi bilo potrebno sprejeti ukrepe, ki bi jim zagotovili pravno varstvo.
- Število prijav na področju kršitev varstva osebnih podatkov je vsako leto na približno enaki ravni. Ta številka znaša približno 60 primerov letno. Bolj kot številka pa je pomemben opis posameznih primerov, s katerim se Varuh RS trudi bralcem ustvariti sliko o problemih in jih tako tudi čimbolj nazorno prikazati.
- Med Varuhom in IP-jem ni nikakršnih konfliktov, ker to področje ureja tudi veljavna zakonodaja. Skladno z njo velja načelo subsidiarnosti Varuhovega posredovanja, kar pomeni, da Varuh posreduje šele, če pristojni organi (IP ali sodstvo) pri svojem delu zagrešijo nepravilnosti, zaradi katerih lahko Varuh RS na podlagi zakonskih določb izvede zahtevane postopke.
- Največji izzivi na področju varovanja osebnih podatkov na internetu so reševanje problemov s področja kraje identitete, lažnega predstavljanja ali zvabljanja, trgovanja z osebnimi podatki, nadzora nad hrambo osebnih podatkov, ipd. Varuh RS opozarja tudi na pomembnost sprejemanja ustrezne pravne regulacije v zvezi s čedalje bolj zmogljivimi algoritmi, ki služijo obdelavi osebnih podatkov, in tudi njeno učinkovito izvrševanje.

1.6 Pristojni organi, zadolženi za izvajanje zakonodaje na področju varstva osebnih podatkov, v Evropski Uniji

Raziskati sem želel tudi evropske institucije, ki se ukvarjajo s problematiko varnosti osebnih podatkov na spletu, za kar sta zadolžena predvsem EDPS in ENISA. Na njiju sem pisno naslovil vprašanja, ki so zajemala njihov pogled na trenutno stanje, prihodnje izzive in mnenja o sodelovanju med različnimi organi znotraj EU. Raziskal sem tudi kako se Slovenija pozicionira glede na EU in naredil primerjalno analizo.

1.6.1 EDPS – Evropski nadzornik za varstvo podatkov

Evropski nadzornik za varstvo podatkov (v nadaljevanju EDPS) je neodvisen nadzorni organ na ravni EU, katerega naloge so sledeče (European Data Protection Supervisor, 2017):

- Nadzor obdelovanja osebnih podatkov institucij in organov Evropske unije.
- Svetovanje pri ustvarjanju politik in zakonodaje na področju zasebnosti.
- Sodelovanje z drugimi organi na tem področju z namenom zagotavljanja usklajenega varstva podatkov.

EDPS vodi decembra 2014 imenovan glavni nadzornik Giovanni Buttarelli s pomočnikom Wojciechom Wieworowskim (European Data Protection Supervisor, 2017). Gre za relativno nov organ, ustanovljen 14. januarja 2004, ki pa zaradi stanja na področju varstva osebnih podatkov pridobiva vedno večji vpliv, saj neposredno vpliva na raven zasebnosti evropskih državljanov. EDPS nadzira Evropska Komisija. Nadzornik EDPS-a zaposluje skupino strokovnjakov s kompetencami na različnih področjih. Sestavljajo jo izkušeni pravniki, strokovnjaki na področju informacijske tehnologije in administratorji, s skupnim ciljem krepitve standardov EU in povečanja ravni varnosti in zasebnosti osebnih podatkov v praksi in zakonodaji. Zakonska podlaga njegovega delovanja je Direktiva o varstvu osebnih podatkov.

Pisni intervju s predstavnikom EDPS-ja, gospodom Courtenay Mitchellom.

Vprašanja, ki sem jih naslovil na EDPS, so bila sestavljena iz dveh delov. Prvi del vprašanj se je nanašal na zakonodajo in nov zakon, imenovan GDPR (angl. General Data Protection Regulative), v drugem delu me je zanimal tehnološki pogled, enkripcija in z njo povezani izzivi.

Ugotovitve iz intervjuja so naslednje:

- Več kot dve tretjini primerov, ki jih EDPS obravnava, se nanašajo na varnost podatkov na internetu, tako na operativni kot tudi na zakonski ravni. EDPS ima oddelek zaposlenih, katerega sestavljajo tehnološki in varnostni strokovnjaki, specializirana agencija, zadolžena za informacijsko varnost, pa se imenuje ENISA, katera bo predstavljena v naslednji točki.
- Evropska zakonodaja je po mnenju g. Mitchella trenutno pred veliko spremembo, saj 25. Maja 2018 v veljavo stopi zgoraj omenjen zakon GDPR, ki vključuje smernice za varovanje osebnih podatkov in obveznost poročanja o tovrstnih varnostnih incidentih. Zmanjševal naj bi tudi obseg birokracije, s katero se podjetja soočajo, in posledično višal stroškovno učinkovitost. EDPS ga pozdravlja, vendar opozarja na pomanjkanje smernic za praktično vpeljavo sprememb. Prav tako je zainteresiranost podjetij za implementacijo primernih varnostnih ukrepov na področju varnosti podatkov na prenizkem nivoju.
- Nekatera podjetja vpeljavo tega zakona jemljejo bolj resno in se zavedajo, da pravočasna priprava na zahtevane spremembe znižuje stroške in niža raven strahu organizacije pred morebitnimi sankcijami ob neupoštevanju zakona in škodo zaradi neprimerne uporabe osebnih podatkov.

1.6.2 ENISA – Agencija Evropske Unije za omrežno in informacijsko varnost

ENISA prestavlja center znanja o kirbernetski varnosti v Evropi. Sedež ima na Heraklionu, Kreta, in operativno pisarno v Atenah. Ustanovljena je bila leta 2004, njena naloga pa je aktivna vključenost v višjo raven informacijske varnosti znotraj Unije in na višjo raven

osveščenosti državljanov o pomembnosti le-te. Poleg ENISE se je znotraj Europola nekaj let nazaj oblikoval tudi Center kompetenc kibernetske kriminalitete, ki se ukvarja s podobno problematiko.

Agencija sodeluje z državami članicami in privatnim sektorjem in jim zagotavlja predloge ter rešitve, kot so:

- Vključenost v pan-evropske vaje kibernetske varnosti.
- Razvoj nacionalnih strategij kibernetske varnosti Unije.
- Izvajanje študij za varno prevzetje rešitev v oblaku.
- Opozarjanje na probleme varnosti osebnih podatkov.
- Identifikacija tveganih področij glede kibernetskih napadov.

V izdani publikaciji, imenovani »ENISA Strategy 2016–2020«, opredeljujejo svoje poslanstvo, strategije višje ravni informacijske varnosti znotraj EU in področja izboljšav.

S pomočjo privatnega sektorja in regulatorjev v državah članicah so oblikovali naslednjih 5 strateških ciljev (European Union Agency for Network and Information Security, 2018):

1. Strokovno znanje – agencija bo poskrbela za zbiranje, analizo in razpoložljivost informacij o glavnih problemih NIS-a (angl. National Intelligence Strategy), ki vplivajo na spremembe v digitalnem okolju EU.
2. Politika – svetovanje in asistiranje evropskim institucijam in državam članicam v zvezi z razvojem in implementacijo politik, smernic in zakonov na vseh področjih, povezanih z NIS.
3. Zmogljivosti – pomoč državam članicam pri izboljšavi in povečanju kapacitet informacijskih sistemov. ENISA bo s pomočjo priporočil pomagala članicam pri oblikovanju strategij, privatnemu sektorju bo svetovala pri implementaciji kibernetske varnosti v njihove poslovne načrte, institucijam EU pa bo pomagala s koordinacijo in podporo zakonov.
4. Skupnost – izboljšanje sodelovanja med državami članicami na evropskem nivoju predvsem glede vprašanj, ki se nanašajo na CSIRT (angl. Computer Security Incident Response Team), organizacijo, ki skrbi za analizo kibernetskih napadov in se nanjo ustrezno odzove.
5. Omogočanje – povečanje vpliva agencije, izboljšanje njenega managementa in izboljšanje učinkovitosti sodelovanja z državami članicami in institucijami EU.

1.7 Primerjava stanja glede varnosti osebnih podatkov med Slovenijo in Evropsko Unijo

Slovenija je, kar smo spoznali že na samem začetku, glede informacijske varnosti nad evropskim povprečjem, saj se po ravni varnosti podatkov uvrščamo pred mnoge bolj razvite države. Kljub temu pa bo potrebno še veliko sprememb. Spodnja tabela nam prikazuje, kako se Slovenija pozicionira glede na različne dejavnike informacijske varnosti znotraj EU.

Tabela 3: Primerjava med dejavniki informacijske varnosti v Sloveniji in EU

	Evropska unija (EU-28)	**Slovenija**
Raven razvitosti informacijske infrastrukture	Zahodnoevropske države nadpovprečno, vzhodnoevropske pa podpovprečno.	Slovenija ima nadpovprečno razvito informacijsko infrastrukturo.
Strateški cilji	EU ima probleme pri usklajevanju skupne politike informacijske varnosti	Slovenija nima strategij, ki bi se nanašale izključno na ta problem
Razpoložljivi viri agencij, ki se ukvarjajo s področjem informacijske varnosti v letu 2017	ENISA – 11,3 mio € - nizek proračun glede na rast in velikost panoge, katero agencija pokriva	IP RS – 1.5 mio € - IP ima poleg obravnavanega področja pristojnosti še na mnogih drugih
Delež prebivalstva, starega med 16–74 let, ki obvlada veščine za varno uporabo interneta	31% - tretjina Evropejcev ima t.i. e-veščine, ki neposredno vplivajo na višjo raven varnosti osebnih podatkov	30 % - Slovenija se uvršča blizu povprečja, potrebno bi bilo več izobraževanja prebivalstva o varni uporabi interneta
Delež ljudi, ki niso delili osebnih podatkov preko interneta v letu 2016 (% prebivalstva, ki ni uporabljal interneta v zadnjem letu	27 % posameznikov	37 % posameznikov

Vir: Eurostat (2016), Surs (2017).

Dejavniki ravni informacijske varnosti so stvar subjektivne presoje. V analizo sem zajel tiste, ki imajo po mojem mnenju največji vpliv in za katere obstajajo uradne statistike, ki to potrjujejo. Kot lahko vidimo na primerih, se Slovenija glede na EU, uvršča okoli povprečja oziroma je v določenih delih nadpovprečna. To gre deloma pripisati tudi njeni ugodni legi in koncentraciji prebivalstva.

Še vedno pa bo potrebno veliko napora za preboj na vrh evropskih držav in za učinkovito vpeljavo boljših varnostnih sistemov. Procent prebivalstva, ki uporablja internet se sicer povečuje, vendar je zavedanje in znanje posameznikov o potrebi po informacijski zaščiti še vedno na prenizkem nivoju. Pri tem je potrebno poudariti, da morajo posamezniki stremeti k individualni motivaciji in proaktivnosti za preprečitev zlorab njihovih podatkov, k čemer pa lahko pripomorejo državne institucije s primernim obveščanjem in izobraževanjem populacije o načinih zaščite.

Velik preboj na tem področju so naredili nekateri zaposleni v ameriških vojaških in obveščevalnih službah, ki so močno spremenili javno percepcijo o metodah delovanja tajnih agencij. V naslednjem poglavju bom raziskal njihova razkritja in kakšne posledice so imela za državne službe in širše prebivalstvo.

1.8 Dogodki, ki so zaznamovali področje varnosti osebnih podatkov in opozorili na ranljivost njihovih lastnikov

V tem delu bom raziskal nekaj ključnih dogodkov na obravnavanem področju, ki so postavili legitimnost nekaterih državnih ustanov in tajnih služb pod vprašaj. Primeri nazorno prikazujejo tanko mejo med zasebnostjo posameznikov in masovnim nadzorom s strani državnih institucij in tajnih služb. Vključil bom tudi dejanske primere neetičnih praks, posledice ogrožanja državne varnosti in preučil, kako so razkritja nadzora prebivalstva vplivala na tajne službe in njihovo delovanje.

1.8.1 Žvižgaštvo in njegov vpliv na osveščenost ljudi o problematiki masovnega nadzora prebivalstva

Ljudi, ki razkrivajo državne skrivnosti in prakse s strokovnim izrazom imenujemo žvižgači (angl. Whistleblower). Žvižgaštvo v najbolj osnovni obliki ponazarja poročanje neetičnih ravnanj državnih organov širši javnosti (Dungan, Waytz & Young, 2015).

Živžgače širša javnost obravnava z dveh splošnih vidikov:

- **Vidik heroja -** Ljudje, ki pripadajo temu polu, se zavzemajo za spoštovanje človekove zasebnosti in varnosti svojih osebnih podatkov. Žvižgače vidijo kot heroje, ki so s svojim žrtvovanjem prispevali k večjemu zavedanju o obsegu poseganja v zasebnost javnosti in ogroženosti varnosti njihovih podatkov.
- **Vidik Izdajalca** - Drugi tip pogleda pa pripada polu, ki meni da so žvižgači državni izdajalci, ki s svojimi razkritji škodujejo državni varnosti. Razkritja dojemajo kot posredovanje tajnih praks in skrivnosti sovražnikom in terorističnim skupinam, zato jih mnogi označujejo tudi za vohune.

V članku Psihologija žvižgaštva (angl. The psychology of whistleblowing) avtorji ugotavljajo, da so dejanja žvižgačev največkrat »trade-off« izbira med dvema temeljnima vrednotama – poštenostjo in zvestobo. Ta ugotovitev bazira na teoriji moralnih vrednot, ki navaja 5 osnovnih moralnih vrednot: škodovanje, poštenost, zvestoba, avtoriteta in nedolžnost (Dungan, Waytz, & Young, 2015). Študija se nadaljuje z ugotavljanjem faktorjev, ki vplivajo na tovrstna dejanja. Te dejavnike je po mnenju avtorjev mogoče razdeliti v naslednje tri skupine:

- Osebni faktorji – Demografski faktorji, povezani s predispozicijami zvižgačev, so povezani z višjo plačo na delovnem mestu, večjim dostopom in pooblastili, višjo stopnjo izobrazbe in moškim spolom. Ljudje z večjim občutkom odgovornosti so bolj nagnjeni k razkritjem iz dobronamernih razlogov. Ekstrovertirani ljudje in ljudje z proaktivnimi osebnostmi so manj podvrženi situacijskim vplivom, a imajo enaka nagnjenja. Zaključimo lahko, da so žvižgači ljudje z osebnostnimi lastnostmi, ki povzročajo, da so nagnjeni proti neskladjem.

- Situacijski faktorji – Velik vpliv na dejanja zaposlenega imajo organizacije, v katerih delujejo. Včasih prav te vplivajo na to, ali se bo oseba odločila razkriti neetična ravnanja, ali ne. V študiji na neki ameriški univerzi so ciljno skupino postavili pred dejansko neetično odločitev, od vseh vključenih pa se jih je zgolj 10% odločilo prijaviti takšno ravnanje. Čeprav se je večini ljudi zdela prijava kršitve edina prava stvar, so podlegli pritiskom avtoritete in vrednoti zvestobe skupini.
- Kulturni faktorji – Variabilnost kulturnih norm vpliva na verjetnost žvižgaštva. Azijske države, kot so Japonska, Kitajska ali Tajvan, so žvižgaštvu veliko manj naklonjene kot na primer ZDA. Ta naklonjenost je neposredno povezana z režimom v posamezni državi.

1.8.2 Primer Edward Snowdna

Verjetno najbolj znan žvižgač na svetu je trenutno Edward Snowden, ameriški računalničar in bivši uslužbenec ameriške tajne službe CIA (angl. Central Intelligence Agency) in NSA (angl. National Security Agency). Že pri starosti 27 let je pridobil dostop do najbolj zaupnih državnih dokumentov. Zaradi svojih prepričanj o svobodi posameznikov in njihovih pravicah je leta 2013 v javnost posredoval do sedaj najbolj obsežen paket tajnih dokumentov v zgodovini. Po razkritju so ga ZDA označile za državnega izdajalca in ga začele sodno preganjati. Azil je našel v Moskvi, kjer še danes prebiva na neznani lokaciji.

Njegovo razkritje je javnosti pokazalo tajne prakse nadzora ljudi in kontroverzne načine zbiranja zasebnih podatkov. Dokumenti prikazujejo, kako velike telekomunikacijske korporacije sodelujejo s tajnimi agencijami in jim posredujejo informacije o državljanih. Edward Snowden predstavlja velik mejnik na področju podatkov in zasebnosti, saj je njegovo razkritje razburilo širšo javnost, ki o tem ni vedela nič. Tajne službe so s pomočjo protiterorističnega akta, ki jim je dal veliko večja pooblastila kot pred njegovim sprejetjem, izkoriščale pristojnosti za zbiranje podatkov tudi takrat, ko ni bilo utemeljenega suma. Zakonska podlaga jim je v tem primeru omogočala, ne preprečevala, dostop do podatkov, zato se lahko utemeljeno vprašamo, kaj so s temi podatki počeli in komu vse so jih v tajnosti posredovali.

1.8.3 Primer Chelsea Elizabeth Manninga

Chelsea Elizabeth Manning (rojen Bradley Edward Manning) je bivša ameriška vojakinja, ki je razkrila tajne dokumente ameriške vojske in s tem resno ogrozila varnost ameriških obrambnih organov. Zaposlena je bila kot informacijski analitik in imela dostop do najbolj zaupnih podatkovnih baz, ki so vsebovale zaupne dokumente. Dokumenti so večinoma imeli oznako tajnosti in so bili razkriti preko strani Wikileaks. Po razkritju številnih praks nečloveškega mučenja, zasliševanja zapornikov in novačenja vladnih uslužbencev ameriške vojske, je bila Manningova obsojena na 35 let zaporne kazni z možnostjo pogojne izpustitve po 8 letih. Podlaga za njeno sodbo je bil Vohunski akt (angl. Espionage act), kateri sega še v dobo 2. svetovne vojne. Spoznana je bila za krivo na podlagi 22 kršitev, med katerimi je

bila najbolj resna kršitev pomoč sovražnikom. Kazen bi bila verjetno nižja, če ji ne bi sodili na vojaškem sodišču.

Njeni motivi za razkritje dokumentov so bili predstavljeni v članku revije Rolling Stone (Reitman, 2013), kjer je bil predstavljen njen pogled na dogajanja znotraj vojske. Razočarana nad protiterorističnimi akcijami je opisovala obsedenost ameriške vojske z ujetništvom in ubijanjem, njen osrednji cilj pa je bil ustvariti boljši svet in preprečiti nehumana dejanja. Bolelo jo je dejstvo, da v sodobnem razvitem svetu vodilna svetovna sila kot je ZDA za dosego določenih ciljev sklepa »pogodbe pod mizo« z tujimi diplomacijami in deluje na podoben način kot kriminalne združbe.

2 KRIPTOGRAFIJA PODATKOV

Kriptografija (gr. kryptós – skrit, gráphein – pisati) je veda o matematičnih tehnikah in algoritmih, ki jih lahko uporabljamo za zagotovitev informacijske varnosti. Le-ta vključuje tudi zaupnost in celovitost podatkov. Kriptografija obstaja skoraj od izuma pisave, zato jo uvrščamo med prastare vede. D'Agapeyeff jo opisuje kot vedo, ki je nastala zaradi potrebe po prikritju pomena napisane vsebine in za njen razvoj podaja naslednjo razlago:

»Potreba po pošiljanju sporočil na način, ki bo razumljiv zgolj izbranim posameznikom, se je pojavila že v zelo zgodnjih časih in od takrat naprej postala temelj za razvoj znanosti kriptografije.« (D'Agapeyeff, 1949)

Glavna naloga kriptografije je oblikovanje in analiza protokolov, ki preprečujejo tretjim osebam ali javnosti branje zasebnih sporočil. Kriptografija povezuje 3 znanstvene vede: matematiko, računalništvo in elektrotehniko. Nedavno se je v njo vključenim vedam pridružila tudi fizika, natančneje kvantna fizika, uporaba katere je po mnenju mnogih strokovnjakov naslednji korak na področju zaščite podatkov (Batelle, 2017). Kriptografija je del kriptologije, ki ima širši pomen in ju ne smemo enačiti. Kriptoanaliza pa preučuje kriptografijo in njene pomanjkljivosti.

Z besedo *enkripcija* primarno označujemo proces šifriranja podatkov v nerazumljiv format, ki se nato preko različnih kanalov prenesejo na končni cilj, kjer jih dešifriramo in vrnemo v prvotno stanje. V večini primerov za uspešno šifriranje potrebujemo enkripcijski ključ, katerega lastnik je edina oseba, ki lahko podatek dešifrira v prvotno stanje. Poznamo več načinov enkripcije, ki so predstavljeni v naslednjih točkah.

Poznamo 3 glavne vloge enkripcije (Aiello, 2018):

1. **Zaupnost** – Zagotavljanje zasebnosti podatkov.
2. **Integriteta** – Zagotavljanje točnosti podatkov.
3. **Dostopnost** – Zagotavljanje nemotenega delovanja strežnikov in dostopnosti podatkov.

Te 3 dimenzije ponazarjajo »trade-off« izbiro, s katero se soočamo pri vpeljavi varnostnih rešitev v informacijske sisteme. Aiello poudarja pomembnost identificiranja **kritičnih podatkov.** To so zelo občutljivi podatki, ki so dostopni le majhnemu številu ljudi, in ki zahtevajo visoko raven enkripcije. Pri načinu enkripcije podatkov je potrebno izbrati uravnoteženo razmerje med nivojem zaščite, dostopnostjo in zanesljivostjo, kar pa je odvisno od tipa podatkov, ki ga želimo zaščititi (Aiello, 2018).

2.1 Kriptografija in njen pretekli razvoj

Začetki kriptografije segajo več kot 4000 let v preteklost in je eno najstarejših znanstvenih področij v zgodovini človeštva (Cohen, 2017). Prvič se je pojavila v egipčanskih hieroglifih, kjer so vključevali zgodbe življenja preminulih vladarjev in njihove dosežke, vendar je bil njihov namen bolj posvečen izgledu pisave kot dejanski zaščiti sporočila. Kasneje so jo za enkripcijo sporočil in občutljivih podatkov uporabljala skoraj vsa ljudstva: Stari Grki, Kitajske dinastije, Rimljani, Mezopotamci, idr.

Kriptografija je odigrala zelo pomembno vlogo med obema svetovnima vojnama, predvsem med drugo svetovno vojno, ko je dešifriranje rotornih strojev in posledično pridobitev tajnih podatkov sovražnikov zaveznikom omogočilo nekaj ključnih zmag. Pred pojavom interneta je kriptografija služila zgolj zaščiti sporočil pred tretjimi osebami.

V zadnjih desetletjih se je razširila na mnoga druga področja, kot so overjanje in zaščita transakcij, preverjanje pristnosti in verodostojnosti sporočil, ugotavljanje identitete pošiljatelja oziroma prejemnika, unikatni digitalni podpisi, idr. Kriptografija je v večini današnjih varnostnih sistemov osnovna veda, na kateri temelji večina informacijske infrastrukture in tehnologij, povezanih z varnostjo vseh vrst podatkov.

2.2 Uporaba kriptografije in njihov pomen v sodobnih poslovnih sistemih

V tem poglavju bom raziskal področja, kjer je kriptografija najbolj uporabljena, kjer zagotavlja največjo poslovno vrednost in kjer učinkovito rešuje probleme varnosti in zasebnosti naših podatkov.

Varnost elektronskih sistemov in aplikacij temelji na kriptografiji. Številne prednosti njene uporabe so vprašljive. Da bi jih dognali, bi bila potrebna analiza stroškov in koristi, saj včasih ne gre za najcenejšo možnost, ampak za najbolj varno. Industrija varnosti sistemov in podatkov, ki uporablja kriptografijo, se tega zelo dobro zaveda, saj se na dnevni bazi srečuje s t.i. »trade-off« izbirami, torej ali želimo večje stroške sistema in višjo raven varnosti ali obratno (Maxim Integrated, 2017).

Uporaba kriptografije je na vsakem koraku, od najbolj preprostih uporab do kompleksnih. Želimo ali ne, šifriranje podatkov nas spremlja povsod. Pokriva komunikacijske platforme,

vse vrste elektronskih medijev, zdravstvo, obrambo, zavarovalništvo, šolstvo, bančništvo in finančne trge, vladne službe in medvladne transakcije ter še mnoga druga področja.

Uspešna vpeljava enkripcije in njenih izzivov mora enakomerno pokriti pravice, potrebe in odgovornosti (BSA, The Software Alliance, 2018):

- Državnih služb (zaščita zaupnih informacij z namenom preprečitve terorističnih in kriminalnih dejanj).
- Posameznikov (pravica do zaščite osebnih podatkov).
- Ponudnikov kritične infrastrukture (zaščita pred kibernetskimi napadi na vodovodna, električna, logistična, bančna in zdravstvena omrežja.
- Tretjih oseb (zaščita osebnih podatkov in poslovnih skrivnosti).
- Inovatorjev (razvoj produktov in storitev, ki nam izboljšujejo življenje in skrbijo za gospodarsko rast).

Kriptografija je prisotna vsakič, ko opravimo klic, kupimo nekaj s kreditno kartico, ali zgolj dvignemo denar na bankomatu. Zagotavlja zasebnost in varnost za uspešno izvedbo vseh vrst transakcij. Večine transakcij ne bi bilo mogoče izvesti brez uporabe kriptografije. Najbolj enostavna definicija opredeljuje enkripcijo kot transformacijo števil in besedila v zaporedje nesmisla (Ward, 2013).

Poznamo več vrst enkripcije. Nekatere so preproste, druge zelo kompleksne. Ne glede na metodo pa rezultat v nobenem primeru ne bi smel namigovati na način šifriranja vsebine. V moderni dobi je postala najpomembnejša enkripcija s pomočjo dveh ključev; javnega in zasebnega, imenovana tudi asimetrična enkripcija (Ward, 2013). Javni ključ je lahko dostopen vsem, a brez zasebnega ključa nima nobene vrednosti. Zgolj oseba, ki ima zasebni ključ, lahko pride do njegove vsebine.

V ZDA deluje več kot 6000 bank z 80 000 podružnicami, 6000 bolnišnic in več tisoč zavarovalnicami s podatki, ki jih želijo imeti zaščitene, zaradi česar uporabljajo enkripcijo (Batelle, 2017). Kljub relativno učinkoviti zaščiti pa se zaradi napredka tehnologije srečujejo s problemi zaostajanja. Najpogosteje uporabljen standardni kriptografski ključ RSA-1024 postaja zastarel in s strani ameriškega inštituta za varnost podatkov ni več priznan kot varen. Vedno večja je potreba po bolj varni in učinkoviti zaščiti podatkov: kvantni kriptografiji (Batelle, 2017).

Specifične uporabe kriptografije po področjih varnosti podatkov v poslovnih sistemih bom natančneje raziskal v naslednjih podpoglavjih.

2.2.1 Pomen kriptografije pri odjemalcih spletne pošte

Zaradi porasta zanimanja za bolj varne načine komunikacije so ponudniki spletne pošte ugotovili, da je za konkurenčnost na trgu potreben sistem obojestranske enkripcije, kar se je

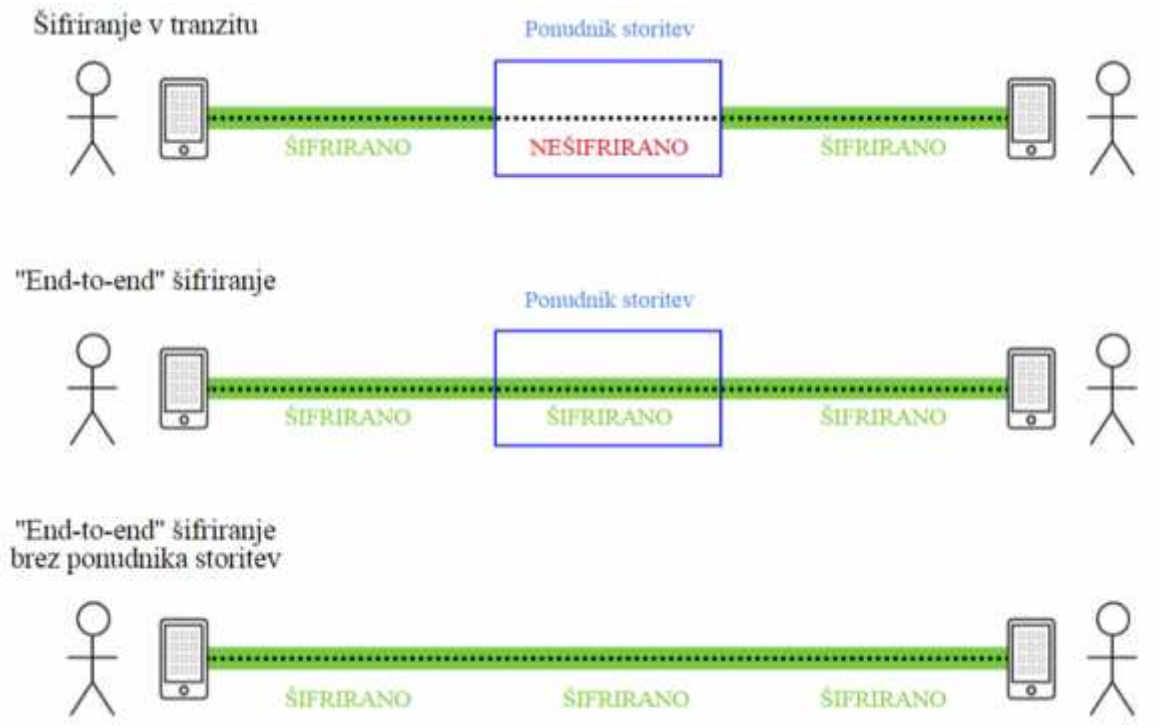
v zadnjih petih letih odrazilo na visoki rasti števila ponudnikov varne spletne pošte, kot so: Protonmail, Tutanota, Lavabit, Cisco, Sophos, Countermail in Posteo. Vsi našteti ponudniki uporabljajo t.i. end-to-end enkripcijo, kar pomeni, da je celotna pot vsebine od začetka do konca šifrirana in uporablja vsaj dva ključa, potrebna za dešifriranje.

Zanimiv je primer Lavabita, preference ameriškega žvižgača, ki je uporabljal njihovo spletno pošto za uspešno razkritje zaupnih dokumentov javnosti in za komunikacijo z novinarji, predvsem Glenom Greenwaldom (Poitras, 2014). Po razkritjih tajnih dokumentov je lastnika Lavabita Ladarja Levisona pridržal ameriški urad FBI in od njega zahteval ključe do vsebine elektronske pošte njegovih uporabnikov. Zaradi svojih moralnih prepričanj jim jih Levison ni predal in je raje zaprl celotno platformo, kot da bi izdal ključe za dostop do vsebine. Levison je pričal tudi pred Evropsko Komisijo in jih posvaril pred agresivnimi praksami, ki jih izvajajo ameriške in evropske tajne službe. Poudaril je tudi pomen temeljih človekovih pravic in pravico do zasebnosti ter predstavil osebne poglede na aktivnosti državnih tajnih služb in neupravičen nadzor prebivalstva.

2.2.2 Pomen kriptografije pri komunikacijskih platformah

Komunikacijske platforme so danes zelo razširjene, srečujemo jih na vsakem koraku, na primer kadar želimo komunicirati preko socialnih omrežij, mobilnih aplikacij, intraneta, ipd. Od običajnih platform se razlikujejo po eni glavni lastnosti, kar je razvidno s slike 3.

Slika 2: Primerjava med nešifriranim in šifriranim prenosom podatkov



Vir: Heimdal Security (2017).

Ta lastnost je šifriranje na strani ponudnika storitve. Podoben način šifriranja uporabljajo ponudniki varne spletne pošte, omenjeni v poglavju 2.3.1.

Najbolj razširjena komunikacijska platforma Whatsapp (preko 1 milijarda uporabnikov) je za implementacijo t.i. »end-to-end« šifriranja potrebovala kar 6 mesecev, s čimer je dala jasen signal konkurentom, da mora ta varnejši način komunikacije postati univerzalna vrednota in norma (Zaharia, 2017). Takšno šifriranje onemogoča vdore v sistem oziroma tudi ob potencialnem vdoru preprečuje možnost dostopa do vsebine sporočil.

Takoj za Whatsappom je njegov sledilec Viber (780 milijonov uporabnikov), ki uporablja podoben način enkripcije, poleg tega pa je izdal t.i. Viber Encryption Overview, ki služi kot vodnik za uporabo enkripcije za tiste, ki želijo vedeti več o tej temi. Ta vodnik opozarja na eno izjemo, katere ta nivo enkripcije ne pokriva: priponke, ki jih pošiljamo preko Applovega operacijskega sistema IOS (Zaharia, 2017).

Druge platforme, ki uporabljajo omenjen način šifriranja, so na primer Signal, Telegram, ChatSecure, CyberDust, CacaoTalk in Line.Glede na razširjenost in rast števila vpeljav bolj varne enkripcije je pričakovati, da bo v prihodnje to zagotovo temeljna konkurenčna prednost ponudnikov komunikacijskih platform. Potrebno bo bolj poglobljeno razumevanje učinkovite zaščite uporabnikov in interakcij med njimi. Steve Aiello, arhitekt spletnih rešitev iz podjetja Online Tech, v svojem članku, imenovanem »Challenges to encrypting data«, omenja, da bo predvsem hitrost platform v kombinaciji z visoko stopnjo varnosti in zanesljivosti glavni dejavnik za njihovo uspešno in razširjeno uporabo.

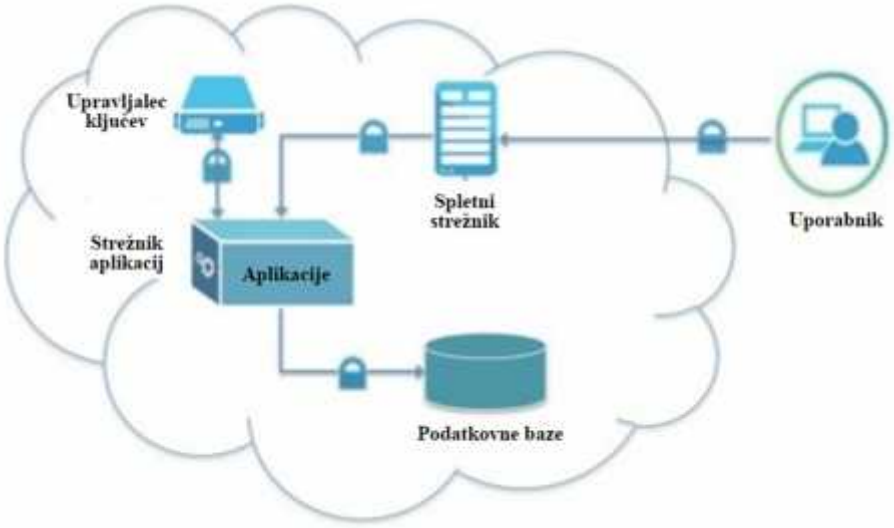
2.2.3 Pomen kriptografije za računalništvo v oblaku

Računalništvo v oblaku se je v zadnjih letih razširilo in postalo dostopno vsem. Še vedno pa obstaja veliko pomislekov glede poglavitnih dejavnikov, ki so bili izpostavljeni na 7. Mednarodni konferenci o komunikaciji, računalništvu in virtualizaciji v Bombaju, Indija (Manish Potey, Dhote & Deepak, 2016):

- Varnost podatkov v oblaku.
- Zasebnost podatkov v oblaku.
- Načini preverjanja pristnosti uporabnika.

Skrb glede učinkovitosti tovrstnega shranjevanja je mnoge odvrnila od uporabe računalništva v oblaku in posledično od koristi, ki jih ta način shranjevanja podatkov ponuja. Večina ponudnikov storitev v oblaku ne ponuja dodatne zaščite in shranjuje podatke v standardni obliki brez enkripcije ter pričakuje, da bo uporabnik sam poskrbel za primeren način zaščite, tako na vhodni kot tudi izhodni strani (Manish Potey, Dhote & Deepak, 2016).

Slika 3: Kako deluje šifrirano računalništvo v oblaku



Vir: Encryiption in the Cloud (2017).

Slika 3 nam prikazuje postopke zaščite uporabnikovih podatkov. Gre za trojni način »end-to-end« zaščite, kjer so podatki med celotno potjo v šifrirani obliki. Ta način zaščite se od zaščite, ki jo uporabljajo običajni ponudniki podobnih storitev, razlikuje po tem, da izvajalec storitve poskrbi za varnost, ne uporabnik.

Zaščita je potrebna na vseh treh ravneh delovanja: ravni ponudnika storitve, programski ravni oziroma ravni aplikacij in ravni baz podatkov. Ob upoštevanju varnostnih vidikov ne smemo pozabiti na hitrost dostopa, ki je pri večjih količinah podatkov še posebej pomembna, in na ukrepe v primeru neželenega vdora tretjih oseb v uporabnikovo bazo.

2.2.4 Pomen kriptografije pri ERP sistemih

Enterprise resource planning (v nadaljevanj ERP) sistemi ponujajo podjetjem celovite programske rešitve in zvišujejo raven povezanosti različnih oddelkov podjetji, kot so na primer nabava, prodaja, računovodstvo, proizvodnja, ipd. Prvo jih je leta 1990 omenilo podjetje Gartner Groupkot naslednjao generacijo programov za upravljanje proizvodnje in za načrtovanje resursov. Danes je ERP obravnavan kot »cena vstopa za delovanje na modernem trgu. Takšni sistemi so v uporabi že relativno dolgo, v sedanjih časih pa se srečujejo s spremembo, ki bo transformirala njihovo obliko in delovanje. Razvijali se bodo v bolj inteligentne, integrirane, prilagodljive in varne sisteme (She & Thiraisingham, 2007).

Poleg standardnih lastnosti ERP sistemov je v ospredju varnost in odpornost proti vdorom tretjih oseb. Gre namreč tako za občutljive osebne podatke zaposlenih, kot tudi za poslovne skrivnosti podjetja. ERP sisteme uporablja tudi vojska, tajne službe, zdravstvo in finančni trgi, zato je varnostni vidik še toliko bolj pomemben (She & Thiraisingham, 2007). Največji izziv v prihodnosti bo transformacija zaprtih ERP sistemov v odprte brez zmanjšanega

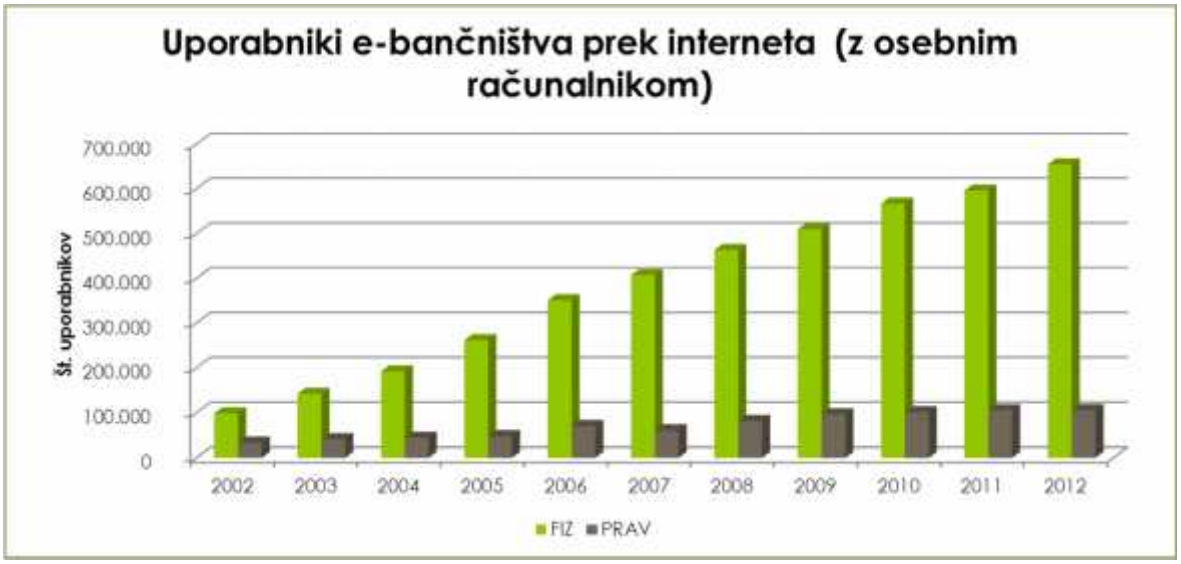
nivoja varnosti, kar bo mogoče doseči z enkripcijo in primernim preverjanjem pristnosti. Potrebna bo nova zasnova varnostne arhitekture in večji poudarek na spremljanju gibanja dokumentov znotraj sistema (She & Thiraisingham, 2007).

2.2.5 Pomen kriptografije v E-bančništvu

E-bančništvo je finančna panoga, kjer je potreba po varnosti še toliko bolj izrazita. Do vseh podatkov o katerikoli opravljeni transakciji, kot tudi do ostalih informacij uporabnika te storitve je mogoče dostopati preko spleta, kar zvišuje raven izpostavljenosti uporabnikov. Sodobni načini preverjanja, kot so gesla, PIN kode, digitalni podpisi, idr., ne zadovoljujejo več varnostnih standardov (Khatri & Budhiraja, 2013). Koncept, ki bi lahko rešil ta problem, se imenuje UTII (angl. Unique Thumb Impression Idenity), ki onemogoča dostop in opravljanje transakcij, tudi kadar ima uporabnik ustrezne podatke, tako o karticah, kot tudi o geslih in podatke, potrebne za ostale načine preverjanja. UTII dostop omogoči le eni osebi in ga ni mogoče ponarediti. Gre za preverjanje avtoritete preko prstnega odtisa, kjer se lahko transakcije izvajajo pod pogojem, da se prstni odtis ujema s tistim v bančni bazi podatkov.

Bančništvo se je v zadnjih dveh desetletjih spremenilo in se preselilo s papirnatega poslovanja v elektronsko. Transakcije se ne opravljajo več fizično, ampak elektronsko preko e-bančništva ali m-bančništva.

Slika 4: Rast e-bančništva



Vir: Banka Slovenije (2013, str. 45).

Raven zaupanja v te sisteme je bila dovolj visoka, da je krog njihovih uporabnikov postal precej širok, vendar so številni vdori in kraje postavili elektronsko bančništvo pred preizkušnjo. Tsarenko in Tojib v svoji študiji o zaupanju uporabnikov v banke in njihovih odnosih s finančnimi institucijami v Avstraliji, ugotavljata, da obstajajo tri skupine lastnosti uporabnikov z vidika skrbi za zasebnost:

- **Pragmatiki** – Visoka raven pripravljenosti deliti svoje podatke ob primerni kompenzaciji in močno prepričanje, da vladne službe zagotavljajo zadovoljivo raven varnosti podatkov.
- **Indiferentni uporabniki** – Nizka raven zaskrbljenosti glede ravni zasebnosti, pripravljenost deljenja podatkov in relativno nizka raven zaskrbljenosti glede zakonodaje, ki regulira raven zasebnosti in zaupanja.
- **Kompetentni uporabniki** – Najvišja raven zavedanja glede zasebnosti in varnosti in nizka raven zaupanja v zakonodajo ter učinkovito izvajanje le-te.

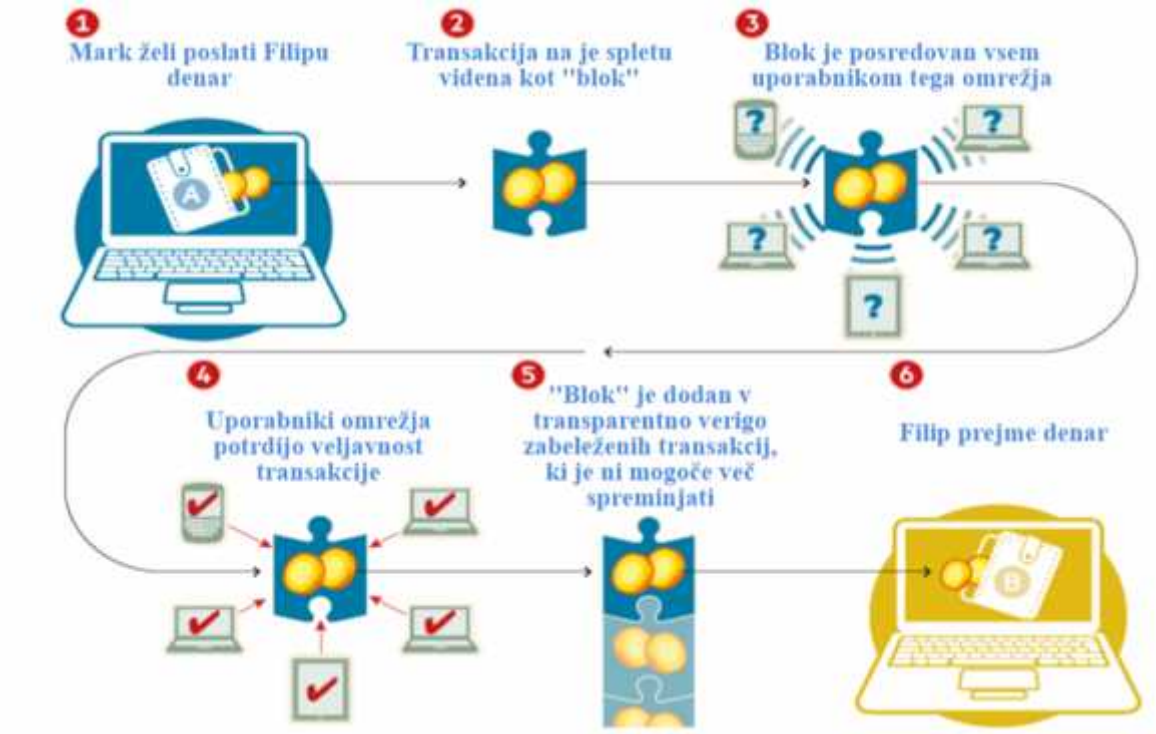
V študijo sta zajela 5 dejavnikov: skrb za zasebnost, zaupanje, skrb za izjave o zasebnosti, vladna zaščita zasebnosti in pripravljenost za kompenzacijo (Tsarenko & Tojib, 2009). Rezultat je pokazal, da še vedno obstaja visok delež ljudi, ki jih zasebnost ne skrbi, in ki so pripravljeni deliti vse svoje podatke, nekateri v zameno za določene koristi. Izpostavljen je bil tudi problem nezavedanja o procesiranju in deljenju naših podatkov med institucijami in o moralnih vprašanjih, povezanih s takšnimi dejanji.

Vprašanje zaupanja v bančne institucije postaja osrednja tema, saj imajo banke v okviru bančne tajnosti moč upravljati z našimi podatki brez naše vednosti. Vsak naš poskus nadzora njihovega delovanja bo najverjetneje neuspešen, saj si bodo banke močno prizadevale, da nam onemogočijo vpogled v njihove evidence. Z vidika strank se poraja vprašanje legitimnosti bank za posredovanje naših podatkov drugim bankam in organizacijam. Težava je tudi v zakonodaji, ki ne preprečuje takšnih posegov, zakoni, ki se jih regulirajo, pa so slabo izvrševani.

2.2.6 Uporaba kriptografije v tehnologiji veriženja blokov

Verjetno najbolj obetaven koncept varnih transakcij in varstva osebnih podatkov temelji na matematičnih principih enkripcije. Tehnologija veriženja blokov, v nadaljevanju blockchain tehnologija, označuje sistem porazdeljenih podatkovnih baz imenovanih bloki. Vsak naslednji blok vsebuje podatke in povezavo do prejšnjega bloka in je odporen proti spremembam. Ko je enkrat urejen, se ne more več spreminjati. To tehnologijo je prvič uporabil in opredelil Satoshi Nakamoto (2008), za katerega se domneva, da je izumil Bitcoin. Blockchain metoda uporablja »peer-to-peer« omrežje in porazdeljeno bazo časovnic. Za boljšo predstavitev si oglejmo sliko 5.

Slika 5: Delovanje mreže veriženja blokov



Vir: How Blockchain works, (2017).

Metoda veriženja blokov deluje na principu vzajemnega priznavanja in je trenutno eden najbolj obetavnih konceptov novega način varnejšega interneta, imenovanega »Web 3.0« (Walsh, 2017). Kriptovaluta Bitcoin bi lahko bila prvi korak vpeljave in medmrežja nove generacije. Te aplikacije Dean Welsh iz skupnosti Cryptorials prepoznava kot D'Apps (angl. Distributed Applications) oziroma porazdelitvene aplikacije. Web 3.0 temelji na principu varnosti in odprtosti transakcij, kar zagotavlja popolno transparentnost in odpornost proti kibernetski kriminaliteti. Veriga blokov namreč vsak poskus t.i. neavtentične transakcije nemudoma zavrne in ga ne vključi v svojo mrežo preverjenih blokov. Ena izmed glavnih pomanjkljivosti blockchaina je potreba po večji kapaciteti podatkovnih baz (beležijo se vse transakcije) in počasnejšem delovanju zaradi časa, potrebnega za preverjanje avtentičnosti transakcije. Dejansko pa je potrebna visoka zmogljivost računalniške infrastrukture, ki omogoča delovanje verige blokov, hkrati tudi prednost, saj ta t.i. procesna moč predstavlja tudi moč odpornosti proti napadom, saj so računalniki povezani v skupno omrežje. Splošno gledano prednosti znatno pretehtajo slabosti.

S poslovnega vidika metoda veriženja blokov prinaša dodano vrednost predvsem zaradi odpornosti proti kraji občutljivih podatkov in poslovnih skrivnosti. Poleg tega nas varuje pred nepooblaščenimi transakcijami in spremembami identitet. Identitete na verigi so unikatne in jih ni mogoče spreminjati. Podjetjem tako ni potrebno namenjati mnogo sredstev za zagotavljanje varnosti njihovih podatkov, saj jim vključenost v močno verigo in

sodelovanje pri preverjanju transakcij zagoravlja varnost, vzdrževanje takšnih sistemov pa je cenejše kot od vzdrževanja pri tradicionalnih načinih zaščite.

2.3 Prihodnost kriptografije

To poglavje bo zajemalo prihodnje načine enkripcij, ki obetajo korenite spremembe na področju varnosti in transakcij. Predvsem kvantna enkripcija je trenutno eno najbolj obetavnih področij, a bo za njeno uspešno uporabo potrebnih še veliko raziskav in testiranj. Kvantna ekripcija bo ob uspešni uvedbi popolnoma spremenila način zavarovanja naših podatkov in občutno zvišala odpornost proti zlorabami le-teh.

Biometrična enkripcija za dešifriranje ključa uporablja posameznikove unikatne lastnosti, kot na primer skeniranje prstnega odtisa ali skeniranje šarenice. S pomočjo biometrike uporabniku omogoča učinkovito zaščito pred zlorabami in krajo njegovih podatkov.

2.3.1 Pojav in razvoj kvantne kriptografije

Naslednji korak pri enkripciji bo uporaba porazdelitvene kvantne kriptografije, ki obljublja nezlomljivo kodo (The Optical Society, 2013). Za razliko od običajne metode enkripcije kvantna metoda ne združuje ključev in podatkov. Kvantna metoda temelji na principih in zakonih kvantne fizike in ne matematike. Za prenos podatkov je potrebno kvantno omrežje, kjer se podatki preko optičnega kabla prenašajo v obliki fotonov oziroma svetlobnih delcev.

Slika 6: Postopek delovanja šifriranja preko kvantne enkripcije

Vir: Mitsubishi Electric (2017).

Distribucija kvantnega ključa (angl. quantum key distrubution – QKD) oblikuje ključ v obliki razpršenega gesla. Kadar želi tretja oseba prestreči del tega ključa, sta obe strani nemudoma obveščeni, podatki pa se v istem trenutku transformirajo v neuporabno obliko. Takšna metoda je v teoriji nezlomljiva in odporna proti vsem vrstam napadov (Batelle, 2017). Kljub temu ima Renato Renner, profesor teoretične fizike na Inštitutu teoretične fizike v Zürichu, pomisleke glede tega koncepta. Renner je mnenja, da nič ni absolutno in da bi ta način deloval popolno le kadar bi bili izpolnjeni naslednji trije pogoji:

- **Tajnost gesla.**
- **Zanesljivost naprav.**
- **Popolnost in točnost kvantne teorije.**

Ne glede na pomisleke pa so mnoge države že prepoznale uporabnost kvantne kriptografije in začele z testiranjem in grajenjem omrežij. ZDA in Kitajska pospešeno raziskujeta to področje, slednja naj bi že zgradila 2000 km dolgo kvantno omrežje med Pekingom in Šanghajem. Omenja se tudi, da naj bi bilo v prihodnosti mogoče takšno vrsto prenosa podatkov opravljati preko satelitov, kar bi bistveno povečalo doseg in dostopnost naprav (Ruhr-Universitaet-Bochum, 2017).

2.3.2 Razvoj metode veriženja blokov in področja njene uporabe v prihodnosti

Ena večjih prednosti metode veriženja blokov je v njeni univerzalni uporabi in možnosti apliciranja na skoraj vsako panogo, ki beleži transakcije. Sprva mišljena kot podpora za kriptovalute danes pridobiva na vrednosti kot osnova za vse vrste platform. Največji apetit in interes zanjo se kaže v finančnem sektorju, kjer ugotavljajo, da so možni izjemni prihranki stroškov transakcij in delovanja (Grut, 2016).

Revizijska družba Deloitte je v svoj članek, imenovan »Blockchain Technology«, vključila prednosti in izzive, ki bodo definirali tehnologijo veriženja blokov v prihodnosti.

Izzivov je mnogo, glavna pa sta zagotovo zagotavljanje hitrosti in zanesljivosti. Pri tem ne gre zgolj za hitrost transakcij, ampak tudi za hitrost preverjanja pristnosti in legitimnosti. Ta tehnologija je razmeroma mlada in je dolgoročno še nepreverjena. Naslednji izziv je vprašanje odobravanja tehnologije s strani državnih regulatorjev. Že BitCoin je naletel na precejšnje neodobravanje državnih organov zaradi negativnih vplivov na anonimne transakcije, ki so koristile nezakonitim aktivnostim.

Velika potrošnja električne energije, ki je vidna pri rudarjenju kriptovalut, kaže na potrebo po ponovnem razmisleku o primernosti obstoječega način potrjevanja transakcij in zadovoljivosti trenutne učinkovitost sistema. Integracija verižnih metod nam lahko pokaže, če obstaja način vpeljavo tehnologije veriženja blokov brez popolne spremembe obstoječih sistemov. Slednja opcija lahko povzroči visoke stroške in čas implementacije. Ker pri tej implementaciji ne gre za majhne spremembe, ampak za celovito prenovo sistema, se pojavlja

vprašanje zaupanja v takšno tehnologijo, pripravljenosti zagotoviti potreben znesek investicije in pripravljenosti sprejeti izvedbo projekta, temelječega na takšnem konceptu. Vsa ta vprašanja so izhodišče za nadaljne razprave, ki bi lahko pripomogle k boljšem, varnejšem in bolj učinkovitem poslovanju in delovanju sistemov, ki slednje omogočajo, v prihodnosti.

2.3.2.1 Področja uporabe tehnologije veriženja blokov v prihodnosti

Oscar Williams-Grut, novinar priznane revije Business Insider v svojem članku navaja 5 različnih panog, pri katerih spreminja in optimizira način poslovanja in odpravlja probleme glede varnosti, pojavljanja napak in kraje identitete. Podatke je črpal iz poročila ameriške banke Goldman Sachs o prihodnosti donosnih naložb, imenovanem Goldman Sachs Global Investment Research. Ker za Evropo ni podatkov, bodo predstavljeni podatki za ZDA.

Gospodarstva deljenja resursov (angl.. Sharing economies). Goldman Sachs prepoznava v tem sektorju prednosti na področju shranjevanja identitete posameznikov na verigi blokov, kjer so ocene in priporočila posameznikov pristne in videne tudi na drugih platformah (Grut, 2016). V primeru najemanja sobe ali apartmaja od fizičnih oseb lahko ljudje hitro izvedo, ali gre za zanesljivega gostitelja ali ne, saj lahko imajo na voljo mnogo pristnih informacij o njem. Identitete se na takšni platformi ne da ponarediti. Nekateri največji ponudniki teh platform, kot sta na primer Airbnb in Homeaway, že razmišljajo o tem in vlagajo sredstva v raziskavo in razvoj tovrstnih metod. Velikost trga kratkoročnega najema bivalnih površin v ZDA je od 3 do 9 milijard ameriških dolarjev letno.

Trg električne energije. Veriženje blokov posameznikom, ki s proizvodnjo energije iz alternativnih virov ustvarjajo viške, omogoča njeno prodajo na trg in večjo učinkovitost letega (Grut, 2016). Ameriška banka Goldman Sachs ima vizijo skupnega trga elektrike, na katerem bi poleg elektrarn nastopali tudi posamezniki, ki bi z pomočjo svoje identitete na verigi blokov lahko legitimno prodajali elektriko. Ta nov način trgovanja z energijo omogoča transakcije med strankami, ki se sploh ne poznajo, imajo pa preverjeno identiteto (Grut, 2016). Nekatere platforme že prakticirajo ta način distribucije. Podjetja, kot sta TransActive Grid in Grid Singularity, trenutno operirata na trgu, velikem med 2.5 in 7 milijard ameriških dolarjev letno.

Nepremičninski trg. Podatki o nepremičninah so shranjeni na verigi blokov, kjer posamezniki hitro in enostavno preverijo, ali ima domnevni prodajalec hišo res v lasti ali ne. Trenutno je ta proces upravljan ročno, kar je dražje in bolj dovzetno za napake. Kasneje, ko bi koncept bil že bolj razvit, naj bi takšni sistemi bili veliko bolj uporabni in točni, predvsem pa bi odpravljali dolgotrajno iskanje nepremičnin, ki je mnogokrat povezano z visokimi transakcijskimi stroški (Grut, 2016). Podjetji, ki uporabljata to tehnologijo, se imenujeta BitFura in Factom, prihranki pa znašajo od 2 do 4 milijard ameriških dolarjev letno.

Trg vrednostnih papirjev. Goldman Sachs meni, da kljub nizkim stroškom transakcij obstaja tveganje napak, ki se zgodijo v 10 % primerov transakcij. Predvideni prihranki zaradi uporabe blockchain tehnologije so od 11 do 12 milijard ameriških dolarjev letno. Podjetja, kot so Digital Asset Holdings, itBit, Ripple in Axoni, to tehnologijo že uporabljajo in beležijo pozitivne rezultate (Grut, 2016).

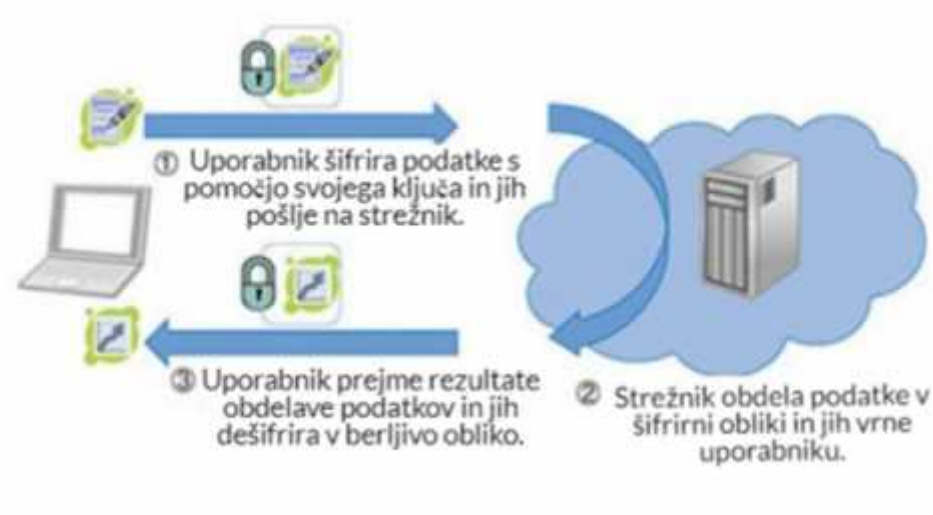
Finančni trgi. Uporaba tehnologije veriženja blokov na finančnih trgih podobno kot v primeru gospodarstva deljenja resursov temelji na principu unikatne identitete na verigi blokov. Prihranke časa in denarja omogoča na primer banki, saj gre za neke vrste digitalni potni list, ki že vsebuje podatke o nas. Primer uporabe te tehnologije je pri zahtevi za pridobitev kredita ali pri odobritvi posojila, koristi pa prinaša tudi na področju t.i. sumljivih transakcij in pranja denarja, saj je za uspešno transakcijo potrebna preverjena identiteta. Uporablja jo podjetje SWIFT, prihranki pa segajo med 3 in 4 milijard ameriških dolarjev letno.

2.3.3 Homomorfična enkripcija

Ena izmed možnih rešitev za povišanje ravni varnosti osebnih podatkov v prihodnosti je t.i. homomorfična enkripcija. Standardna metoda enkripcije nam omogoča uporaben tip datoteke šele po dekripciji. Brez dekripcije je naša datoteka brez vrednosti, saj je šifrirana in z njo ni mogoče operirati. To je sicer pozitivna lastnost takšne enkripcije, vendar je časovno dokaj potratna, saj je potrebno podatke dešifrirati, jih procesirati in spet šifrirati.

Homomorfična enkripcija odpravlja ta problem, saj omogoča procesiranje šifriranih podatkov, ne da bi jih kadarkoli bilo potrebno dešifrirati (Manish Potey, Dhote & Deepak, 2016).

Slika 7: Delovanje homomorfične enkripcije



Vir: Tibouchi (2017).

Na zgornjem primeru lahko vidimo, da naši podatki v nobenem transakcijskem delu komunikacijske poti niso v dešifrirani obliki, in da so popolnoma odporni proti vdorom tretjih oseb. Uporablja poenostavljen algoritem, katerega lahko apliciramo na različna področja, kot so spletne dražbe, zdravstveni sistemi, poslovne platforme, idr.

Trenutna »hiba« homomorfične enkripcije je učinkovito delovanje. Ta način namreč za transformacijo podatkov še vedno zahteva veliko časa, zato v trenutnem stanju ni ekonomičen. Potrebno bo najti rešitev, kako ob enakem nivoju varnosti, zagotoviti uporabniku hitrejšo obdelavo in shrambo njegovih podatkov.

IBM je na začetku leta 2018 predstavil nov koncept homomorfične enkripcije imenovan HElib, za katerega trdi, da je 75 krat hitrejši kot tisti, ki so ga izdali pred tremi leti (Chirgwin, 2018). Ekipi IBM je to uspelo s spomočjo učinkovitejših algoritmov in t.i. posebnih avtomorfizmov (matematična operacija).

2.3.4 Biometrična enkripcija

Ta vrsta enkripcije za svoje delovanje uporablja posameznikove unikatne karakteristike, s katerimi preverja njegovo pristnost in identiteto. Ker je težko ponarediti naše naravne lastnosti, je ta način zelo odporen proti zlorabam.

Biometrična enkripcija lahko vključuje naslednje lastnosti:

- Obraz.
- Prstni odtis.
- Glas.
- Način podpisa.
- Očesna šarenica.
- Oblika ušesa.
- DNA vzorec.
- Tudi druge manj učinkovite lastnosti (vonj, hoja idr.).

Identifikacija poteka v dveh fazah. V prvi fazi, imenovani vpis, sistem pridobi našo biometrično lastnost. Potem s pomočjo ekstrakcije ustvari digitalno verzijo vzorca. V drugi fazi, imenovani preverjanje, se ustvarjen digitalni vzorec primerja z originalnim in ugotavlja ali gre za ujemanje ali ne.

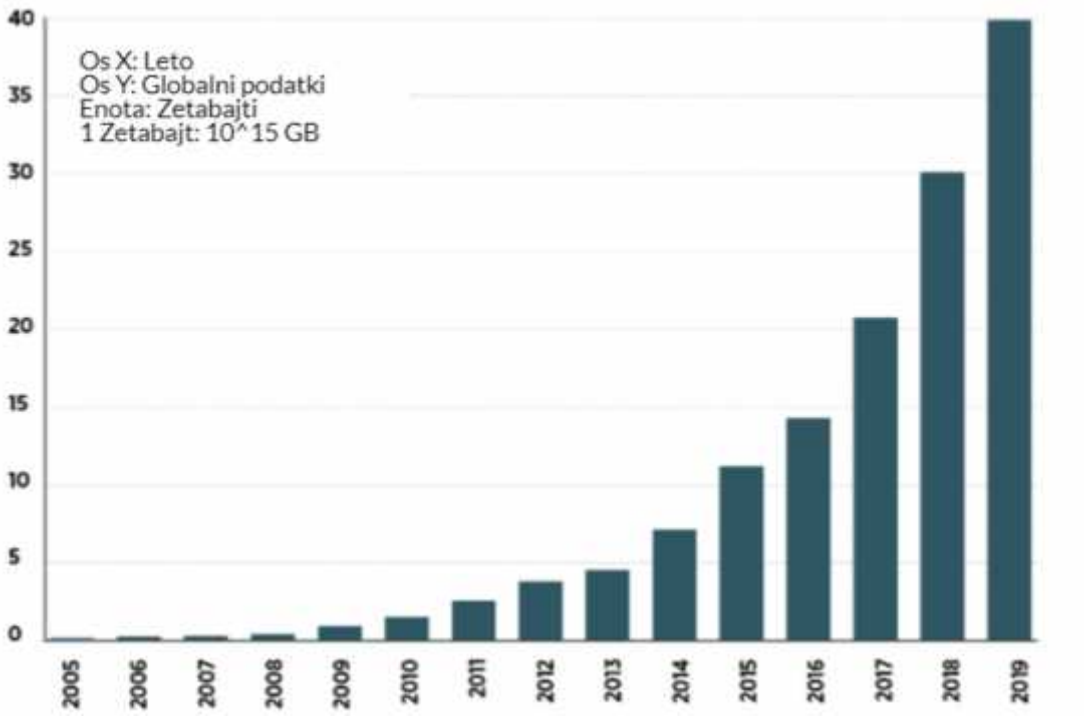
Težave, s katerimi se soočajo snovalci varnih transakcijskih sistemov, izhajajo iz zastarelih metod preverjanja in splošnih problemov z gesli. Biometrično preverjanje nam lahko omogoča dostop do spletnega bančništva, elektronske pošte in drugih platform (Marous, 2016). Če pogledamo zgolj panogo pametnih telefonov, je že skoraj 50 % le-teh opremljenih s senzorjem za skeniranje prstnega odtisa (Simic, 2016).

Paul Lee, vodja tehnološkega oddelka za raziskave in razvoj v revizijski hiši Deloitte je izjavil: »Z drugimi osebami lahko delite gesla, ne morete pa deliti prstnega odtisa.« To je v veliki meri res, vendar obstaja veliko pomislekov glede tega načina preverjanja pristnosti. Mnoga podjetja, ki delujejo na področju biometrične tehnologije že razmišljajo kako bi lahko še izboljšali varnosti in odpravili ovire pri prehajanju na biometrična gesla iz tradicionalnih gesel. Podjetje HYPR Corp., eno vodilnih ameriških podjetij ki ponujajo varnostno tehnologijo, razvija način preverjanja identitete, ki bo vključeval več biometričnih lastnosti (Simic, 2016). Tako bi lahko informacijski sistem od nas zahteval skeniranje šarenice, prstnega odtisa in dlani za dostop do podatkov, kar bi bistveno povečalo varnost in odpornost proti zlorabam. Vprašanje pa je ali bi takšen sistem deloval učinkovito in koliko časa bi za takšno aktivnost potreboval.

3 POMEN KRIPTOGRAFIJE ZA VARNOST OSEBNIH PODATKOV NA SPLETU IN KORISTI NJENE UPORABE V GOSPODARSTVU

V prejšnjih poglavjih sem raziskal pomembnost zavedanja o problematiki varstva osebnih podatkov, zakonodaji in državnih službah ki se ukvarjajo s to problematiko, ter ugotovili, da je potreba po učinkoviti enkripciji podatkov iz leta v leto večja. Za boljšo predstavo, zakaj potrebujemo enkripcijo, si oglejmo sliko, ki prikazuje globalno rast količine zbranih podatkov.

Slika 8: Rast količine zbranih podatkov



Vir: Audin (2015).

Slika 8 nam prikazuje eksponentno rast količine zbranih podatkov med letoma 2005 in 2019. Z rastjo t.i. »big data« industrije, ki se ukvarja z obdelavo in analizo ogromnih količin podatkov, raste tudi potreba po učinkoviti in varni hrambi le-teh.

Podjetja stremijo k temu, da bi čimbolj podrobno poznala svoje potrošnike in temu primerno prilagodila svoje proizvode ali storitve. Podatki, ki jih zbirajo, so iz leta v leto številčnejši in bolj raznoliki. Podatke je potrebno sortirati, jih urediti in izvesti njihovo analizo, ki lahko poda relevantne informacije o potrošnikih.

Informacijska infrustruktura podjetij, ki poslujejo na internetu, za svoje delovanje zahteva natančno in strateško planiranje, pri čemer enkripcija igra ključno vlogo. Slednja omogoča zaščito poslovnih skrivnosti podjetja, informacij o njegovem delovanju in njegovih potrošnikih.

3.1 Področja, kjer je možno izboljšanje varnosti osebnih podatkov s pomočjo kriptografije

V tem poglavju bom preučil, katera področja enkripcija pokriva in kateri so načini, ki omogočajo višjo raven varnosti osebnih podatkov. Raziskal bom tudi, s kakšnimi metodami lahko svoje podatke bolje zaščitimo in uporabljamo internet varno ter brez »puščanja sledi«. Te metode so danes dostopne vsakomur in ne potrebjemo posebnih znanj za njihovo uporabo. Z uporabo teh metod lahko občutno znižamo raven sledljivosti naših dejanj in učinkovito zaščitimo svoje podatke, ki vključujejo internetno zgodovino, IP naslov in lokacijo.

3.1.1 Področja, kjer je možna zaščita osebnih podatkov, in metode, ki omogočajo to zaščito

Najbolj razširjena uporaba kriptografskih zaščit je na področju varovanja občutljivih podatkov in dokumentov. Kot smo že ugotovili, obstaja več različnih vrst enkripcije, ki se razlikujejo v načinu šifriranja in dolžini ključa. Potrebno je poznati značilnosti, prednosti in slabosti različnih metod, ter se na podlagi analize stroškov in koristi odločiti za primerno rešitev.

Načini šifriranja podatkov:

- Simetrični način

Pri simetričnem šifriranju uporabljamo zgolj en ključ tako za šifriranje, kot tudi za dešifriranje podatkov. Podatke na pošiljateljevi strani s simetričnim ključem pretvorimo v šifrirano besedilo, ki se na prejemnikovi strani s pomočjo istega ključa dešifrira v originalno obliko. Ta metoda je sicer najhitrejša, a ima določene pomanjkljivosti, ki jih odpravlja

asimetrična enkripcija. Zaradi svoje učinkovitosti je uporabna predvsem pri zaščiti večjih količin podatkov.

- Asimetrični način

Asimetrično šifriranje uporablja 2 šifrirna ključa: javnega in zasebnega. Javni ključ je brez zasebnega neuporaben in obratno. Za uspešno dešifriranje podatkov sta potrebna oba ključa, zato je ta način bolj varen od simetričnega. Pomanjkljivost tega načina je dolgotrajen proces šifriranja zaradi daljših procesov reševanja matematičnih izračunov. Visoka raven varnosti tega načina šifriranja pomeni, da je le-ta primeren za šifriranje manjših, a vrednejših podatkov, kot so na primer kode za aktivacijo sistemov, gesla in druge vrste strogo zaupnih podatkov.

Enosmerno šifriranje. Temu načinu šifriranja pravimo tudi funkcija konzumiranja ali strnjevanja sporočil. V osnovi se ta metoda razlikuje od prvih dveh po načinu uporabe, saj je njen namen potrditev opravljene transakcije in ne zaščita vsebine. Enosmerno šifriranje spremeni besedilo v binarno zaporedje simbolov in je nepovratno, kar pomeni, da je vsebino sporočila po transformaciji nemogoče matematično pretvoriti nazaj v berljivo obliko. Pri šifriranju tako kot prva dva načina ne uporablja šifer, ampak kompleksne matematične izračune. Uporablja se predvsem kot digitalni podpis.

Oba načina imata prednosti in slabosti. Simetrični ključ ima prednost predvsem pri hitrosti delovanja, saj je učinkovit in preprost. Ima pa pomanjkljivosti pri dogovoru o ključih in ga lahko uporabljamo zgolj kadar smo povezani z internetom. Asimetrični ključ je zaradi svoje kompleksnosti mnogo počasnejši od simetričnega (RSA je približno tisočkrat počasnejši od DES), je pa bolj varen in zanesljiv (Chandramouli, Iorga & Chokhani, 2013). Lahko ga uporabljamo v obeh primerih; kadar smo povezani z internetom in kadar nismo.

Pomemben dejavnik, ki prispeva k učinkoviti zaščiti, je zavedanje o lokacijah kritičnih podatkov in dodatna zaščita najbolj tveganih in zaupnih, pri katerih bi bila škoda v primeru pridobitve ključa s strani tretjih oseb, največja.

3.1.2 Zaščita pred sledljivostjo na internetu in dostopom do podatkov s strani tretjih oseb

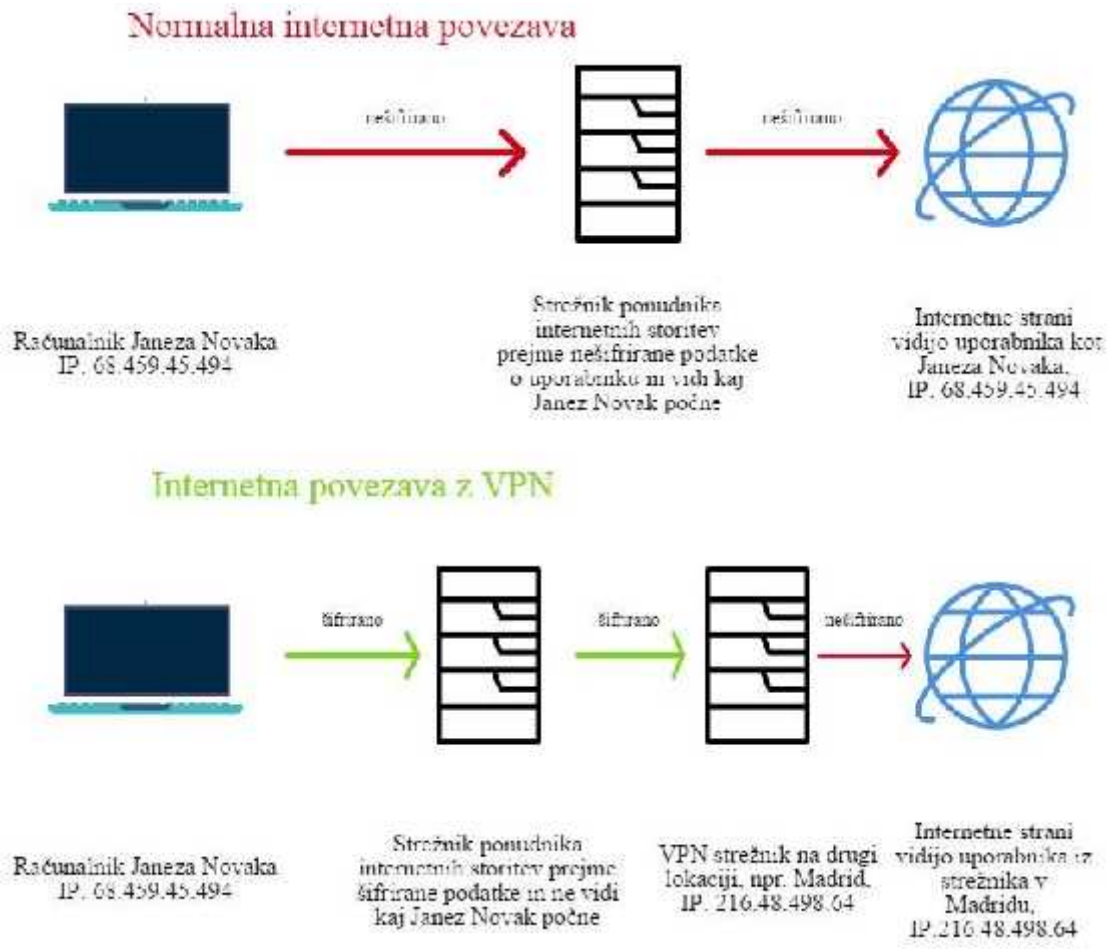
Kriptografija igra pomembno vlogo pri preprečevanju nadzora prebivalstva. Kot smo že ugotovili, nam le-ta zagotavlja anonimnost pri uporabi komunikacijskih kanalov in podatkovnih baz. Razkritja žvižgačev v zadnjih letih so pokazala, kako razširjen je nadzor množic. Nekateri ljudje v tem ne vidijo nič negativnega, strokovnjaki v industriji varnostnih produktov pa so mnenja, da so tovrstne prakse nedopustne in da so v nasprotju z temeljno človekovo pravico – pravico do svobode. Evropska direktiva o zaščiti osebnih podatkov

natančno definira, kdaj gre za zakonsko dovoljeno zbiranje podatkov in kdaj ne (European Commission, 2017).

Za učinkovito zaščito pred nadzorom in sledenjem je potrebna vpeljava enkripcije na več področjih:

- **Telefonski klici in sporočila** – Nedavna razkritja Wikileaks-a so pokazala, da ima ameriška tajna služba NSA dostop do največjega ponudnika telefonskih storitev, preko katerega prisluškujejo posameznikom, zato je prvi korak do varnejše komunikacije uporaba enkriptiranih platform, ki nam omogočajo komunikacijo. Primer takšne platforme je platforma Signal. Le-ta ponuja t.i. »end-to-end« enkripcijo, kar pomeni, da je klic ali sporočilo zaščiten(-o) skozi celotno komunikacijsko pot; od pošiljatelja do naslovnika.
- **Elektronska pisma** – Prav tako kot klici in sporočila so elektronska pisma postala tarča nadzora, zato opažamo vedno več ponudnikov enkriptiranih platform. Primeri takšnih ponudnikov so ProtonMail, Tutanota in Lavabit (slednjega je uporabljal Edward Snowden in preko njega komuniciral z novinarji). Kljub visoki ravni varnosti naj bi tajne službe imele protokole za dešifriranje sporočil, vendar za to potrebujejo mnogo resursov in časa (Schneier, 2013).
- **Spletni brskalniki –** Preko spletnih brskalnikov se v največji meri zbirajo podatki o našem obnašanjem na spletu, iskanju ključnih besed v iskalnikih in nakupovalnih navadah. Spletne strani te podatke uporabljajo za ciljano trženje. V določenih primerih so tovrstne prakse (trženje na podlagi ključnih besed) prenesli v ponudnike spletne pošte (na primer Gmail), kjer na podlagi analize naših komunikacij prikazujejo oglase oceni našega potrošniškega vedenja ustreznih produktov ali storitev. Brskalnik, ki uspešno onemogoča nadzor spletnega obnašanja je brskalnik TOR (angl. The Onion Router), ki preko razpršenih paketov večkrat enkriptiranih podatkov na principu delovanja veriženja blokov, podatke pripelje do končne destinacije. Ironično je to, da je ta koncept izumila prav vlada ZDA z namenom omogočanja svobodne komunikacije aktivistom iz držav, v katerih je prisotna represija. Primarna funkcija tega brskalnika je zakritje sporočila in identitete sporočevalca in onemogočanje njegovega nadzora.
- **Navidezna zasebna omrežja** (angl. Virtual Private Network, v nadaljevanju VPN) – Programi za navidezna zasebna omrežja nam s pomočjo šifriranj IP naslovov omogočajo zakritje naše dejanske lokacije. Njihovo funkcijo bi lahko opisali kot nekakšen dodaten požarni zid.

Slika 9: Razlika med normalno internetno povezavo in VPN



Vir: ICO Services (2017).

Kadar uporabljamo internet brez dodatne zaščite, se naša identiteta in početje zabeleži na strežnikih ponudnika spletnih storitev (na primer Telekom Slovenije ali Amis). Naš IP naslov se nato na podlagi informacije ponudnika izpiše na spletnih straneh, do katerih dostopamo.

VPN učinkovito rešuje to težavo, saj še pred posredovanjem informacij ponudniku šifrira poslane podatke. Šifrirani podatki v naslednji fazi potujejo do VPN strežnika, ki je lahko kjerkoli na svetu. Šele s tega strežnika podatki potujejo na spletne strani, katere ne prejmejo uporabnih podatkov o naši pravi lokaciji ali identiteti.

Povezovanje računalnikov na internetu omogoča dostop do oddaljenih podatkov, to pa pomeni, da postanejo naši podatki dostopni drugim. Poznamo 2 načina povezovanja računalnikov v sistem, ki se med seboj razlikujeta po stopnji tveganja in dostopnosti (Kelly & McKenzie, 2002):

1. **Internet** – Odprti sistem, ki nam omogoča dostop do podatkov kjerkoli po svetu. To pomeni višjo raven tveganja vdora in potrebo po višji ravni zaščite, saj smo tudi sami

dostopni vsem uporabnikom v omrežju. Posamezni računalnik imenujemo »otok elektronskih podatkov«, ki ima postavljene točno določene meje dostopa do njih. Ko se računalnik poveže z internetom, pa so te meje podrte in njegova varnost postane ogrožena. Učinkovita raven enkripcije nam omogoča zaščito podatkov in otežen dostop nepooblaščenih oseb do njih.

2. **Intranet** – Zaprti sistem, ki deluje znotraj organizacij. Čeprav gre v tem primeru za bolj varno delovanje vključenih računalnikov, je velika pomanjkljivost dostopnost do podatkov izven sistema. Kot smo spoznali v analizi vloge enkripcije pri varnosti, je vedno prisotna »trade-off« izbira, ki nam določa zahteve glede na tip podatkov (Aiello, 2018). Tudi Intranet ni popolnoma varen, saj lahko tretje osebe preko šibkih členov znotraj sistema vdrejo vanj, zato je potrebno vpeljati varovala, ki reagirajo že ob prvi zaznavi nepooblaščenega vdora in tako preprečijo škodo, ki bi nastala, če bi tretja oseba lahko dostopala do vseh uporabnikov in njihovih podatkov.

3.2 Konkurenčne prednosti podjetij, ki uporabljajo kriptografijo

Rast trga kibernetske varnosti (predvsem po nedavnih razkritij vdorov v velike tehnološke korporacije, kot so Sony Pictures, Anthem in T-Mobile) je zgolj eden izmed pokazateljev prihodnosti spletne varnosti, ki bo temeljila na kriptografskih principih. Vrednost panoge je zrasla z 1.3 milijard $ leta 1996 na več kot 100 milijard $ leta 2015 z napovedmi vrednosti 170 milijard $ leta 2020 (Macri, 2015). Kriptografska tehnologija koristi tako uporabnikom, kot tudi ponudnikom in ima pomembno vlogo pri gospodarski rasti. Vrednost trga enkripcijskih programov naj bi leta 2021 dosegla vrednost skoraj 9 milijard $

Skrb za varnost vseh vrst podatkov je danes večja kot kadarkoli prej, tega pa se zavedajo tako podjetja, kot tudi stranke. V drugem poglavju sem ugotovil, da utegnejo biti finančne posledice vdorov v sisteme velikih korporacij enormne, zato podjetja vedno več sredstev namenjajo varnosti njihovih informacijskih sistemov. Ugotovimo lahko, da je pomen enkripcijske tehnologije v sodobnih gospodarstvih ogromen in da pozitivno vpliva na gospodarsko rast. Avtorji nedavnih raziskav o pomenu enkripcije so v le-te vključili skoraj vsako pomembno povezavo med kriptografijo gospodarskimi panogami. Vključili so spletno bančništvo, investicije, zaposlovanje, zavarovalništvo in e-poslovanje. Te panoge skupaj so med letom 1994 in 2009 po letnih prihodkih zrasle s 100 mio $ na kar 250 milijard $ (Macri, 2015).

Konkurenčne prednosti kot rezultat uporabe tovrstnih tehnologij, so naslednje:

- **Večja diferenciacija**

Podjetja z učinkovito varnostno infrastrukturo signalizirajo strankam, da si resno prizadevajo zavarovati njihove podatke. Stranka, ki se zaveda, kako pomembno je informacijska varnost, bo tako prej izbrala podjetje, ki ji zagotavlja ustrezno raven le-te.

- **Povečanje prihodkov, prejetih s strani strank z občutljivimi podatki**

Stranke, ki se ukvarjajo s posebno občutljivimi podatki, kot na primer zdravstvene ustanove, organi pregona ali tajne službe, za svoje potrebe včasih potrebujejo zunanje izvajalce in najvišjo raven varnosti. Podjetja lahko v primeru, da imajo višjo raven varnosti kot ostala, pričakujejo dodatne prihodke s strani strank z občutljivimi podatki in posledično višje dobičke.

- **Zagotovitev varnega odstopa od poslovnega sodelovanja strankam brez zadržanja njihovih podatkov**

Ta prednost je v možnosti zagotovitve strankam, da bodo v primeru odstopa od pogodbe njihovi podatki odstranjeni iz baz podatkov. Stranke se tako zavarujejo pred nepričakovanimi dogodki ali konflikti, ki bi bili posledica zlorabe neodstranjenih podatkov.

- **Odpornost proti kraji poslovnih skrivnosti konkurentov**

Višja raven varnosti podatkov pomeni tudi, da imamo boljšo zaščito poslovnih skrivnosti pred našimi konkurenti. Včasih se razkritja skrivnosti podjetij končajo celo s propadom le-teh. Potrebno je poskrbeti za dobro izdelan načrt dostopa do takšnih občutljivih podatkov. Dober primer je recept za Coca-Colo, katerega naj bi poznali zgolj dve osebi, ki pa ne smeta biti hkrati ob istem času na letalu, saj bi se skrivnost lahko za vedno izgubila v primeru letalske nesreče.

- **Zagotovitev izpolnjevanja varnostnih standardov regulatorja (države)**

Tukaj pravzaprav ne gre za konkurečno prednost, gre bolj za ustrezanje zakonu in za prikazovanje podjetja kot organizacije, ki ji lahko varno zaupamo naše podatke. Podjetja, ki upoštevajo zakonske zahteve in hitro spreminjajoče se varnostne strandarde, so v očeh strank videna kot podjetja, ki upoštevajo tudi ostale zakone in poslovanje z njimi ne predstavlja tveganja.

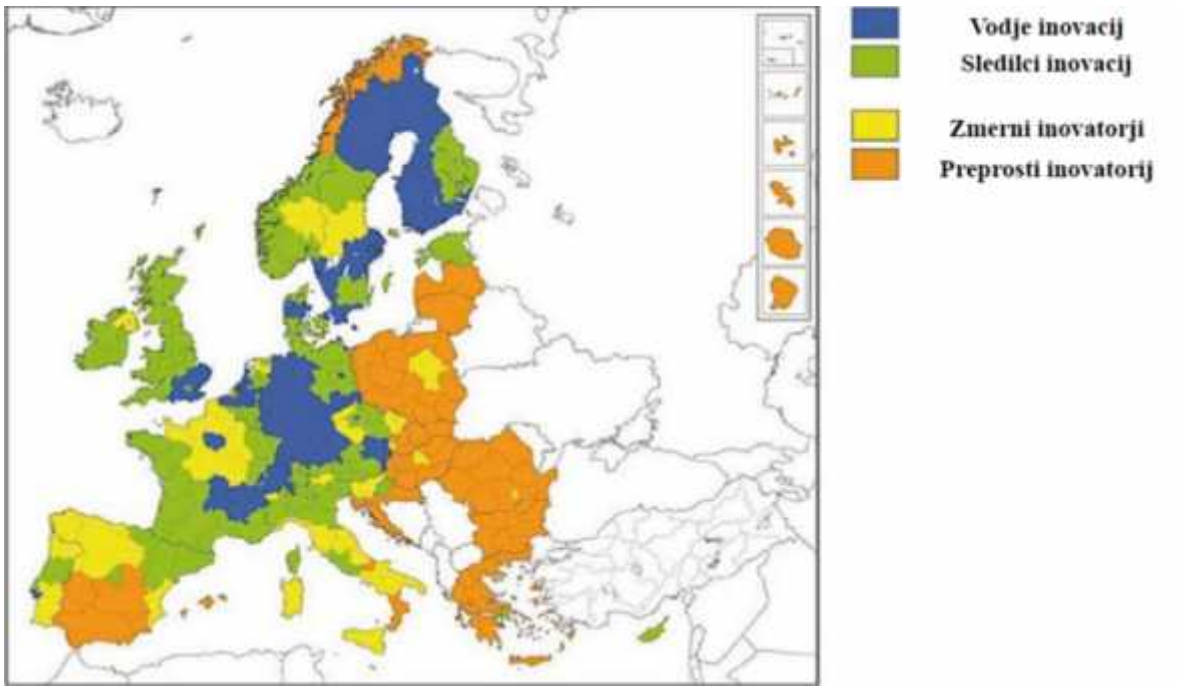
Zanimivo dejstvo glede uporabe enkripcije v poslovnem svetu je, da se večina vključenih strank sploh ne zaveda njenega obstoja, ker se jim zdi samoumevno, da so platforme, kot so na primer Amazon, Ebay in Overstock, varne ter odporne proti napadom in kraji njihovih podatkov. Dejstvo je, da brez šifrirnih protokolov, kakršna sta SSL (angl. Secure Socket Layer) in TLS (angl. Transport Layer Security), te platforme ne bi obstajale oziroma bi obstajale z nezavarovanimi praktično vsemi podatki, vključno s podatki o in transakcijah.

3.3 Vpliv inovacijske ravni družbe na razvoj enkripcijskih tehnologij

Varstvo podatkov zaradi posrednega vpliva na skoraj vsako panogo lahko analiziramo tudi v povezavi z inovacijsko ravnjo družbe in količino sredstev, ki jih ta družba namenja raziskavam in razvoju. Ko analiziramo inovacijsko raven v gospodarstvih razlikujemo med

štirimi različnimi tipi inovatorjev. Za primer vzemimo gospodarstva Evropske Unije, kjer so razlike med njimi na področju inovacij še vedno precejšnje.

Slika 10: Faze inovacijskih ravni evropskih gospodarstev leta 2014



Vir: European Commission (2015).

Problem evropskih gospodarstev je neenakomeren razvoj vzhodnega in zahodnega dela. To se odraža na ravni tehnološke razvitosti gospodarstva in posledično tudi na ravni varnosti podatkov pred potencialnimi napadi. Če želimo doseči ustrezno raven te varnosti, je potrebno vlagati v razvoj tehnologije in ne zgolj prevzemati obstoječo tehnologijo, ki se dokaj hitro izkaže kot zastarela in neučinkovita. Zaradi visokih finančnih vložkov, ki so potrebni za ta razvoj, je potrebno sodelovanje in vsem zagotovljen dostop do znanja in literature.

Gospodarstva, ki so kot vodje inovacij že prepoznala potenciale novih razvijajočih se tehnologij, kakršni sta biometrična in kvantna enkripcija, bodo odigrala pomembno vlogo pri postavljanju ustreznih varnostnih standardov in temeljev za nove načine zagotavljanja varnosti. Sklepamo lahko, da bodo zaradi teh zaščit takšna gospodarstva uživala mnoge konkurenčne prednosti, ki bodo izhajale iz varnosti njihovih podjetij in prebivalstva. Poleg tega bodo verjetno tudi prejemala prihodke od izvoza teh tehnologij v druge, manj razvite države.

3.4 Pomen kriptografije za državne institucije

Enkripcija in z njo povezana tehnologija imata pomemben vpliv na gospodarsko rast in varnost praktično vseh informacijskih sistemov v državi. V večini primerov je ta vpliv

posreden, na primerpreko višje ravni varnosti, tajnosti, zasebnosti ali standardizacije informacijskih arhitektur. Tehnologija, povezana z enkripcijo, se uporablja v vseh večjih sektorjih javnih sistemov, kot so:

- **Vojska**

Vloga kriptografije pri rasti in varnosti vojaške industrije je ogromna. Omogoča namreč ščitenje zelo občutljivih podatkov o vojaških skrivnostih, zaposlenih v vojski in komunikaciji med njimi. Zanimivo dejstvo je, da je ameriška vojska avtor večine široko uporabljenih protokolov in standardov, kakršna sta DES ali SSL, ter platform, kakršna je TOR (angl. The Onion Router – najbolj razširjena platforma za dostop do t.i. Deep Web-a, preko katerega se s pomočjo kriptovalute Bitcoin izvajajo kriminalne aktivnosti). Vojaška industrija uporablja še bolj šifrirano enkripcijo od enkripcije pri standardnih sistemih, imenovano enkripcija vojaškega nivoja (angleško »Military-grade encryption«). S tem izrazom označujemo standard AES-256 (angl. Advanced Encryption Standard), ki je prvi javnosti dostopen ključ za zaščito podatkov najvišje tajnosti,ki je odobren s strani NSA (Guillory, 2017).

Enkripcija poleg varnosti prinaša tudi dodaten vir prihodkov preko izvažanja enkripcijske tehnologije v druge države. To je postalo mogoče šele po umiku stroge prepovedi izvoza tovrstne tehnologije leta 1992. Danes v ZDA takšne omejitve določa Ministrstvo za industrijo in varnost (angl. Bureau of Industry and Security – BIS), nanašajo pa se predvsem na izvoz omenjenih tehnologij v tvegane države in na prodajo le-teh domnevnim terorističnim skupinam.

- **Zdravstveni informacijski sistemi**

Porast informatizacije zdravstva in naraščajoče število napadov na podatke pacientov kaže na potrebo zdravstvenih ustanov po boljšem in bolj varnem delovanju njihovih sistemov. Poleg standardnih izboljšav in informatizacije poslovanja, kot so e-recepti in povezani sistemi zdravstvenih podatkov o pacientih, se v zdravstvu že pojavljajo bolj napredne, na enkripciji temelječe oblike sistemov, kot so celovite rešitve in računalništvo v oblaku.

Zdravstvene ustanove so dolžne zagotavljati in vzdrževati visoko raven varnosti podatkov pacientov in zaposlenih, da lahko sploh konkuriraj na trgu, kljub temu pa nekatere še vedno večino izdatkov namenjajo omrežjnim in končnim rešitvam, kot pa enkripciji. Uporaba tehnologij, kot so »Big Data«, »Internet of Things« in računalništvo v oblaku, zahteva primerno zaščito le-teh, ki je ni mogoče zagotoviti brez enkripcije. Peter Galvin, podpredsednik podjetja Thales E-Security, ki se ukvarja z varnostnimi rešitvami za podjetja, je izjavil: »Podjetja morajo investirati v t.i. oblikovano zasebnost obrambnih mehanizmov,primer česar je enkripcija,za učinkovito zaščito občutljivih podatkov in intelektualne lastnine, in gledati na varnost kot na podlago posla, ki omogoča grajenje zaupanja med partnerji in kupci.«

Pomembno je poudariti, da so ustanove v ZDA do dolžne vzpostaviti primerno raven varnosti podatkov, saj obstaja zakonska podlaga HIPAA (angl. Health Insurance Portability and Accountability Act), katera natančno določa zakonske zaščite vseh zdravstvenih podatkov posameznikov. Gre za podatke, ki se nahajajo tako v elektronski, kot tudi pisni ali govorni obliki, imenujejo pa se zaščiteni zdravstveni podatki – PHI (angl. Protected healthcare information) (U.S. Department of Health & Human Services, 2017).

⁾ Izobraževalni informacijski sistemi

Inštitut Ponemon ocenjuje, da se v povprečju 26% vseh organizacij sooča z možnostjo vdora v podatke, izobraževalne ustanove pa postajajo vedno bolj ranljive (Apricorn, 2016)**.** Ne gre zgolj za podatke o ocenah in za gradiva, ampak tudi za podatke o kreditnih karticah, vozniških dovoljenjih, naslovih, telefonskih številkah, ipd. Poleg navedenega imajo te ustanove v nekaterih primerihv lasti tajne podatke državnih služb, poslovne skrivnosti in vojaške skrivnosti, ki jih prejmejo v raziskovalne namene (Apricorn, 2016).

Nemalo šol se znajde v situaciji, ko zaradi zaščite velikih količin podatkov nanje pritiskajo institucije, ki zahtevajo določeno raven varnosti. Poleg tega so dolžne spoštovati in izvajati strogo postavljene standarde, kot so na primer standardi glede varstva osebnih podatkov,standardi glede varstva zdravstvenih podatkov in standardi glede varstva podatkov o kreditnih karticah.

Izobraževalne ustanove, ki ne zagotovijo ustrezne ravni varnosti in ne uporabljajo enkripcije, tvegajo izrek visokih kazni za nespoštovanje zakonov, izrečene s strani države, in tudi morebitne tožbe. Takšni sistemi so idealna tarča napadalcev, saj podatki o študentih vsebujejo vse potrebne podatke za krajo njihove identitete. S pridobitvijo teh podatkov imajo kibernetski kriminalci prosto pot do povzročitve resne škode ali oskrunitve ugleda. Takšnim situacijam se je možno izogniti z upoštevanjem in izpolnjevanjem ustreznih standardov glede enkripcije in z vpeljavo dodatnih varnostnih elementov Kot smo že prej omenili, se je nemogoče izogniti nemoralnim in dejanjem ljudi in njihovi malomarnosti, katerih na more preprečiti nobena oblika tehnološke zaščite. Ponemonova študija je pokazala, da je prav tveganje nemoralnih dejanj in malomarnosti zaposlenih glavna skrb ustanov. Kar 51 % ustanov je izrazilo skrb glede takšnih dejanj in malomarnosti zaposlenih, sledita jim skrb glede dejavnosti kibernetskih kriminalcev s 35 % in glede odpovedi sistemov z 19 %. Pri tem je potrebno poudariti, da malomarnosti zaposlenih ne smemo mešati z namerno krajo podatkov s strani zaposlenih, katere angleško imenujemo »malicious insiders« (angl. Malicious – škodljiv, insider – oseba, ki je del organizacije, in ima zato dostop do podatkov) (Apricorn, 2016). 19 % ustanov skrbijo dejanja te skupine, ker s svojega računalnika lahko dostopajo do velike količine zaupnih podatkov šolskega sistema.

3.5 Pomen kriptografije za finančne institucije

Vsaka elektronska transakcija je danes izvedena s pomočjo enkripcije. Brez uporabe slednje bi lahko kdorkoli z osnovnim znanjem programiranja pridobil naše podatke in jih zlorabil. Podjetja, ki ponujajo finančne storitve, se že dolgo časa borijo v »dirki« ponujanja najsodobnejših digitalnih tehnologij. Medtem so državni organi zaposleni z preprečevanjem uporabe trdnih modelov šifriranja, saj naj bi bila z njimi ogrožena nacionalna varnost in onemogočen nadzor (Ginsberg, 2016).

7. septembra 2006 je 5 finančnih ustanov, med katerimi sta tudi American Express in Visa, formiralo odbor PCI SSC (angl. Payment Card Industry Security Standards Council), ki je postavil temelje standardu PCI DSS (angl. Payment Care Industry Data Security Standard). Njegovo poslanstvo je trajnostni razvoj, izboljšanje in uspešna vpeljava varnostnih standardov za zaščito podatkov (PCI Security Standards Council, 2017). Njihovi standardi vključujejo preverjene modele enkripcije in izsledke študij o novih tehnologijah. Vsebujejo tudi smernice za uspešno implementacijo varnostnih produktov.

Finančne ustanove upravljajo ogromne zbirke občutljivih podatkov, ki so shranjene na strogo varovanih strežnikih. Količina podatkov, ki jih kot stranke delimo z njimi, je indikator našega zaupanja v njihovo varnost. Banke, katerim stranke zaupajo več podatkov, niso deležne zgolj večjega ugleda na trgu, ampak so tudi bolj produktivne, saj lahko za analizirajo več različnih vidikov vedenja potrošnikov in temu primerno prilagodijo svojo ponudbo. Enkripcija jim pri tem zagotavlja prednosti pred konkurenti in ustrezno raven varnosti.

Digitalizacija je v zadnjih 10 letih za finančni sektor storila veliko dobrega, od poenostavitve procesov do prihrankov. Zgolj procesi digitalizacije računov naj bi povzročili 60–80 % nižje stroške, saj podatki o računih ne zahtevajo več fizične oblike (Ginsberg, 2016). Uporabnikova izkušnja je postala fokus ponudnikov finančnih storitev in temelj za razvoj slednjih. Finančne ustanove so pod konstantnim pritiskom uporabnikov po boljših in bolj varnih platformah, razvoj in implementacija katerih zahteva čas in sredstva. Enkripcija pomaga pri vpeljavi varne komunikacije med bankami in strankami in pri vpeljavi stroškovno bolj učinkovitih sistemov. Po uspešni vpeljavi lahko banke uporabnikom ponudijo kvalitetnejšo in varnejšo storitev.

3.6 Pomen kriptografije za podjetja in problematika njene vpeljave

Podjetja se med seboj razlikujejo tudi po tem, kako se soočajo s spremembami, ki so v določenih primerih nujno potrebne. Tako so na primer morali vsi zaposleni v zdravstvu v Sloveniji prevzeti sistem E-receptov, vse pravne in fizične osebe, ki zaračunavajo DDV, pa uvesti davčne blagajne. V tem poglavju bom raziskal, kateri so najpogostejši problemi pri vpeljavi enkripcijske tehnologije v informacijske sisteme podjetij in zaradi česa te problemi nastanejo. Kljub temu, da so mi evropske institucije dale jasno vedeti, da je enkripcija še

kako pomembna, sem med raziskavo ugotovil, da se mnoga podjetja še vedno ne zavedajo njenega vpliva na varnost podatkov in posledično na konkurenčnost teh podjetij.

3.6.1 Splošni problemi vpeljave enkripcije v podjetja

Podjetja varnosti osebnih podatkov še vedno namenjajo premalo pozornosti. Ne zavedajo se namreč, da je varnost njihove informacijske infrastrukture pogoj za ustvarjanje konkurenčnih prednosti in zaupanja njihovih strank. Čeprav je enkripcija prisotna že od samega pojava informacijske tehnologije, se njene metode spreminjajo. Vzrok temu je poleg ostalega povečano število napadov in vdorov. Zaradi tega se pojavljajo novi, bolj učinkoviti načini zaščite. Podjetja, ki se ukvarjajo zinformacijskimi tehnologijami, imajo zaradi svojega tehničnega znanja o enkripciji na področju varnosti in implementacije novih rešitev prednost, saj delujejo v poslovnem okolju, kjer so spremembe nekaj običajnega. V tem delu se bomo osredotočili na poročilo ameriškega podjetja Townsend Security, ki že 20 let deluje na področju enkripcijskih storitev, in podjetjem nudi rešitve, ki jim omogočajo skladnost z varnostnimi standardi regulatorjev.

Probleme organizacij na tem področju je možno razčleniti na 5 različnih področij (Townsend Security Inc., 2017):

1. Vpeljava enkripcije bo vplivala na zmogljivost naših sistemov

Nekatera podjetja so mnenja, da bi vpeljava enkripcije povzročila nižjo zmogljivost njihovih sistemov. Enkripcija sicer vpliva na to, vendar je ob njeni pravilni implementaciji ta vpliv minimalen, zgolj med 2 in 4 %. Ta vpliv pa je odvisen tudi od strukture organizacije in količine podatkov, s katerimi upravlja. Pri velikih podjetjih je zato potrebno vložiti čas in sredstva za analizo potreb in izbiro primernih rešitev. Problemi nastanejo, kadar se podjetja odločijo, da bodo sama razvila in vpeljala varnostno rešitev, ki vključuje enkripcijo. Vpeljava enkripcije je zahtevna, zato mnogokrat podjetjem, ki to skušajo storiti sama, slednja bolj vpliva na zmogljivost sistema, kot bi vplivala v primeru, da bi to vpeljavo prepustili specializiranemu podjetju. Pomembno je tudi, da vodilni v podjetjih razumejo delovanje enkripcije in da nekaj izdatkov namenijo tudi rezervnim strežnikom za enkripcijske ključe, ki služijo kot varovalni element v primeru sesutja sistema ali vdora. Te strežniki namreč zagotavljajo nemoteno delovanje njihovih platform tudi kadar pride do vdorov.

2. Management enkripcijskih ključev je preveč zapleten

V preteklosti je ta trditev držala. Ne le, da je bilo njihovo upravljanje zapleteno, bilo je tudi zelo drago in časovno potratno. Včasih je bilo potrebno ob vsaki potrebni spremembi znova razviti nov sistem in ni bilo odprtih platform in standardov, kakršnih poznamo danes. Danes ponudniki tovrstnih storitev poskrbijo, da so ključi generirani avtomatično in ne zahtevano nikakršnega programiranja. S pomočjo SDK-ja (angl. Software Development Kit),

standardiziranih knjižnjic programskih jezikov in t.i. »ready-to-use« programov na uporabniški strani, je postala vpeljava enkripcije bistveno hitrejša in cenejša. Z vidika uprabnika torej uporaba enkripcije ne zahteva več nikakršnega programiranja. Ocenjevanje odpornosti in vpeljava managerja ključev, sta danes poleg ostalega tudi s pomočjo oblaka in virtualnih strojev lahko nalogi, opravljeni v nekaj minutah. Pri ocenjevanju odpornosti je pomembno sistem testirati s standardom NIST FIPS 140-2, ki je eden najvišjih standardov na področju varnostnih sistemov.

3. Skrb pred izgubo enkripcijskega ključa

Eden največjih strahov; izguba enkripcijskega ključa, je brez rezervnih ključev nočna mora vsakega vzdrževalca ali CIO-a. To ima največje posledice, kadar gre za velike količine občutljivih podatkov, ki vsebujejo podatke o kreditnih karticah, osebne podatke in podobno. Šifrirani podatki brez ustreznega ključa za dešifriranje so namreč popolnoma neuporabni. Ta problem v veliki meri rešuje ustrezen manager ključev, ki je strojni zaščitni modul (največkrat v skladu z omenjenim zgornjim standardom NIST FIPS 140-2) na virtualnem stroju ali v oblaku. Ta modul upravlja lokacije ključev, oblikovanje novih ključev, njihov izbris, njihovo rotacijo in njihovo shranjevanje. Ta model ne ščiti zgolj ključev, ampak tudi podatke, saj so podatki in njihovi ključi shranjeni na različnih lokacijah.

4. Management ključev je predrag

V preteklosti so projekti implementacije managementa ključev zahtevali mesece in mesece preden so bili vzpostavljeni, potrebno pa je bilo tudi veliko finančnih sredstev, ki so lahko močno vplivala na finančno stanje podjetja, zato so bili takšni projekti včasih malim in srednjim podjetjem nedosegljivi. Danes so te rešitve bistveno cenejše in njihova implementacija traja zgolj nekaj dni. Poleg tega pa nam ugleden ponudnik tovrstnih rešitev ne bo v pogodbo skril dodatnih stroškov ali provizij ter nam zaračunal več kot je bilo dogovorjeno. Nudil nam bo tudi brezplačno pomoč pri izbiri primerne rešitve za naše podjetje. Podjetja se morajo zavedati, da se sicer načini zaščite podatkov spreminjajo, vendar lahko sklepamo, da »hekerji« ne bodo nikdar prenehali, kar pomeni, da so vsi sistemi potencialne žrtve napadov.

5. Število zaposlenih v oddelku informatike v našem podjetju je prenizko

Vpeljava enkripcije je postala tako preprosta, da v večini primerov sploh ne potrebujemo strokovnjakov zanjo, oziroma je njihova vloga minimalna. Seveda je to odvisno od velikosti in infrastrukture obstoječih sistemov. Najlažji način je implementacija v oblaku, katera je tudi stroškovno najbolj učinkovita. Za dosego primerne ravni varnosti je ključen učinkovit manager ključev.

3.6.2 Pomanjkanje testiranj in primerov dobrih praks

V drugem poglavju sem raziskoval področja uporabe enkripcije, kjer smo ugotovili, da je njena uporaba skoraj na vsakem koraku in pri skoraj vsaki transakciji, ki jo opravimo. Zaključimo lahko, da je enkripcija v uporabi že tako dolgo, da jo obravnavamo kot uveljavljen način zaščite. Kljub temu pa so načini enkripcije, ki sem jih navajal, vedno manj odporni pred napadi, saj je skupaj z njihovim razvojem napredoval tudi razvoj kibernetske kriminalitete, iz česar izhaja potreba po naprednejših načinih zaščite.

Problem novih novih in domnevno bolj varnih načinov, kakršna je kvantna enkripcija, je pomanjkanje dolgoročnih testiranj zanesljivosti in odpornosti pred napadi. Prav tako se pojavljajo pomisleki glede njene učinkovitosti. V prvem delu smo namreč ugotovili, da morajo za uspešno implementacijo in delovanje biti izpolnjeni vsi trije omenjeni pogoji: tajnost gesel, popolnost in točnost kvantne teorije in zanesljivost naprav v kvantnem sistemu komunikacij (The Optical Society, 2013). Eden izmed ekonomskih faktorjev je tudi cenovna neučinkovitost, saj ta način zaščite še ni doživel takšnega razcveta, kot ga je tradicionalni simetrični ali asimetrični način enkripcije. Kvantna enkripcija namreč zahteva posebne komunikacijske kanale, preko katerih se podatki v obliki fotonov prenašajo od pošiljatelja do prejemnika. Izgradnja takšnih kanalov je danes relativno draga, kljub temu pa nekatera gospodarstva, kot sta ZDA in Kitajska (slednja naj bi že imela zgrajeno 2000 km dolgo omrežje med Pekingom in Šanghajem) že uspešno gradijo tovrstna omrežja. Če znanstvenikom uspe vpeljava, naj bi se te kanali razširili tudi na satelite, in tako imeli doseg po celem svetu.

Skeptiki kvantne enkripcije menijo, da obstaja možnost, da je predpostavka o varnosti njenega delovanja že bila ovržena. Sklicujejo se na skupino raziskovalcev iz Massachusetts Institute of Technology, ki naj bi izkoristili prepletenost fotonov in brez vpliva na verigo komunikacije na podlagi tega prišli do določenih informacij. Gre sicer za zelo majhno količino informacij, menijo pa, da bi z izpopolnjeno tehniko bilo mogoče izvesti bolj učinkovit vdor.

Strah pred vpeljavo novih nepreverjenih načinov zaščite bo v podjetjih vedno prisoten, vprašanje je le, katera podjetja bodo prva sprejela tveganje in posledično tudi uživala pozitivne posledice. Profesor računalniške znanosti z Yale University, ki med drugim poučuje tudi kriptografijo in informacijsko varnost, je izjavil: »Največji varnostni problem danes predstavljajo ljudje. Najlažji način za vdor v sistem je podkupiti ali prevarati nekoga, ki nam omogoči dostop do podatkov. Tudi najbolj sodobne tehnologije tega ne morejo preprečiti.« Temu problemu mnoga podjetja namenjajo premalo pozornosti in večino časa in denarja namenjajo zgolj tehničnemu vidiku varnostne rešitve. Glede kvantne kriptografije je mnenja, da jo je sicer mogoče razbiti, vendar bi to bilo možno zgolj, če bi s tem kršili osnovne zakone fizike. Kvantna teorija namreč temelji na principih fizike in ne matematike, kot tradicionalni načini enkripcije.

3.6.3 Zagotavljanje varnosti osebnih in poslovnih podatkov podjetja ob odhodu zaposlenih, zadolženih za varnostno infrastrukturo

Problemu odhajajočih zaposlenih podjetja pogosto namenjajo premalo pozornosti. Tudi v primerih, kadar je fluktacija zaposlenih nižja, obstajajo večja varnostna tveganja, kadar nekdo, ki je imel v lasti enkripcijske ključe ali druge občutljive podatke, zapusti to organizacijo (Buttler, 2017). Govorimo o moralnem hazardu zaposlenega, ki je bil odpuščen, dal odpoved ali pa se zgolj upokojil. Ne glede na raven zvestobe in pripadnosti zaposlenih morajo podjetja poskrbeti za vpeljavo varnostnih varovalk in politik organizacije, ki za zaposlenega stopijo v veljavo že prvi dan zaposlitve.

Načini za znižanje ravni varnostnih tveganj v času tranzicije zaposlenih:

1. **Sledenje dostopa** – Potrebno je natančno sledenje dostopu zaposlenih in učinkoviti preprečitvi le-tega ob odhodu.
2. **Centralizirana gesla** – Ustvariti sistem upravljanja gesel, ki je voden s strani podjetja, in ki omogoča dostop zaposlenim brez dejanskega gesla.
3. **Podrobna dokumentacija** – Vsak dostop v bazo podatkov je zabeležen in nadzorovan. Takšno beleženje aktivnosti služi tudi kot zavarovanje pri morebitnih tožbah ali sporih, ki bi lahko škodovali organizaciji.
4. **Pravilno beleženje** – Imeti učinkovit sistem beleženja, ki nas v trenutku nepooblaščenega dostopa ali škodljivih aktivnosti opozori na to in nam omogoči hitro ukrepanje. Tak sistem beleži tudi shranjevanje podatkov s strani zaposlenih.
5. **Predhodno načrtovana incidentna politika** – Mnoga podjetja doživijo napade zaradi popolne odsotnosti tovrstnih načrtov, ki pa so nujni za zagotavljanje poslovne kontinuitete in zavarovanja pred novimi vdori.

3.7 Pogled institucij na pomembnost kriptografije

Zanimalo me je, kako institucije, ki delujejo na področju informacijske varnosti, vidijo obravnavano problematiko, in kakšno je njihovo mnenje o njeni pomembnosti ter prihodnjih izzivih na področju informacijske varnosti. Glavni instituciji sta Evropski supervizor za varnost podatkov in agencija ENISA, ki se ukvarja z kibernetsko varnostjo in kriminaliteto. Želel sem tudi mnenje privatnega sektorja v Sloveniji, a po mnogih poskusih nisem prejel odgovora.

3.7.1 Pogled EDPS-a

Obrnil sem se tudi na Evropskega supervizorja za zaščito podatkov (EDPS) in nanj naslovil vprašanja, ki bi mi pomagala še bolj natančno razumeti problematiko enkripcije in njen vpliv na varnost podatkov, zakonodajo in informacijsko okolje znotraj EU.

G. Courtenay Mitchell, predstavnik EDPS-a za komunikacije, mi je pojasnil, da je enkripcija na lestvici pomembnosti za zagotovitev varnosti (točkovanje med 1 in 10) na najvišjem mestu, torej ima 10 točk, in da je edini način za zagotovitev tajnosti in integritete elektronskih komunikacij. Povprašal sem ga tudi o biometrični in kvantni enkripciji.Obravnava ju kot nadgradnjo obstoječih konceptov in ne kot zamenjavo. Poleg tega obe tehnologiji še nista na trgu za množično uporabo, potrebne bodo dodatne raziskave, preden se bo to zgodilo.

G. Mitchell pri informacijski infrastrukturi in njenih kapacitetah opozarja tudi na različne ravni razvoja znotraj EU, kar se neposredno navezuje tudi na inovacijsko raven v družbi, in na lokacijo infrastrukture (mestno okolje, podeželjsko okolje, ipd.)

Glede varnosti podatkov je opaznih mnogo trendov, ki kažejo na to, da se bo potreba po obdelavi podatkov povečevala. Primeri teh trendov so: sledenje internetnim aktivnostim, povezani senzorji na Internetu stvari (angl.. Internet of things), snemanje s strani avtonomnih naprav (droni, samovozeča vozila, ipd.), in druge nove tehnologije, ki omogočajo sledenje v vsakdanjem življenju (videokamere, prepoznava obraza, idr.). Poleg privatnega sektorja bodo okrepili zbiranje in obdelavo podatkov tudi transportna in mejna kontrola, policija in drugi organi pregona. Povečanja kapacitet, ki omogočajo zbiiranje in obdelavo podatkov, bodo mogoča z že predstavljeno »big data« tehnologijo in z umetno inteligenco.

Pri enkripciji zamenjava zastarelih mehanizmov zaščite na vseh področjih še vedno ni popolnoma pod nadzorom in bo potrebno dodatno usklajevanje ter analiza za uspešno vpeljavo novih načinov zaščite.

3.7.2 Pogled agencije ENISA

Na to agencijo sem preko kontaktnega obrazca naslovil konkretna vprašanja glede njihovega pogleda na enkripcijo, vendar po kar nekaj poskusih odgovora nisem prejel. Kasneje sem na njihovi spletni strani odkril dokument, v katerem so predstavili njihov pogled na enkripcijo osebnih podatkov in podali smernice za prihodnost.

Poročilo označuje informacije kot drugo najpomembnejše sredstvo podjetij, takoj za človeškimi viri. Večina informacij je danes v digitalni obliki, takšna oblika pa ima poleg očitnih prednosti eno poglavitno pomanjkljivost: zaščito. Enkripcija po mnenju agencije rešuje ta problem in skupaj z tajnostjo podatkov postaja norma za organizacije (ENISA, 2016).

Pri analizi žvižgaštva in masovnega nadzora prebivalstva sem ugotovil, da je v digitalni dobi zelo tanka meja med varnostjo in zasebnostjo. Poročilo agencije omenja tudi to področje in obravnava pomembnost ravnotežja med legitimnostjo posredovanja tajnih služb in zakonodaje, ki preprečuje prestrego informacij in pravico do zasebnosti posameznikovih komunikacij.

ENISA sodeluje tudi z Europolom z namenom izboljšanja zakonodaje, ki ureja področje varnosti in pooblastil obeh agencij. Ustanovili so strokovno skupino, imenovano »Vpliv kriptografije na organe pregona« (angl. The impact of cryptography on Law Enforcement Agencies«). Europol ima tudi poseben sektor strokovnjakov, ki so zadolženi za kibernetsko kriminaliteto.

Sklepi in ugotovitve poročila: Agencija vidi kriptografijo kot sredstvo, ki je elektronski ekvivalent pečatu ali podpisu. V primerih terorističnih groženj in organiziranega kriminala organi pregona in tajne službe zahtevajo obhod teh varnostnih sistemov. Kljub upravičenim zahtevam kakršnokoli omejevanje kriptografskih orodij naredi sistem ranljiv in lažje dostopen, to pa predstavlja tveganje kriminalnih aktivnosti in zmanjšuje raven zaupanja v elektronske storitve. Takšne prakse bi škodovale podjetjem in evropskemu prebivalstvu.

Tehnologija se zelo hitro spreminja, zato je vprašljivo, ali bodo nove rešitve res tako učinkovite, glede na to, da tudi kriminalci lahko razvijejo svoje enkripcijske sisteme, preko katerih nemoteno komunicirajo. To predstavlja problem za organe pregona, saj morajo takšne sisteme najprej identificirati, nato pa še dešifrirati. Potrebna je analiza prednosti novih tehnologij v primerjavi s potencialno škodo, ki bi nastala zaradi oteženega dostopa do informacij kriminalnih združb.

3.7.3 Pogled privatnega sektorja

Želel sem tudi mnenje privatnega sektorja, vendar kljub temu, da sem želel izvedeti zgolj nekaj osnovnih informacij, ki bi se navezovale na mojo temo, nisem dobil odgovora. Pri podjetju Data.si so mi odgovorili da se ne ukvarjajo z takšnimi vprašanji, kar pa je nenavadno glede na to, da so glavni organizatorji seminarjev z naslovi, kot so »Zaščita osebnih podatkov za 21. stoletje« in »GDPR (angl. General Data Protection Regulative) – ste pripravljeni?«

Kontaktiral sem tudi mnoga druga podjetja, vendar od nikogar nisem dobil odgovora.

3.8 Predlogi za učinkovitejšo implementacijo kriptografske tehnologije

Po ugotovitvah je v podjetjih prisotno slabo poznavanje varnostnih produktov in pomanjkanje izobraževanja zaposlenih na to temo. Menim, da bi bilo potrebno več pozornosti nameniti razumevanju delovanja in osnovnih konceptov enkripcije. Še vedno obstaja relativno velik delež organizacij, ki so toge in nenaklonjene spremembam. To se odraža v njihovem odporu proti novim tehnologijam in posledično odrekanju konkurenčnim prednostim, ki bi jih s tem lahko pridobila.

Največji strah podjetij je vpliv enkripcijske tehnologije na njihovo učinkovitost, ta strah pa izvira ravno iz pomanjkanja znanja o njej. Tudi državne institucije delno nosijo krivdo za to. Menim, da so gospodarske zbornice dolžne obveščati poslovne subjekte o novih načinih zaščite, saj gre za področje, ki vpliva na vse udeležence v gospodarstvu. Za višjo raven

varnosti bi morale vsako leto izdajati ustrezne brošure, kjer bi bili opisani in predstavljeni novi načini zaščite in primeri dobre prakse, podprti z izsledki raziskav. Primerno bi bilo tudi vključiti smernice za t.i. **strategijo enkripcije**, ki bi podjetjem predstavila pozitivne učinke razvoja takšnih strategij.

Izobraževanje podjetij in zaposlenih bi poleg varnostnih konceptov moralo vključevati širši vidik informacijske varnosti, ki bi vključeval konkurenčne prednosti, zmanjševanje moralnega hazarda in ustvarjanje boljše poslovne klime v organizacijah. Podjetja bi se tako bolj zavedala potenciala in pozitivnih učinkov vpeljave. Organizirati bi bilo potrebno tudi delavnice, kjer bi se zaposlene poučilo o varnostnih tveganjih, in jih naredilo bolj osveščene o pomenu enkripcije podatkov in potrebe po njej. Nekatera podjetja, ki delujejo v panogi informacijske tehnologije, to že počnejo, saj se zavedajo, kako pomembno je, da zaposleni ne obravnavajo informacijske varnosti kot samoumevne.

Zaposlenim v organizaciji je potrebno s ustreznimi primeri pokazati, da so varnostna vprašanja pomembna tema in da kraja podatkov predstavlja resna tveganja za organizacijo. Raven informacijske varnosti lahko zvišamo že s standardnim paketom varnostnih programov, ki so nameščeni v vsakem računalniku organizacije in katerih uporaba je za vse obvezna. Nemogoče je pričakovati, da bi vsak zaposlen samoiniciativno uporabljal programe za enkripcijo datotek, virtualna omrežja in specifične antivirusne programe. Sposobnosti in znanje o informacijski varnosti zaposlenih bi lahko preverjali z testi socialnega inženiringa in tako ugotovili, ali je poznavanje le-te v organizaciji zadovoljivo, ali ne.

SKLEP

Zagotavljanje varnosti osebnih podatkov predstavlja vedno večji izziv, tako s tehničnega, kot tudi z zakonskega vidika. Razumevanje delovanja kriptografskih tehnologij in njihovih prednosti je pomemben del njihove uspešne vpeljave in uporabe teh prednosti. Podjetja morajo stremeti k informiranju vodstva in zaposlenih o problematiki varnosti pomembnih podatkov in preprečevati moralni hazard zaposlenih, ki ga tudi najbolj sodobna enkripcijska zaščita ne odpravlja.

Na eni strani se pojavljajo vprašanja glede ravni zaščite in zastarelosti obstoječih načinov zagotavljanja le-te, ki postajajo neučinkoviti in ranljivi. Razvoj novih konceptov zahteva visoke investicije in je trenutno počasnejši od napredka industrije. Določena gospodarstva temu problemu namenjajo več pozornosti kot ostala. Pričakujemo lahko, da bodo postavila ustrezne standarde in pokazala prakse uspešne implementacije. Če se izkaže, da je biometrična enkripcija res tako učinkovita kot kažejo raziskave, bo le-ta predstavljala pomemben korak naprej na področju varnosti podatkov pred napadoi (Alberto Torres, Bhattacharjee & Srinivasan, 2015). Enako velja za kvantno enkripcijo.

Na drugi strani je problematika zakonodaje in državne regulacije varnostnih produktov. Zakoni o varstvu podatkov na internetu, ki ni geografsko omejen, nimajo skoraj nobenega

učinka, oziroma je ta minimalen. Kljub določenim zakonom, ki naj bi veljali tudi na internetu, je slednji slabo reguliran. Med drugim je za to kriv tudi osnoven koncept medmrežja, katerega glavno načelo je, da je internet dostopen celemu svetu, in da na njem ne obstajajo nikakršne meje. Mnogi poskusi regulacije so se izkazali za neuspešne, saj so bili dojeti kot poseg v zasebnost ljudstva. Za višjo raven urejenosti interneta bo potrebno globlje razumevanje problematike škodljivih praks in spoštovanja zasebnosti. Državni organi bodo morali v prihodnje pri oblikovanju zakonov, ki regulirajo področje varstva podatkov na internetu, vključiti več interesnih skupin in širšo javnost.

Višja raven osveščenosti javnosti o pomenu enkripcije je ključna za učinkovito postavitev standardov, ki bodo v bodoče določali obliko varnostne infrastrukture. Potrošniki se morajo izobraziti o nevarnostih brezglavega deljenja podatkov, pri čemer morajo svojo vlogo odigrati državne institucije, in s projekti kot je ARCADES, poskrbeti za poznavanje te problematike že v zgodnjih fazah življenja.

Enkripcija podatkov je trenutno najvarnejši način zaščite osebnih podatkov, vendar njena uspešna implementacija predstavlja velik izziv. Potreba po varnosti podatkov postaja vedno bolj pomembna, česar se mnoga velika podjetja že zavedajo. Za učinkovito zaščito je potrebno več kot zgolj postaviti standarde in se ravnati po njih. Potrebna bo proaktivnost in sodelovanje med podjetji, ki skrbijo za razvoj enkripcije, in podjetji, ki upravljajo večje zbirke podatkov. Pri tem morajo svojo vlogo odigrati tudi vladne institucije in zagotoviti podjetjem neovirano vpeljavo in razvoj enkripcijskih sistemov.

LITERATURA IN VIRI

1. Aiello, S. (2018, 15. marec). What role does encryption play in data security? *Online Tech.* Pridobljeno iz Pridobljeno 9. maja 2018 iz http://www.onlinetech.com/resources/videos/what-role-does-encryption-play-in-data-security
2. Ajibuwa, F. O. (2009). *Data and Information Security in Modern Day Businesses.* Honolulu, Hawaii: Atlantic International University.
3. Alberto Torres, W. A., Bhattacharjee, N. & Srinivasan, B. (2015). Privacy-preserving biometrics authentication systems using fully homomorphic encryption. International *Journal of Pervasive Computing and Communications*, *11*(2), 151–168.
4. *An international benchmark of the world's safest - and riskiest - data locations*. Pridobljeno 23. junija 2018 iz https://www.artmotion.eu/risk-map/
5. Apricorn. (2016). *Encryption in Education. Poway*. California: Apricorn.
6. Audin, G. (2015, 2. julij). *The Network Impact of Big Data.* Pridobljeno 12. maja 2018 iz https://www.nojitter.com/post/240170228/the-network-impact-of-big-data
7. *Arcades project.* Pridobljeno 9. maja 2018 iz http://www.arcades-project.eu
8. Banka Slovenije. (2013). Rast e-bančništva. *Bilten Banke Slovenije, XXII*(3), 45.

9. Bankrate Corporation. (2017, 10. marec). 11 data breaches that stung US consumers. *Bankrate*. Pridobljeno 9. maja 2018 iz http://www.bankrate.com/finance/banking/us-data-breaches-12.aspx
10. Batelle, D. H. (2017, 19. januar). *The Future of Security: Zeroing In On Un-Hackable Data With Quantum Key Distribution*. Pridobljeno 9. maja 2018 iz https://www.wired.com/insights/2014/09/quantum-key-distribution/
11. BSA, The Software Alliance. (2018, 28. februar). *Encryption: Why it matters:* Pridobljeno 9. maja 2018 iz http://encryption.bsa.org/
12. Buttler, P. (2017). E*nsure security employees quit without taking passwords, encryption keys.* London: SC Media.
13. Chandramouli, R., Iorga, M. & Chokhani, S. (2013). *Cryptographic Key Management Issues & Challenges in Cloud Services*. National Institute of Standards and Technology Interagency .
14. Chirgwin, R. (2018, 9. avgust). IBM's homomorphic encryption accelerated to run 75 times faster. *The register*. Pridobljeno 9. maja 2018 iz https://www.theregister.co.uk/ 2018/03/08/ibm_faster_homomorphic_encryption/
15. Cohen, F. (2017, 20. januar). *A short history of cryptography*. Pridobljeno 9. maja 2018 iz http://www.all.net/books/ip/Chap2-1.html
16. *Crisp project*. Pridobljeno 9. maja 2018 iz http://www.crisp-projec.eu
17. D'Agapeyeff, A. (1949). *Codes and Ciphers - A History of Cryptography.* London: Oxford University Press.
18. Dungan, J., Waytz, A. & Young, L. (2015). The psychology of whistleblowing. *Current Opinion in Psychology, 6*, 129–133.
19. *Encryiption in the Cloud.* Pridobljeno 23. junija 2018 iz https://image. slidesharecdn.com/incloudweencrypt-151028003627-lva1-app6892/95/in-cloud-we-encrypt-ghc15-8-638.jpg?cb=1446052194
20. Enterprivacy Consulting Group. (2018, 28. februar). Pridobljeno 9. maja 2018 iz https://enterprivacy.com/wp-content/uploads/2017/03/Categories-of-personal-information_web-612x480.jpg
21. European Commission. (2015). *Regional Innovation.* Pridobljeno 23. junija 2018 iz http://ec.europa.eu/enterprise/policies/innovation/policy/regional-innovation/index_en.html .
22. European Commission. (2017, 12. januar). *Data collection: What is legal?* Pridobljeno 9. maja 2018 iz http://ec.europa.eu/justice/data-protection/data-collection/legal/ index_en.htm
23. *European Data Protection Supervisor*. Pridobljeno 18. junija 2018 iz https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/cache/offonce?lang=sl
24. European Union Agency for Network and Information Security – ENISA. (2016, december). *ENISA's Opinion Paper on Encryptio.* Pridobljeno 9. maja 2018 iz https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/ enisas-opinion-paper-on-encryption

25. European Union Agency for Network and Information Security. (2018, 22. marec). *ENISA Strategy 2016-2020*. Pridobljeno 18. junija 2018 iz https://www.enisa.europa.eu/publications/corporate/enisa-strategy
26. GDPR Portal. (2018, 26. julij). *The Regulation.* Pridobljeno 18. junija 2018 iz https://www.eugdpr.org/the-regulation.html
27. Ginsberg, J. (2016). *Solving the Encryption Conundrum in Financial Services*. Toronto, ON: EchoWorx.
28. Greenwald, G. (2014). *No place to Hide, Edward Snowden, the NSA and the U.S. Surveillance state.* Macmillan: Metropolitan Books.
29. Grut, O. W. (2016). *GOLDMAN SACHS: 5 practical uses for blockchain*. Pridobljeno 18. junija 2018 iz http://uk.businessinsider.com/goldman-blockchain-beyond-the-hype-practical-uses-2016-5
30. Guillory, T. (2017, 24. marec). *Military grade encryption* [objava na blogu]. Pridobljeno 18. junija 2018 iz https://blog.dashlane.com/dashlane-explains-military-grade-encryption/
31. Hardesty, L. (2014). *Raising cryptography's standards*. Cambridge, MA: MIT News.
32. Heimdal Security. (2017). *End to end encryption comparison* [objava na blogu]. Pridobljeno 23. junija 2018 iz https://heimdalsecurity.com/blog/wp-content/uploads/end-to-end-encryption-comparison.png
33. Hosie, R. (2017, 16. januar). Ashley Madison hacking: What happened when married man was exposed. *The Independent*. Pridobljeno 18. junija 2018 iz http://www.independent.co.uk/life-style/love-sex/ashley-madison-hacking-accounts-married-man-exposes-cheating-website-infidelity-rick-thomas-a7529356.html
34. *How Blockchain works*. Pridobljeno 23. junija 2018 iz https://cdn.datafloq.com/cms/2016/08/18/how-blockchain-works-3.png .
35. ICO Services. (2017). *VPN*. Pridobljeno 23. junija 2018 iz http://www.icoservices.com/images/_global/vpn_EN.jpg
36. Informacijski pooblaščenec Republike Slovenije. (2015). *Letno poročilo 2015.* Pridobljeno 9. maja 2018 iz https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2015_web.pdf
37. Intuit Online Security Center. (2017, 19. januar). *Phishing, Pharming, Vishing, and Smishing.* Pridobljeno 18. junija 2018 iz https://security.intuit.com/index.php/protect-your-information/phishing-pharming-vishing-and-smishing
38. I-SCOOP. (2018, 26. julij). *GDPR encryption: what you should know and what you do not know*. Pridobljeno 18. junija 2018 iz https://www.i-scoop.eu/gdpr-encryption/
39. Kelly, G. & McKenzie, B. (2002). Security, privacy, and confidentiality issues on the Internet. *Journal of medical internet research, 4*(2), e12.
40. Khatri, A. & Budhiraja, I. (2013). E-Banking: Cryptography with unique identity. *International Journal of Research in IT & Management, 13*, 36–41.
41. Macri, G. (2015). *Economists Say Encryption 'Significantly' Boosts Economy*. Pridobljeno 18. junija 2018 iz http://www.insidesources.com/economists-say-encryption-significantly-boosts-economy/

42. Manish Potey, M., Dhote, C. A. & Deepak, H. S. (2016). Homomorphic Encryption for Security of Cloud Data. *Procedia Computer Science, 79*, 175–181.
43. Marous, J. (2016). The biometric future of banking. *The Financial Brand*. Pridobljeno 18. junija 2018 iz https://thefinancialbrand.com/61449/biometric-banking-password-trends/
44. Maxim Integrated. (2017). *Cryptography in Software or Hardware - It Depends on the Need*. Pridobljeno 9. maja 2018 iz https://www.maximintegrated.com/en/app-notes/index.mvp/id/5421
45. Miller, M. (2008). *Data Theft: How Big a Problem*. London: Pearson.
46. Mitsubishi Electric. (2017). *CRY2*. Pridobljeno 23. junija 2018 iz http://www.mitsubishi electric.com/company/rd/research/highlights/communications/images/cry2.gif
47. Nakamoto, S. (2008). *BitCoin: A Peer-to-Peer Electronic Cash System*. Pridobljeno 18. junija 2018 iz https://bitcoin.org/bitcoin.pdf
48. Office of the Privacy Commissioner New Zealand. (2017, 6. januar). *Purpose for collection of personal information.* Pridobljeno 18. junija 2018 iz https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-principles/purpose-for-collection-of-personal-information-principle-one/
49. PCI Security Standards Council. (2017, 5. april). *Securing the future of payments together.* Pridobljeno 18. junija 2018 iz https://www.pcisecuritystandards.org
50. Poitras, L. (Režiser). (2014). *Citizenfour* [Film].
51. Reitman, J. (2013). Bradley Manning Explains His Motives. *Rolling Stone.* Pridobljeno 18. junija 2018 iz https://www.rollingstone.com/politics/politics-news/bradley-manning-explains-his-motives-98563/
52. Ridley-Siegert, T. (2015). Data privacy: What the consumer really thinks. *Journal of Direct, Data and Digital Marketing Practice, 17*, 30–35.
53. Ruhr-Universitaet-Bochum. (21. Januar 2017). Encryption technologies for the era of quantum computers: Effective protection for microdevices. *ScienceDaily.* Pridobljeno 18. junija 2018 iz https://www.sciencedaily.com/releases/2015/12/151218085927.htm
54. Schneier, B. (2013). NSA surveillance: A guide to staying secure. *The Guardian*. Pridobljeno 18. junija 2018 iz https://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance
55. She, W. & Thiraisingham, B. (2007). Security for Enterprise Resource Planning Systems. *Information Systems Security*, 152–163.
56. Simic, B. (2016). The Promise And Challenges Of Biometrics. *Forbes*. Pridobljeno 18. junija 2018 iz https://www.forbes.com/sites/forbestechcouncil/2016/12/22/the-promise-and-challenges-of-biometrics/
57. Swenson, C. (2008). *Modern Cryptanalysis: Techniques for Advanced Code Breaking.* Indianapolis, IN: Wiley Publishing, Inc.
58. The Optical Society. (2013, 20. januar). Just how secure is quantum cryptography? ScienceDaily. Just how secure is quantum cryptography? *ScienceDaily* Pridobljeno 18. junija 2018 iz http://www.sciencedaily.com/releases/2013/05/130528122435.html

59. Tibouchi, M. (2017). *Fully Homomorphic Encryption over the Integers: From Theory to Practice.* Pridobljeno 23. junija 2018 iz https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa5.html
60. Townsend Security Inc. (2017, 28. marec). *Overcome the Top 5 Fears of Encryption & Key Management:* Pridobljeno 18. junija 2018 iz https://townsendsecurity.com/sites/default/files/Overcome-Top-5-Fears.pdf
61. Tsarenko, Y. & Tojib, D. R. (2009). Examining customer privacy concerns in dealings with financial institutions. *Journal of Consumer Marketing, 26*(79, 468–476.
62. Tyldum, M. (Režiser). (2014). *The Imitation* Game [Film].
63. U.S. Department of Health & Human Services. (2017, 24. marec). *Summary of the HIPAA Privacy Rule* Pridobljeno 9. maja 2018 iz https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/
64. UC Berkeley. (2017, 8. marec). *Data Classification Standard*. Pridobljeno 9. maja 2018 iz https://security.berkeley.edu/data-classification-standard
65. Varuh človekovih pravic Republike Slovenije. (2017, 21. januar). *Varovanje osebnih podatkov.* Pridobljeno 18. junija 2018 iz http://www.varuh-rs.si/o-instituciji/podrocja-dela-varuha/varstvo-osebnih-podatkov/
66. Walsh, D. (2017, 20. januar). *The Decentralized Internet: How To Make Decentralized Websites and Apps.* Pridobljeno 9. maja 2018 iz http://cryptorials.io/decentralized-internet-make-decentralized-websites-apps/
67. Ward, M. (2013). *How the modern world depends on encryption*. London: BBC News.
68. *World's Biggest Data Breaches.* Pridobljeno 23. junija 2018 iz http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
69. Zaharia, A. (2017, 2. marec). The best encrypted messaging apps you can (and should) use today. *Heimdal Security.* Pridobljeno 23. junija 2018 iz https://heimdalsecurity.com/blog/the-best-encrypted-messaging-apps/

PRILOGE

Priloga 1: Intervju z predstavnikom Varuha RS.

1. **Ali obstaja oddelek Varuha RS, ki je zadolžen zgolj za področje interneta in če ja, katere so njegove naloge?**
   Takega oddelka pri Varuhu človekovih pravic RS nimamo.

2. **Ali menite, da imate za opravljanje svojih pristojnosti in nalog zadostno zakonsko podlago ali ne? Če ne, kje se to najbolj odraža?**

Varuh je ustavna kategorija (je opredeljen v ustavi) v 159. členu:

»Za varovanje človekovih pravic in temeljnih svoboščin v razmerju do državnih organov, organov lokalne samouprave in nosilcev javnih pooblastil se z zakonom določi varuh pravic državljanov.

Z zakonom se lahko za posamezna področja določijo posebni varuhi pravic državljanov.«

Zakon o varuhu človekovih pravi (ZVarCP – A) nam za opravljanje nalog daje zadostna pooblastila.

Kar pa zadeva varstvo osebnih podatkov je s spremembami in dopolnitvami Zakona o varstvu osebnih podatkov (ZVOP-A), ki jih je sprejel Državni zbor RS na seji dne 26. 6. 2001, veljati pa je začel 24. 7. 2001, varuh človekovih pravic dobil zadolžitev tudi kot neodvisna institucija za varstvo osebnih podatkov.

Naloge

- neposrednega nadzora spoštovanje predpisov o varstvu osebnih podatkov pri upravljavcih zbirk in pri uporabnikih osebnih podatkov,
- spremljanje oziroma nadziranje dela Inšpektorata za varstvo osebnih podatkov,
- svetovanja v zadevah na tem področju,
- sodelovanja v postopkih sprejemanja predpisov in
- opravljanja drugih naloge na podlagi zakona

je opravljal do sprejema Zakona o varstvu osebnih podatkov ZVOP-1 15.07.2004 in začetka njegove veljavnosti 01.01.2005. ZVOP-1 je za varovanje osebnih podatkov zadolžil Informacijskega pooblaščenca, Varuh človekovih pravic RS pa ima po tem zakonu le še te pristojnosti.

3. **Kaj je po Vašem mnenju največja pomanjkljivost zakonskih podlag za varstvo podatkov na spletu?**

Varuh se s problematiko varstva osebnih podatkov obravnava, če nam pobudniki zatrdijo, da so bile kršene njihove pravice v odnosu do državnih organov, organov lokalne skupnosti in nosilcev javnih pooblastil. Načeloma ne analiziramo zakonodaje iz vidika njene pomanjkljivosti, razen, če ugotovimo, da so določene kršitve, ki jih zaznamo iz pobud,

sistemskega izvora oziroma posledica nedovršene zakonodaje. Takrat predlagamo, da vlada oziroma državni zbor zadeve uredi na način, da so spoštovane pravice ljudi v odnosu do države in njenih organov.

Predpisi tudi ne določajo za Varuha, da mora podajati predhodna mnenja o usklajenosti določb predlogov zakonov ter ostalih predpisov z zakoni in drugimi predpisi, kot to na primer za Informacijskega pooblaščenca določa ZVOP-1 v 48. členu: "Državni nadzorni organ daje predhodna mnenja ministrstvom, državnemu zboru, organom samoupravnih lokalnih skupnosti, drugim državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov ter ostalih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke."

Varuh je o problematiki varstva oseb pred posegi v osebnostne pravice, storjene preko spletnih vsebin pisal v letnem poročilu za leto 2014 (stran 43–45). Takrat je ocenil, da veljavna ureditev ne omogoča učinkovitega pravnega varstva žrtev posegov v osebnostne pravice, storjene prek spletnih vsebin. Več o tem si lahko preberete v omenjenem letnem poročilu.

4. Ali beležite poraste prijav na področju kršitev osebnih podatkov?

Varuh ne opaža porasta, temveč je število pobud vsako leto približno na istem nivoju. Posebno vprašanje pa je njihova utemeljenost: Varuh iz prejetih pobud redko oceni, da je šlo za kršenje pravic iz naslova varstva osebnih podatkov.

Obravnavane zadeve v 2014: 66
Obravnavane zadeve v 2015: 61 /// Število utemeljenih (kjer smo ugotovili kršitev): 8
Obravnavane zadeve v 2016: 50 /// Število utemeljenih: 2
Obravnavane zadeve v 2017: 69 /// Število utemeljenih: 3

Varuh se trudi o zaznani problematiki veliko bolj kot prek golih številk poročati prek opisov posameznih primerov iz njegove prakse, saj bi si vsaj načeloma bralec moral na ta način lažje ustvariti sliko o njej.

5. Kako izgleda izvrševanje pristojnosti Varuha RS na tem področju v praksi? Se večina vprašanj preseli na sodišča? Kolikšen del prijav se preseli na Evropska sodišča?

Kot še rečeno, varuh obravnava pobude, ki jih nanj naslovijo pobudniki. Oceni, ali je šlo pri tem za kršenje njihovih pravic s strani države, predlaga odpravo kršitev oziroma druge ukrepe, pač glede na vsebino posameznega primera. Primere iz področja si lahko pregledate tudi na tej povezavi.

6. Ali obstajajo kakršnikoli konflikti med pristojnostmi Varuha človekovih pravic in IP-jem?

Načeloma ne - že zato ne, ker skladno z veljavno zakonodajo (tudi na področju varstva osebnih podatkov) velja subsidiarnost Varuhovega posredovanja, kar pomeni, da naj bi

Varuh posredoval šele, če pristojni organi (v tem primeru IP in nato eventualno še sodstvo) pri svojem delu zagrešijo kakšno nepravilnost, zaradi katere pri teh pristojnih organih lahko posreduje (takšna možnost se je glede IP na primer nakazovala v situaciji, o kateri smo pisali na str. 92 letnega poročila 2016, št. 1.7-5/2016).

7. **Kateri so po Vašem mnenju največji izzivi na področju zagotavljanja varstva osebnih podatkov na internetu v prihodnosti?**
   Sprejemanje ustrezne pravne regulacije v zvezi s čedalje bolj zmogljivimi algoritmi, ki služijo obdelavi osebnih podatkov - in potem tudi njeno učinkovito izvrševanje. Seveda bodo še vedno ostali aktualni tudi problemi kot so kraja identitete, lažno predstavljanje ali zvábljanje (phishing), trgovanje z osebnimi podatki, nadzor nad hramba zbranih podatkov, idr.

Priloga 2: Intervju z predstavnikom EDPS.

1. **Ali ima EDPS poseben oddelek, ki se ukvarja samo z problematiko podatkov na internet?**

EDPS je nadzorni organ za varstvo osebnih podatkov evropskih institucij. Nadzoruje obdelavo osebnih podatkov s strani institucij EU in svetuje institucijam EU o vprašanjih na področju varstva osebnih podatkov v zvezi s političnimi, pravnimi in operativnimi ukrepi.

Internet igra pomembno vlogo v številnih primerih, s katerimi se ukvarja EDPS, tako v operativnem kot v političnem kontekstu. Skupaj približno dve tretjini osebja EDPS delujeta na primerih s svojim pravnim, tehnološkim in drugim strokovnim znanjem. Eno od ekip sestavljajo večinoma samo strokovnjaki s področja tehnologije in varnosti.

2. **Kako bi opisali trenutno stanje v EU na področju varnosti osebnih podatkov?**

V EU je vzpostavljen celovit pravni okvir glede varnosti osebnih podatkov. Eden glavnih instrumentov je GDPR, ki vsebuje posebne določbe o varovanju osebnih podatkov in obveznostih poročanja o varnostnih incidentih, ki vključujejo na osebne podatke.

Poleg GDPR so pravni instrumenti za nekatere sektorje tudi varnostne določbe, kot so Direktiva o zasebnosti in elektronskih komunikacijah ter Uredba o obdelavi osebnih podatkov s strani institucij EU.

Informacijsko varnost zajemajo tudi drugi pravni instrumenti (ključne infrastrukture, radijski terminali itd.).

Še vedno obstaja zaskrbljenost glede praktičnega izvajanja ustreznih varnostnih ukrepov s strani nekaterih organizacij. S popolno uvedbo GDPR-ja, ki se približuje maja, bi morala biti motivacija in pripravljenost organizacij, da sprejmejo ustrezne varnostne ukrepe za osebne podatke, višja.

3. **Ali menite, da imate za opravljanje svojega dela zadostne pristojnosti, ali bi bili bolj učinkoviti če bi jih imeli več?**

EDPS je pozval zakonodajalca EU, da zaključi zakonodajni postopek o uredbi o varstvu podatkov za institucije EU in novo uredbo o zasebnosti in elektroniki. Za oba predloga je Evropski parlament že sprejel stališče. Za uredbo institucij EU ima Svet tudi stališče, glede razlik pa trenutno še potekajo pogajanja. Za uredbo o zasebnosti in elektronskih komunikacijah se Svet še ni strinjal o skupnem stališču ali splošnem pristopu.

Takoj ko bosta oba instrumenta sprejeta, bo okvir EU za varstvo zasebnosti in osebnih podatkov veliko bolj celovit.

4. **Kako velik vpliv bi imel GDPR na tehnološka podjetja, prebivalstvo in državne institucije? Ali menite, da bo vplival na prihodke podjetij?**

GDPR v celoti začne veljati 25. maja 2018. Zavedamo se, da se številne organizacije, ki obdelujejo osebne podatke, že pripravljajo na njegovo implementacijo. Ustrezni in pravočasni prevzem zmanjšuje stroške in daje organizaciji zaupanje v zaščito pred sankcijami zaradi neskladnosti in škode zaradi zlorabe osebnih podatkov.

Nekatere organizacije so se oprle na operacije, ki niso v celoti spoštovale zakonodaje EU o varstvu podatkov. Če svojih postopkov ne bodo prilagodili pravočasno, se lahko soočijo s težavami. Nekatere organizacije so opravile operacije, ki ne bodo več v skladu z zakonodajo EU. Lahko se odločijo, da bodo te operacije ustavili ali premaknili svoja podjetja izven EU.

Na splošno GDPR zahteva napor organizacij, vendar zmanjšuje birokracijo za podjetja, z namenom zmanjšanja njihovih stroškov.

5. Ali menite, da bi EU morala imeti poseben urad zadolžen zgolj za kibernetsko kriminaliteto in internetno zakonodajo?

ENISA je agencija za kibernetsko varnost EU. Na poti je predlog, ki ji bo zagotovil več pristojnosti na področju kibernetski varnosti.

Pred nekaj leti je bil kot del Europola ustanovljen Kompetenčni center za kibernetske kriminalitete.

6. Ali vidite evropsko informacijsko infrastrukturo kot konkurenčno v primerjavi z ostalim svetom? Kaj bi lahko storili, da jo izboljšamo?

To vprašanje v bistvu ne spada v pristojnost EDPS. Kakovost infrastrukture je v različnih delih EU drugačna. Tudi v drugih delih sveta se infrastruktura razlikuje med mestnimi in podeželskimi območji itd., zato je težko podati splošno primerjavo.

7. Kako pomembna je po vašem mnenju enkripcija za varstvo osebnih podatkov od 1 do 10 in zakaj?

Šifriranje je zelo pomembno (10) za transakcije in interakcije prek interneta, to je namreč edini način za zagotavljanje zaupnosti in celovitosti elektronskih komunikacij.

8. Ste že slišali za biometrično ali kvantno enkripcijo? Če da, kaj menite o njima?

Obe tehnologiji še nista na voljo na trgu v smiselnem obsegu. Dodali bi dodatne možnosti obstoječim orodjem, vendar jih ne bi mogli popolnoma nadomestiti. Zaradi kvantne tehnologije nekatere sedanje šifrirne sheme niso več varne in jih bo treba zamenjati.

9. Kateri so po vašem mnenju največji izzivi na področju varstva osebnih podatkov in enkripcijskih protokolov v EU v naslednjih letih?

Kar zadeva zasebnost podatkov, so opazni številni trendi, ki bodo povečali obdelavo osebnih podatkov, kot so sledenje internetnih transakcij in izmenjav, povezanih senzorjev (internet stvari), snemanje z avtonomnimi napravami (brezpilotna letala, samovozna vozila) in

nadaljnje povečanje tehnologije sledenja v resničnem življenju (nadzorne kamere, prepoznavanje obrazov itd.). Poleg zasebnega sektorja lahko organi kazenskega pregona, transportna podjetja in carinska kontrola poveča zbiranje in obdelavo podatkov. Možnosti obdelave in analize osebnih podatkov bodo podpirale velike podatkovne tehnologije (angl. Big data technology) in umetna inteligenca.

Kar zadeva enkripcijske protokole EU, zamenjava zastarelih mehanizmov za enkripcijo še vedno ni popolnoma pod nadzorom na vseh področjih.

Priloga 3: Intervju z predstavnikom Informacijskega pooblaščenca.

1. **Ali obstaja oddelek Informacijskega Pooblaščenca, ki je zadolžen zgolj za področje interneta in če ja, katere so njegove naloge?**

Informacijski pooblaščenec nima posebnega oddelka, ki bi bil pristojen samo za področje interneta. Nadzor nad izvajanjem ZVOP-1 izvajajo državni nadzorniki za varstvo osebnih podatkov, katerim po potrebi nudijo strokovno pomoč informatiki, ko gre za vprašanja, ki se nanašajo na informacijsko-komunikacijske tehnologije.

2. **Ali menite, da imate za opravljanje svojih pristojnosti in nalog zadostno zakonsko podlago ali ne? Če ne, kje se to najbolj odraža?**

Za opravljanje svojih nalog in pristojnosti imamo zadostne zakonske podlage, s težavami pa se soočamo, ko gre za upravljavce, ki so izven naše jurisdikcije, na primer podjetja, ki so registrirana v tujini in imajo tam svoje strežnike.

3. **Kaj je po Vašem mnenju največja pomanjkljivost zakonskih podlag za varstvo podatkov na spletu?**

Pri varstvu osebnih podatkov, ki se obdelujejo na spletu, je največja težava z vidika zakonskih podlag to, da splet ne pozna meja, in da se kršitelji lahko nahajajo v tretjih državah, kjer kot nadzorni organi težko ukrepamo.

4. **Kako izgleda izvrševanje pristojnosti IP-ja na tem področju v praksi? Se večina vprašanj preseli na sodišča?**

Odvisno o kakšnih primerih govorimo. Kolikor gre za upravljavce ali njihove pogodbene izvajalce, ki se nahajajo na našem ozemlju in obstaja sum kršitve ZVOP-1, imamo dovolj pristojnosti in vzvodov za ustrezno ukrepanje. Če gre za države znotraj EU/EGS lahko za ukrepanje zaprosimo kolege iz nadzornih organov v teh državah. Večje težave nastopijo, če se vsebina nahaja na strežnikih v tretjih državah (na primer Indija, Kitajska ipd.), kjer ni tovrstne zakonodaje o varstvu osebnih podatkov ne sorodnih nadzornih organov. Če govorimo o kaznivih dejanjih (na primer. kršitev tajnosti občil, vdori v informacijske sisteme ipd.), potem je za njihov pregon pristojna policija, ki ima tudi različne možnosti za mednarodno sodelovanje in pomoč, kot je Europol, Interpol in pa druge oblike meddržavnih sporazumov o delovanju na področju preiskave, odkrivanja in pregona kaznivih dejanj.

5. **Ali obstajajo kakršnikoli konflikti med pristojnostmi Varuha človekovih pravic in IP-jem glede pristojnosti?**

Takšnih konfliktov ne zaznavamo.

6. **Kateri so po Vašem mnenju največji izzivi na področju zagotavljanja varstva osebnih podatkov na internetu v prihodnosti?**

Izzive smo opisali v našem letnem poročilu (Informacijski pooblaščenec Republike Slovenije, 2015, str. 64 in naprej).