DIGNITAS
Revija za človekove pravice
Slovenian journal of human rights
ISSN 1408-9653

Ustavnost državnih posegov v zasebnost posameznika na internetu
Patrik Cassol

Article information:
To cite this document:
Cassol, P. (2015). Ustavnost državnih posegov v zasebnost posameznika na internetu, Dignitas, št. 67/68, str. 153-184.

Permanent link to this doument:
https://doi.org/ 10.31601/dgnt/67/68-16

Created on: 16. 06. 2019
To copy this document: publishing@nova-uni.si

Ustavnost državnih posegov v zasebnost posameznika na internetu[1]

Patrik Cassol

POVZETEK

Živimo v času hitrega razvoja tehnologije, kjer se spremembe dogajajo hitro in pravice kršijo dnevno. Govorim o vse razvijajoči se informacijski tehnologiji in vseh njenih prednostih ter slabostih. Prvih ne gre zanikati, druge pa so hujše, kot si jih je sam George Orwell zamislil med pisanjem svojega slovitega znanstvenofantastičnega romana 1984, ki govori o totalitarni državi nadzora in nasilja nad svojimi državljani. Obveščevalno-varnostne agencije so nove tehnike nadzora, pridobljene z razvojem tehnologije, s pridom uporabljale, niso pa se ob tem vprašale, ali je takšno delovanje v nasprotju z ustavo. Pravica do zasebnosti predstavlja pomemben gradnik naše svobode. Tako zasebnost kot svoboda sta namreč bistveni svoboščini in predstavljata temelj današnjih demokratičnih družb. Skozi celotno zgodovino so se ljudje zanju na vso moč borili in bili zanju celo pripravljeni dati svoje življenje.

Ključne besede: ustavnost in zakonitost, test sorazmernosti, pravica do svobode, pravica do zasebnosti, državni nadzor, množični nadzor, obveščevalno-varnostne organizacije, sodobna informacijska tehnologija

The constitutionality of state interference in the individual's right to online privacy

ABSTRACT

We live in a time of rapid digitalization, where changes happen quickly and the rights are violated daily. I am talking about

[1] *Članek je povzetek magistrske naloge Ustavnost državnih posegov v zasebnost posameznika na internetu.*

the information technology and all its advantages and disadvantages. The first cannot be denied, while the latter are worse than even George Orwell himself imagined, while writing his famous science fiction novel 1984, which talks about a totalitarian state of control and violence against its own citizens. Intelligence and security agencies advantageously applied new surveillance techniques, thanks to the evolution of technology, without asking themselves, if such actions are unconstitutional. Right to privacy embodies an important part of our freedom. Both, privacy and freedom are fundamental rights which represent the foundations of today's democratic societies. Throughout history people were fighting for them and even willing to die for them.

Keywords: constitutionality and legality, principle of proportionality, right to freedom, right to privacy, state interference, mass surveillance, intelligence and security agency, modern information technology

1. Uvod

Razvoj nas je popeljal do informacijske dobe, v kateri se nahajamo sedaj, kjer nič ni nemogoče. Oziroma kar je bilo včeraj nemogoče, je danes mogoče. Tako velja tudi za načine množičnega nadzora posameznikov, ki so sedaj postali mogoči zahvaljujoč sodobni tehnologiji. Obveščevalno-varnostne agencije so nove tehnike s pridom uporabljale, ob tem pa se niso vprašale, ali je takšno delovanje v nasprotju z ustavo. Pravica do zasebnosti predstavlja pomemben gradnik naše svobode. Ti dve svoboščini sta temelj današnjih demokratičnih družb in zanju so se ljudje v preteklosti na vso moč borili ter bili zanju celo pripravljeni dati svoje življenje. Trditve nekaterih, da nimajo ničesar za skrivati, ker ne počnejo ničesar narobe, so iz tega vidika zmotne. Postavi se namreč vprašanje: Če ne počnejo ničesar narobe, zakaj so potem nadzorovani? Kajti nadzorovani bi morali biti le tisti, ki dejansko počnejo nekaj narobe. Potrebno je biti previden, kajti kot je dejal William O. Douglas, Vrhovni sodnik ZDA in velikan ameriške pravne misli, ki je za ameriško svobodo in zasebnost verjetno naredil več kot dvesto let kongresne zakonodaje: »Zloraba oblasti, avtokracija in tema nikoli ne pridejo hipoma, vedno je vmesno obdobje mračenja, ko se dan počasi preveša v noč; biti moramo pozorni opazo-

valci okolja in varuhi luči, da ne postanemo nemočni ujetniki teme.«[2]

Članek raziskuje pravico do zasebnosti na področju sodobne informacijske tehnologije, njene omejitve s strani države in obveščevalno-varnostnih organizacij ter samo upravičenost tovrstnih omejitev. Pregled teorije in prakse, same zakonske in ustavne ureditve ter sodne prakse mednarodnih in nacionalnih sodišč nam bo pomagal odgovoriti na zastavljeno raziskovalno vprašanje: Ali državni posegi v posameznikovo svobodo in zasebnost z namenom varovanja nacionalne varnosti izpolnjujejo zahteve načela sorazmernosti? Kakšne izboljšave so mogoče ali celo potrebne na zadevnem področju? Z odgovori na ta vprašanja bomo ugotovili, ali sta bili načeli demokratične in pravne države spoštovani in nista zgolj še mrtve črke na papirju. Slednje je pomembno, kajti pokazalo nam bo, ali so posamezniki izgubili zaupanje v pravo in učinkovito varstvo njihovih pravic.

2. Pravica do zasebnosti

Pravica do zasebnosti je neposredno povezana z nadzorom in s tem z državnimi posegi vanjo. Ko nekdo izvaja nadzor nad nekom, s tem najverjetneje avtomatično posega v njegovo zasebnost. Sama opredelitev pravice do zasebnosti je izredno težavna. Široko razumevanje pravice do zasebnosti kot celote je sestavljeno iz štirih sektorjev, in sicer psihične, odločitvene, prostorske in informacijske zasebnosti.[3] Pravica do zasebnosti je temeljna človekova pravica, ki predstavlja enega izmed nepogrešljivih elementov človekove eksistence in varuje človeka pred državno oblastjo, javnostjo in drugimi posamezniki, je pravica biti sam z minimumom posegov v vse štiri sektorje te pravice.[4]

Ameriška ustava pravice do zasebnosti ne omenja eksplicitno. Ta je zgolj v obliki senc (ang. »penumbra«) vidna predvsem v četrtem amandmaju ameriške ustave. Obstoj pravice do zasebnosti je na tej podlagi skozi svojo sodno prakso razvilo Vrhovno sodišče ZDA. Kot temeljni primer mnogi citirajo zadevo Griswold v. Con-

[2] *J. Trampuš, Goran Klemenčič, strokovnjak za kazensko pravo in človekove pravice, http://www.mladina.si/44062/goran-klemencic-strokovnjak-za-kazensko-pravo-in-clovekove-pravice/ (zadnjič obiskano 27. 12. 2015)*
[3] *R. Lampe, Sistem pravice do zasebnosti, 2004, str. 31.*
[4] *Prav tam, str. 501.*

necticut iz leta 1965.[5] Med drugim so v določenih primerih priznanja pravice do zasebnosti citirali tudi določbe prvega, tretjega, petega, devetega in štirinajstega amandmaja.[6] Ameriška pravna praksa pravico do zasebnosti primarno razume kot pravico biti sam (»the right to be left alone«).[7]

V EU imamo več virov, ki zagotavljajo varstvo človekovih pravic in temeljnih svoboščin, med katere sodi tudi pravica do zasebnosti. Prvi vir je Listina EU o temeljnih pravicah (6. člen), drugi so ustave držav članic, tretji je EKČP (8. člen) in četrti mednarodne pogodbe za varstvo temeljnih pravic, katerih podpisnice so države članice. Pravna ureditev v evropskih državah in EU je drugačna od tiste v ZDA, saj gre tukaj za evropski kontinentalni pravni sistem, ki temelji na zakonih. Zato je pravica do zasebnosti tukaj ustavna kategorija in je izrecno zapisana v ustavah evropskih držav. Kar se tiče pravnega varstva EU je ta najprej izdala Direktivo o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Direktiva 95/46/ES). Nato je leta 2002 dodala novo direktivo za področje varovanja osebnih podatkov in komunikacijske zasebnosti, in sicer gre za Direktivo 2002/58/ES Evropskega parlamenta in Sveta o varstvu zasebnosti v elektronski komunikaciji, ki jamči obdelavo osebnih podatkov in varstvo zasebnosti na področju elektronskih komunikacij. Za to področje zasebnosti je potrebno omeniti tudi precej sporno Direktivo 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij. Sodišče EU jo je 8. aprila 2014 z združenimi zadevami Digital Rights Ireland & Seitlinger in drugi (C-293/12 in C-594/12) razglasilo za neveljavno. S tem je postavilo pomemben precedens k varstvu pravic posameznika do komunikacijske in informacijske zasebnosti na območju Evropske Unije.

Pravna ureditev pravice do zasebnosti je v Republiki Sloveniji dosledno urejena. Toplak v Komentarju Ustave pove, da je potrebno pravico do zasebnosti razumeti v tako imenovanem dualističnem konceptu – kot osebnostno pravico, ki je varovana z instrumenti civilnega prava, ter kot človekovo pravico (javnopravnega

[5] *Mullikin/Rahman, The Ethical Dilemma of the USA Government Wiretapping, IJMIT, No. 4 (2010), str. 33.*
[6] *D. Glancy, At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet, Santa Clara High Technology Law Journal, Iss. 2 (2000), str. 365–366.*
[7] *R. Lampe, 2004, str. 67.*

značaja), ki je varovana z ustavo in mednarodnopravnimi dokumenti.[8] Pravica do zasebnosti je zapisana v več členih Ustave RS in sicer: 35. členu (varstvo pravic zasebnosti in osebnostnih pravic), 36. členu (nedotakljivost stanovanja), 37. členu (varstvo tajnosti pisem in drugih občil) ter 38. členu (varstvo osebnih podatkov). Glede varstva pravice do zasebnosti v Republiki Sloveniji pride v poštev tudi 8. člen EKČP, saj je Republika Slovenija podpisnica mednarodne konvencije EKČP in tako ta na območju Republike Slovenije velja neposredno.[9] Prav tako pridejo v poštev zakoni, ki podrobneje opredelijo varstvo osebnih podatkov. V Republiki Sloveniji smo leta 1999 dobili Zakon o varstvu osebnih podatkov (ZVOP), katerega je leta 2005 nasledila novela ZVOP-1. Slednji vsebuje določbe o varstvu osebnih podatkov, določenih v evropski Direktivi o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (95/46/ES). Ne smemo iti mimo Zakona o Informacijskem pooblaščencu (ZInfP) iz leta 2005, s katerim je bil ustanovljen neodvisen državni organ – Informacijski pooblaščenec, med drugim pristojen za nadzor nad varstvom osebnih podatkov.

3. Omejitev pravic posameznika v korist širše družbe

Načeloma človekovih pravic in temeljnih svoboščin ni mogoče omejiti oziroma ni dovoljeno posegati vanje. V tem poglavju bodo navedeni primeri, kdaj in kako ter kakšni pogoji morajo biti izpolnjeni, da je mogoče na zakonski način omejiti pravice posameznikov v korist širše družbe. Država mora spoštovati pravico do zasebnosti posameznika in v tem sklopu opravljati določena dejanja. Gre za opravljanje dvojne funkcije države oziroma tako imenovane pozitivne obveznosti države. Prvič: s pravnimi akti mora omejiti svoje pristojnosti glede vmešavanja v posameznikovo izvrševanje pravice do zasebnosti in drugič: zagotoviti mora nemoteno izvrševanje pravice do zasebnosti in njeno pravno varstvo nasproti drugim posameznikom.[10] Bistveno vprašanje, ki nas tukaj zanima, je vprašanje konflikta posameznikove pravice do zaseb-

[8] *L. Toplak v: L. Šturm (urednik): Komentar Ustave Republike Slovenije, 2011, str. 368.*
[9] *To določa 8. člen URS, ki pravi, da se ratificirane in objavljene mednarodne pogodbe uporabljajo neposredno.*
[10] *R. Lampe, 2004, str. 389.*

nosti in nacionalne varnosti ter katera in pod kakšnimi pogoji ima prednost. Določene države so namreč izvajale posege v zasebnost posameznika zaradi zagotovitve nacionalne varnosti. Kot uvodno misel naj citiram Rawlsa, ki je v svojem delu Pravičnost kot poštenost dejal, da nobena temeljna svoboščina ni absolutna (mednje sodijo tudi vsi vidiki pravice do zasebnosti), ampak je vseeno potrebno dati temu sistemu temeljnih svoboščin prednost pred drugimi.[11] Nadalje trdi, da je neko temeljno svoboščino mogoče omejiti ali odtegniti samo zavoljo ene ali več drugih temeljnih svoboščin, nikdar pa za večje javno dobro, pojmovano kot večja neto vsota družbenih in ekonomskih prednosti za družbo kot celoto.[12]

3.1. Načelo sorazmernosti

V človekove pravice in temeljne svoboščine se praviloma ne sme posegati oziroma se lahko posega le iz izrecno določenih zakonskih razlogov. Poleg tega je pri tem potrebno upoštevati načelo sorazmernosti, ki se odvija na relaciji ukrepa in cilja. To določa, da je potrebno opraviti tako imenovani test sorazmernosti. Test sorazmernosti uporablja pri sodnem odločanju ustavno sodišče. Kakšen test sorazmernosti bo sodišče izvedlo, je odvisno od področja, na katerem se sodna presoja izvaja. Ustavno sodišče namreč lahko dopusti ožji ali širši manevrski prostor, odloča lahko strožje ali milejše. Če gre za področje, kjer je ustavno sodišče strogo, bo imela stran, ki ukrep zagovarja, težjo nalogo in bo morala tako podati močnejše razloge. Sodišče bo strožje v primeru, ko se odloča o človekovih pravicah in temeljnih svoboščinah. Medtem ko bo milejše odločalo glede finančnih vprašanj ter vprašanj socialne države. V slednjih primerih zakonodajalec lažje zmaga, medtem ko je to v prvih veliko težje. Ustavno sodišče ta test uporablja v primerih konflikta med dvema človekovima pravicama (horizontalni učinek človekovih pravic) oziroma pri sodni presoji ustavnosti, kadar želi zakonodajalec z novim pravnim aktom deloma poseči v določeno človekovo pravico posameznika (vertikalni učinek).[13] V tem delu nas zanima predvsem slednje.

V primerih, ko se načelo sorazmernosti nanaša na zakonodajalca, ga Kresal enači kar s prepovedjo čezmernih posegov dr-

[11] *J. Rawls, Pravičnost kot poštenost: reformulacija, 2011, str. 140.*
[12] *Prav tam, str. 148.*
[13] *J. Zobec v: M. Avbelj (urednik): Izzivi moderne države, 2012, str. 88.*

žave, saj ta zahteva omejuje zakonodajalčeve posege v človekove pravice in temeljne svoboščine ter vzpostavlja kvalificirano povezavo med zakonodajalčevim motivom in namenom, ki ga zasleduje, ter sredstvi in pravno normativnimi rešitvami, ki jih v ta namen uporabi.[14] Dodaja, da to zavezuje vse državne organe – zakonodajalca, izvršilno oblast, sodišča in druge nosilce javnih pooblastil. Toda ne samo pri njihovih realnih dejanjih in posegih, ampak tudi pri njihovih splošnih pravnih predpisih in pri konkretnih pravnih aktih.[15] Kresal ga deli na dva testa, in sicer: test legitimnosti, kjer se gleda cilj, in nato še »standardni« test sorazmernosti.

»Splošno ustavno načelo sorazmernosti predpostavlja najprej *test legitimnosti*, tj. preizkus,

– ali je cilj, ki ga zasleduje država, legitimen, to je stvarno upravičen in

– ali so od države uporabljena sredstva kot taka pravno dopustna.«[16]

»Nato sledi *test sorazmernosti*, in sicer preizkus,

– ali so izbrana sredstva za dosego cilja *primerna, tj. smiselna (razumna), uporabna in možna* in ali kot taka pridejo v poštev;

– ali so v poštev prihajajoča sredstva za dosego cilja *potrebna oz. nujna*;

– ali izbrana sredstva niso zunaj razumnega razmerja do družbene ali politične vrednosti cilja oz. ali je bilo vzpostavljeno proporcionalno sorazmerje *(načelo sorazmernosti v ožjem pomenu besede oz. načelo proporcionalnosti)* med prizadetostjo ustavne pravice posameznika, ki jo povzroči uporaba sredstva, in med ustrezno koristjo, ki jo pridobimo z uporabo sredstva za varstvo pravic drugih in na ta način v prid skupnosti.«[17]

Uporaba načela sorazmernosti in tehtanja (ang. »balancing«) med pravicami na podlagi tega testa ni značilno le za slovensko Ustavno sodišče, ampak je to splošna sodna praksa pri reševanju težjih vprašanj ter zagotavljanja normalnega delovanja demokratične in pravne države. Pri svojem odločanju ga uporabljajo tako evropska sodišča – Sodišče EU ter ESČP, kot tudi Vrhovno sodišče ZDA.

[14] *B. Kresal v: L. Šturm (urednik): Komentar Ustave Republike Slovenije, 2011, str. 55.*
[15] *Isto.*
[16] *Isto.*
[17] *Prav tam, str. 55–56.*

3.2. Test sorazmernosti – posameznik v. država

Kot uvod v to poglavje naj začnem z mislimi J. S. Milla. Ta v svojem delu sicer govori o svobodi posameznika in ne zasebnosti, ampak njegove ugotovitve smatram relevantne tudi za področje zasebnosti. Iz njih lahko namreč potegnemo analogijo na pravico do zasebnosti in posegov države vanjo; ti dve pravici sta med seboj precej povezani. Mill je pisal o mejah oblasti družbe nad svobodo posameznika in navedel eno pomembno pravilo. Pri vprašanju, kolikšen delež svobode pripada posamezniku in kolikšen družbi, pove, da naj »Individualnosti pripade tisti del, ki praviloma zanima posameznika, družbi pa oni, ki v glavnem zanima družbo.«[18] Življenje posameznika deli na dva dela in za vsakega določa drugačne pravice oblasti nad njimi.[19] Prvi del se tiče posameznika samega in zadeva samo njega. Njegovo ravnanje tukaj nima vpliva na druge. Tukaj ima posameznik popolno svobodo nad svojim ravnanjem in država oziroma oblast vanjo ne sme posegati. Pod drugi del sodijo ravnanja, ki imajo vpliv na druge ljudi. Za tega je značilno, da ima oblast pravico posegati v njegovo svobodo z namenom zaščite drugih – javnega interesa in javnega dobrega. Tako kot je veljalo v preteklosti, velja tudi danes: oblast si želi čim večji vpliv na posameznikovo življenje, svobodo in zasebnost, čeprav na drugačen način kot nekoč. To je na primer razvidno tudi iz samih dejavnosti obveščevalno-varnostnih agencij, ki so imele pooblastila s strani države. Ne moremo namreč trditi, da so vohunile za veliko večino svetovnega prebivalstva zgolj zato, ker jih je skrbelo za nacionalno varnost družbe. Jasno je, da so dandanes informacije ključnega pomena; več kot jih nekdo ima, večjo moč ima. Zavedati in držati pa bi se morali Millove delitve in posamezniku pustiti določeno stopnjo zasebnosti in svobode, v katero se preprosto ne more in ne sme posegati, razen izrecno v določenih primerih, ki pa morajo biti čim redkejši.

Mill trdi, da kdor uživa družbeno varstvo, tej družbi tudi nekaj dolguje. Pri ravnanju z drugimi ljudmi mora spoštovati določena pravila. Ravnati mora tako, da ne prizadene interesov drugih ljudi, bodisi zakonsko določenih ali tistih, ki se jih v skladu s tihim razumevanjem šteje za pravice. Prav tako mora nase prevzeti določen delež opravkov in žrtev, potrebnih za zavarovanje družbe

[18] *J. S. Mill, Utilitarizem; in O svobodi, 2003, str. 211.*
[19] *Prav tam, str. 147.*

in njenih članov pred krivico in nadlegovanjem.[20] Iz tega je razvidno, da je bil mnenja, da se mora posameznik prostovoljno odreči delu svoje svobode zaradi koristi celotne družbe. Če posameznik prekrši pravila, ki so nujna zaradi individualne ali kolektivne varnosti soljudi, mora za to odgovarjati. Pogubne posledice njegovih dejanj prizadenejo ljudi in zato se mu mora družba kot zaščitnik vseh svojih članov »maščevati«.[21] Ob tem se postavlja vprašanje, v kolikšni meri sme oblast legitimno poseči v svobodo, da bi preprečila zločin ali nesrečo. Mill navaja dve vrsti ukrepov, ki jih ima oblast na voljo in ki se odražata kot preprečevalna ter kaznovalna funkcija.[22] Pod prvo spadajo ukrepi, ki jih oblast sprejme za preprečevanje zločinov, medtem ko druga vsebuje ukrepe za odkrivanje in kaznovanje njihovih storilcev, potem ko so bili ti zločini že storjeni. Na škodo svobode posameznika oblast veliko lažje zlorabi preprečevalno funkcijo, saj komaj obstaja kakšen del legitimne svobode človekovega ravnanja, za katerega ne bi mogli prepričljivo pokazati, da krepi spretnosti za takšno ali drugačno obliko prestopka. Prav tukaj je razvidno moje razmišljanje iz prejšnjega odstavka: jasno je, da dejavnosti obveščevalno-varnostnih agencij sodijo v sklop preprečevalne funkcije, kar pomeni večjo možnost zlorabe. Ob tem Mill zaključuje, da je eno najtežjih in najbolj zapletenih vprašanj, »... kako določiti, kje se pričenja zlo, ki ogroža človeško svobodo in napredek oziroma natančneje, kje pričenja to zlo prevladovati nad koristmi, ki jih prinaša kolektivna uporaba družbene prisile [...], namenjena odstranitvi preprek na poti do družbene blaginje«.[23] Prav tako velja omeniti misel Galstona glede samega bistva omejevanja svobode, in sicer, da je cilj táko »omejevanje svobode vsakega posameznika [...], da je ta svoboda v harmoničnem odnosu s svobodo vseh drugih«[24]. To tezo lahko razširimo na vse temeljne človekove pravice in svoboščine. Vsakdo ima pravico do njih in te morajo biti v harmoničnem odnosu med seboj. Zato pa ima ustavno sodišče težko nalogo, ko pride do konflikta med njimi in mora nato tehtati, katera ima v konkretnem primeru večjo težo.

Osrednji problem tega članka je vprašanje, komu dati prednost – posamezniku ali družbi oziroma ali ima prednost pravica do za-

[20] *Prav tam, str. 211.*
[21] *Prav tam, str. 216.*
[22] *J. S. Mill, 2003, str. 233.*
[23] *Prav tam, str. 250.*
[24] *W. A. Galston, Liberalni nameni: Dobrine, vrline in raznolikost v liberalni državi, 2008, str. 109.*

sebnosti ali nacionalna varnost. Odgovor na prvi pogled niti ne izgleda toliko težaven. 2. odstavek 8. člena EKČP namreč že govori, da je možno pravico do zasebnosti omejiti iz izrecno določenih razlogov, ki so tam našteti. Med njimi je tudi razlog nacionalne varnosti. Ob tem naj opomnim, kot je bilo že omenjeno, da so kriteriji za omogočanje državnih posegov v pravice do zasebnosti neprimerno strožji v slovenski Ustavi, saj ta določa dodaten pogoj, in sicer: tovrstne akcije morajo temeljiti na odločbi sodišča.[25]

V uvodu sem zastavil vprašanje ali državni posegi v posameznikovo svobodo in zasebnost z namenom varovanja nacionalne varnosti izpolnjujejo zahteve načela sorazmernosti ter kakšne izboljšave so mogoče ali celo potrebne na zadevnem področju. Sam sem mnenja, da tovrstni posegi niso bili ustavni, saj niso izpolnili vseh zahtev testa sorazmernosti. Ker gre za področje človekovih pravic in temeljnih svoboščin, bi sodišče uporabilo strogi test sorazmernosti, kar pomeni manjšo možnost odobritve posegov vanje. Test bi prestal predpostavko legitimnosti oziroma ustavne dopustnosti cilja, saj se pravico do zasebnosti lahko omeji zaradi varovanja nacionalne varnosti. Čeprav se v skladu s slovensko Ustavo že tukaj pojavi težava. Določbe Ustave namreč zahtevajo kot pogoj tudi sodni nalog, ki ga v večini primerov obveščevalne agencije niso pridobile. Ker druge ureditve tega ne zahtevajo, tehtanje nadaljujemo. V naslednjem koraku se obrnemo k samemu ukrepu in najprej preverimo, ali je ta primeren. Z nadzorom posameznika na področju informacijske tehnologije je možno doseči zastavljeni cilj, saj se tako izve marsikatero podrobnost iz zasebnega življenja opazovanega, kar nato organom pregona omogoči njegovo prijetje in s tem zaščito nacionalne varnosti. Sledi tretja faza, in sicer je potrebno preveriti, ali so ta sredstva nujna oziroma potrebna za dosego tega cilja in ali ni na voljo milejših ukrepov. Vsesplošni nadzor ni najmilejši ukrep. To mesto zaseda ciljni nadzor, kjer je tarča nadzora eden ali več posameznikov in ne celotno prebivalstvo sveta. Vsi posamezniki že ne morejo biti potencialni sovražniki, ki ogrožajo nacionalno varnost. V tem delu zato izvajanje operacij obveščevalno-varnostnih organizacij spodleti in ne izpolni zahtev testa sorazmernosti, kljub temu da so bile izvajane v imenu nacionalne varnosti. Prav tako menim, da bi moral obstajati vsaj utemeljen sum pri določenem posamezniku, da se

[25] *R. Lampe, 2004, str. 473.*

ga nato lahko podrobno opazuje. Tovrstna pravila obstajajo že v kazenskem pravu in so nujno potrebna, če želimo govoriti o pravni državi. Tako z upoštevanjem vsega navedenega pri tehtanju in presojanju sorazmernosti v ožjem smislu ne morem trditi, da ukrepi množičnega nadzora lahko prestanejo test sorazmernosti. Tovrstnih ukrepov ne vidim kot sorazmernih, saj posegajo v pravico do zasebnosti vseh posameznikov za namene odkritja določenega odstotka posameznikov, ki bi lahko ogrožali nacionalno varnost. Tako menim, da so izbrana sredstva zunaj razumnega razmerja do družbene ali politične vrednosti cilja med prizadetostjo ustavne pravice posameznika, ki jo povzroči uporaba sredstva, in med ustrezno koristjo, ki jo pridobimo z uporabo sredstva za varstvo pravic drugih in na ta način v prid skupnosti. Če ukrepi nadzora testa sorazmernosti ne prestanejo uspešno, potem je zakonodaja, ki tak nadzor dovoljuje, protiustavna. Z menoj se strinja tudi Lampe, ki v svojem delu ne zanika tveganja varnosti drugih ljudi in s tem družbe in države, ampak kljub temu pove, da ne gre zagovarjati ekstremnih represivnih ukrepov državne oblasti pod krinko preprečevanja nereda ali zločina, beri nacionalne varnosti.[26] Tukaj je vredno omeniti še Jeffersonov citat »Kjer se svoboda krati zaradi varovanja svobode, vlada tiranija«.[27]

3.3. Omejitev – da ali ne?

Za širšo javnost pripravljena kratka anketa s preprostejšimi vprašanji je pokazala koliko posamezniki cenijo zasebnost in kaj so pripravljeni storiti za njeno zaščito.[28] 77 % anketiranih je dejalo, da se mora pravico do zasebnosti spoštovati. Medtem ko jih je bilo 15 % mnenja, da nimajo ničesar za skrivati in jih tako za njihovo zasebnost očitno ne skrbi. To je rahlo zaskrbljujoče, saj kljub temu da posameznik nima ničesar za skrivati, še ne pomeni, da lahko dovoljuje posege v svojo zasebnost oziroma da ga ti posegi ne interesirajo. Glede spoštovanja njihove zasebnosti jih je 85 % odgovorilo, da po njihovem prepričanju pravica do zasebnosti na in-

[26] *R. Lampe, 2004, str. 494.*
[27] *T. Jefferson v: R. Lampe, 2004, str. 494.*
[28] *Objavil sem jo na slovenskem tehnološkem forumu Slo-Tech ter v Facebook skupini Ius farma, namenjeni študentom prava. Med 124 anketiranci je bilo 63 % moških ter 37 % žensk. Povprečna starost anketiranih je bila od 21 do 40 let. Podrobnejši rezultati ankete z vsemi vprašanji in spremenljivkami so pripeti v prilogi na koncu magistrske naloge Ustavnost državnih posegov v zasebnost posameznika na internetu. Glej P. Cassol, Ustavnost državnih posegov v zasebnost posameznika na internetu, 2015, str. 155 – 162.*

ternetu ni spoštovana. Od tega jih je 66 % dejalo, da bi morala biti. Iz odgovorov na to vprašanje je lepo razvidna izguba zaupanja v pravni sistem, ki bi moral zagotavljati uspešno varstvo pravice do zasebnosti. V prihodnje je tukaj potrebno nekaj korenito spremeniti, če država želi, da posamezniki ponovno pridobijo zaupanje v pravo in učinkovito pravno varstvo svojih pravic. Kar 77 % anketiranih je pripravljenih, bodisi pasivno bodisi aktivno, storiti nekaj za svoje pravice. Večina, 62 %, je pripravljena občasno podpisati kakšno peticijo v podporo boja za varstvo pravice do zasebnosti. Medtem ko je le 15 % takšnih, ki so pripravljeni za svoje pravice aktivno postopati. Žalostno je to, da kar 23 % anketirancev ni pripravljenih storiti ničesar za zaščito svojih pravic. Če želimo, da se bo v prihodnosti naše temeljne pravice, med katerimi je tudi pravica do zasebnosti, spoštovalo, je potrebno čim večje število aktivnih posameznikov, pripravljenih za zagovarjanje svojih pravic. Le tako bodo država in njene organizacije sprevidele, da se ne sme posegati v pravice posameznikov ter da s tovrstnimi dejanji izgubljajo podporo množic. Glede seznanjenosti z ukrepi držav in njenih obveščevalnih agencij ter njihovimi posegi v zasebnost posameznikov na področju informacijske tehnologije, jih je kar 80 % dejalo, da so s temi dejanji seznanjeni, med njimi je 19 % takih, ki novicam redno sledijo in o tem aktivno razpravljajo na raznih forumih. Nezanimanje in ignoriranje nespoštovanja temeljnih pravic je morda najlažja pot, vendar zagotovo ne prava. Če se sami ne bomo zavzemali zase in za svoje pravice, se tudi drugi ne bodo za nas. Pri pregledu odgovorov glede na starost ni bilo večjih odstopanj od povprečja. Odstopanje je opazno samo v primeru zavzemanja za pravico do zasebnosti, kjer se starejši od 61 let niso več pripravljeni aktivno ali pasivno zavzemati za svoje pravice. Razumem, da po določenih letih osebe to ne zanima več in so mnenja, da naj se s tem ukvarjajo raje mladi. Ampak ravno oni, ki imajo največ življenjskih izkušenj, bi morali biti drugim za zgled. Grški pregovor pravi, da se družba najboljše razvija, kadar starejši sadijo drevesa, v katerih sencah vedó, da ne bodo nikoli sedeli.[29] Medtem ko je pri pregledu delitve po spolu moč videti, da moško populacijo nekoliko bolj skrbi za varstvo zasebnosti na internetu kot žensko. Zanimivo je primerjati rezultate pri pripravljenosti zavzemati se za svoje pravice. Odstotek je pri obeh v skladu s povprečjem,

[29] *»A society grows great when old men plant trees whose shade they know they shall never sit in.«*

kar zadeva pripravljenost – da (˜80 % pri obeh) oziroma ne (˜20 % pri obeh). Vendar so se moški bolj pripravljeni aktivno boriti za svoje pravice z raznimi protesti in zborovanji (˜21 % moški v. ˜7 % ženske), medtem ko ženske raje podpišejo kakšno peticijo (˜73 % ženske v. ˜56 % moški). Odstopanja so tudi pri seznanjenosti z ukrepi držav in njenih obveščevalnih agencij ter njihovimi posegi v zasebnost posameznikov na področju informacijske tehnologije. Moški so s tem bolj seznanjeni kot ženske (˜87 % moški v. ˜69 % ženske) in o tem veliko bolj diskutirajo na raznih forumih (˜28 % moški v. ˜4 % ženske).

Po analizi ankete je razvidno, da so posamezniki skeptični glede namenov obveščevalno-varnostnih organizacij in njihovega tajnega delovanja. Če države želijo resnično pomagati in izboljšati svet ter ga narediti varnejšega, je kot prvi in hkrati najpomembnejši korak večja transparentnost delovanja samih obveščevalno-varnostnih organizacij, saj lahko le tako dokažejo, da ne počnejo nelegalnih stvari. In še pomembneje, ne počnejo jih zgolj za večjo kontrolo nad množicami. Drugi korak je, da dejansko upoštevajo zakonodajo, ker je drugače pravzaprav vseeno, ali to skrivajo ali ne – ljudje tega ne bodo odobravali. Oziroma še bolje je, če se tovrstnim dejanjem v celoti odrečejo oziroma jih res izvajajo le v najnujnejših primerih, ko ni na voljo druge alternative. Do tedaj pa bomo imeli posameznike in skupine posameznikov, ki se bodo pripravljene boriti za vse nas in zagotavljati transparentnost ter legitimnost delovanja obveščevalnih državnih organizacij. V mislih imam posameznike, kot so Edward Snowden in Julian Assange ter skupino Anonymous. Slednja je že velikokrat vzela zakon v svoje roke in se odločila odkrito bojevati zoper tovrstna dejanja države in njenih organizacij. Falkvinge, ustanovitelj prve piratske stranke, je napisal članek na temo zasebnosti, kjer je o množičnem nadzoru povedal naslednje: »Škoda zaradi množičnega nadzora precej spominja na škodo, ki jo povzroči radioaktivnost. Uničujočih posledic se družba kot celota zave šele deset, petnajst, mogoče dvajset let kasneje, zato tudi s takšno lahkoto preženemo misel na nevarnost nečesa, kar ne vidimo, ne čutimo in ne vohamo, ko se sprehajamo po cesti. V resnici še predobro vemo, kam korakamo, saj se lahko zatečemo k številnim zapisom in lekcijam zgodovine.«[30] Ob tem naj v razmislek dodam razmišljanja dveh velikih oseb iz preteklo-

[30] *R. Falkvinge, Zakaj pa sploh rabimo zasebnost?, 2015, https://piratskastranka.si/zakaj-pa-sploh-rabimo-zasebnost (zadnjič obiskano: 27. 12. 2015)*

sti. Benjamin Franklin je dejal: »Kdor se je pripravljen odreči pravicam, ki jih prinaša svoboda, za kanček varnosti, si ne zasluži ne svobode, ne varnosti.«[31] Nekateri ljudje se z dejanji obveščevalnih agencij in njihovimi posegi v zasebnost in svobodo strinjajo in so za uvedbo večjega nadzora, saj menijo, da je to potrebno za zagotovitev večje stopnje varnosti. Ampak kot je Mill dejal: »Svoboda ni dovoljenje za odpoved svobodi«.[32] To pomeni, da tudi, če se posameznik želi zavestno odpovedati oziroma dovoli poseg v svojo svobodo (in zasebnost), ta že na sami podlagi načela svobode ni dopusten in tovrstnih akcij ne napravi legitimnih in legalnih.

4. Pravna ureditev poseganja v pravico do zasebnosti

Že omenjena Direktiva 2006/24/ES je bila sprejeta na podlagi pritiska britanske policije na angleški parlament po bombnih napadih v Londonu leta 2005.[33] Za neskladno z nacionalno ureditvijo je bila razglašena in ni bila implementirana v Nemčiji, Romuniji, na Češkem in Cipru. Medtem ko jo je Irska na podlagi predhodnega vprašanja po 267. členu PDEU podala v odločanje Sodišču EU.[34] Direktiva je namreč določala, da telekomunikacijski operaterji in ponudniki internetnih storitev za obdobje od 6 do 24 mesecev zbirajo podatke o svojih strankah – tako klice kot sledenje lokaciji posameznikov, četudi ti niso bili nikoli osumljeni storitve kaznivega dejanja. Sodišče EU jo je z združenimi zadevami Digital Rights Ireland & Seitlinger in drugi (C-293/12 in C-594/12) razglasilo za neveljavno. Sporna pri tej direktivi je njena neizpolnitev zahteve omejenosti zgolj na tisto, kar je strogo potrebno. S tem je sodišče postavilo pomemben precedens k varstvu pravic posameznika do komunikacijske in informacijske zasebnosti na območju Evropske Unije. Pravo ne sme zaostajati za razvojem in ga zavirati. Tega se zaveda tudi EU, zato si je Evropska Komisija zadala cilj, da

[31] *»Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety.« M. W. Echols, Panopticon–Surveillance and Privacy in the Internet Age, 2009, str. 5.*

[32] *J. S. Mill, 2003, str. 240.*

[33] *Da je prišlo do sprejetja tovrstne direktive zaradi pritiska ravno s strani britanske vlade, niti ni presenetljivo, saj Barnard-Wills v svoji raziskavi trdi, da je Velika Britanija že večkrat podelila večjo prioriteto varnosti nasproti zasebnosti, predvsem kar se tiče tehnologije nadzora. D. Barnard-Wills, Security, privacy and surveillance in European policy documents, International Data Privacy Law, No. 3 (2013), str. 171.*

[34] *McNamee/Fielder/Humeau/Dimov, EU Surveillance: A summary of current EU surveillance and security measures, 2012, str. 5.*

do konca leta 2015 oziroma v začetku leta 2016, sprejme posodobljeno različico Direktive 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. To naj bi nadomestila kar uredba z imenom Splošna uredba o varstvu podatkov (ang. »General Data Protection Regulation«), katere ureditev bo prilagojena sodobni tehnologiji digitalne dobe ter bo med drugim uredila tudi trenutna pereča vprašanja o množičnem nadzoru in zbiranju podatkov s strani obveščevalno-varnostnih organizacij.[35]

Pravna ureditev v Republiki Sloveniji je podobna tisti v EU, saj je kot njena članica sodelovala pri harmonizaciji pravne ureditve na evropski ravni in tako implementirala številne direktive. Med drugim je implementirala tudi Direktivo 2006/24/ES in obveznosti o hrambi podatkov prenesla v svoj pravni red že z uveljavitvijo Zakona o spremembah in dopolnitvah Zakona o elektronskih komunikacijah (Uradni list RS, št. 129/06 – ZEKom-A), ki je začel veljati 27. 12. 2006. Določen je bil maksimalen rok hrambe podatkov, in sicer 24 mesecev. Nato je z njegovo novelo leta 2010 hrambo prometnih podatkov na področju telefonije skrajšala na 14 mesecev, hrambo internetnih prometnih podatkov pa na 8 mesecev. Leta 2012 je v veljavo stopil ZEKom-1[36], ki je urejal hrambo podatkov v XIII. poglavju (členi od 162 do 169). Dne 3. 7. 2014 je Ustavno sodišče RS v postopku za oceno ustavnosti, začetem z zahtevo Informacijskega pooblaščenca, te člene razveljavilo, saj na podlagi varstva človekovih pravic predstavljajo prevelike omejitve pravice do zasebnosti na področju informacijskih tehnologij.[37] Možnost poseganja v pravico do zasebnosti v pravni ureditvi Republike Slovenije je določena tudi v Zakonu o kazenskem postopku (ZKP) ter Zakonu o Slovenski obveščevalno-varnostni agenciji (ZSOVA). In sicer je poseg v pravico do zasebnosti mogoč zgolj na podlagi odredbe sodišča iz izrecno določenih razlogov, med katere sodi tudi nacionalna varnost. Tovrstne posege navadno izvajata policija in SOVA na podlagi določb 150. člena ZKP. SOVA ima na voljo tudi določbe iz 24. člena ZSOVA. Na podlagi teh določb izvajajo nadzor komuniciranja, sporočil, prisluškovanje in tajno opazovanje, sledenje ter snemanje. Kadar je potreben zakoniti nadzor s temi

[35] *Varstvo podatkov: Svet dosegel dogovor o splošnem pristopu, 2015, http://www.consilium.europa.eu/sl/press/press-releases/2015/06/15-jha-data-protection/ (zadnjič obiskano: 27. 12. 2015).*
[36] *Zakon o elektronskih komunikacijah, Uradni list RS, št. 109/2012.*
[37] *USRS, 3. 7. 2014 – opr. št. U-I-65/13, http://odlocitve.us-rs.si/sl/odlocitev/US30439*

metodami, pride v poštev še Zakon o poštnih storitvah (ZPSto-2), ki v 55. členu od izvajalcev poštnih storitev zahteva, da morajo na podlagi odredbe pristojnega organa na svoje stroške omogočiti dostop do vsebine poštnih pošiljk ter sporočiti podatke o dejstvih in okoliščinah poštnega prometa. Še najbolj problematičen pa je 21. člen ZSOVA, ki omogoča »spremljanje mednarodnih sistemov zvez«, kar je olepšava za prisluškovanje, in sicer brez sodne odredbe, saj zadostuje že podpis direktorja obveščevalno-varnostne agencije.[38]

Posebej pomembno je omeniti pravno ureditev omejitve pravic posameznika v korist nacionalne varnosti v ZDA, saj so ravno Američani tisti, ki so začeli tovrstne postopke in tudi sprejeli zakonodajo, na podlagi katere so le-te izvajali. Bistvena prelomnica je 11. september 2001, saj ta dan označuje začetek odkritega boja proti terorizmu. Osrednji zakon so sprejeli v nekaj več kot enem mesecu po napadih, natančneje 24. oktobra 2001. Govorim o USA PATRIOT Act-u[39]. Njegovo ime je akronim, ki pomeni »Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT)«. V slovenskem prevodu bi to pomenilo: pravni akt za združitev in krepitev Amerike z zagotavljanjem ustreznih orodij, potrebnih za prestrezanje in preprečevanje terorizma. Že iz samega naslova tega zakona vidimo, čemu je namenjen. Krepko je razširil pristojnosti ameriških agencij za kazenski pregon v boju proti terorizmu. Obstoječi oblasti je omogočil preiskave telefonskih in elektronskih pogovorov, zdravstvenih, finančnih in drugih registrov podatkov; podelil dovoljenje za zbiranje tujih obveščevalnih podatkov znotraj ZDA; razširil je regulacijo finančnih transakcij ter odobril pridržanje neameriških državljanov, osumljenih storitve terorističnih dejanj.[40] Še posebej zloglasna je določba člena 215 PATRIOT Act-a. 1. junija 2015 je USA PATRIOT Act prenehal veljati zaradi pomanjkanja odobravanja s strani ameriškega kongresa. Kot njegovo nadomestilo je ameriški zakonodajalec 2. junija 2015 sprejel »naslednika« tega zakona, ki je določene dele prejšnjega zakona obnovil in zadržal v veljavi do leta 2019. Govorim o USA FREEDOM Act-u[41], ki je prav tako akronim, ki predstavlja naslednji slogan: »Uniting

[38] *M. Drev, Množični nadzor v sodobni družbi, 2010, str. 129.*
[39] *USA PATRIOT Act (H. R. 3162).*
[40] *The ethics (or not) of massive government surveillance, http://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/index3.html (zadnjič obiskano: 27. 12. 2015)*
[41] *USA FREEDOM Act (H. R. 2048).*

and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act«. Kot vidimo, ima novi zakon, vsaj kar se naslova tiče, drugačno nalogo. V slovenščino bi akronim prevedli kot pravni akt za združitev in krepitev Amerike z izpolnjevanjem pravic in prenehanjem s prisluškovanjem, Dragnet-zbiranjem[42] in spletnim nadzorom. Iz samega akronima je razvidno, da naj bi ta zakon »vrnil zadeve nazaj na stare tire« in povrnil posameznikom polno pravico do zasebnosti, kot so je bili ti deležni pred sprejetjem USA PATRIOT Act-a. Vsebuje določbe o omejitvi pridobivanja podatkov, čeprav ne v celoti. NSA lahko sedaj zaprosi družbe za podatke o specifični entiteti – osebi, računu ali napravi ter mora ob tem dokazati, da je ta povezan s tujo silo (ang. »foreign power«) oziroma teroristično skupino.[43] S tem se premakne hramba osebnih podatkov iz NSA na zasebne družbe. Nekateri so mnenja, da zakon kljub temu še vedno dovoljuje pridobivanje podatkov v precej velikem obsegu. Prav tako je za izvajanje nadzora pomemben Foreign Intelligence Surveillance Act (FISA) iz leta 1978.[44] Gre za temeljni zakon, ki je pred terorističnimi dejanji in posledičnim sprejemom posebnih programov in pravnih aktov v sklopu boja proti terorizmu kot glavni pravni akt urejal celoten domač elektronski nadzor zbiranja tujih informacij. Kot že samo ime pove, gre za zakon, ki dovoljuje nadzor komunikacij, vendar le od tujcev. Ameriškim državljanom se na njegovi podlagi ne sme prisluškovati. Najpomembnejša dopolnitev tega zakona je FISA Amendments Act iz leta 2008, ki je omogočil nadzor tudi ameriških državljanov in bil tako pravna podlaga za vsesplošni nadzor.[45] Omogoča namreč vsakršno prestrezanje komunikacij med Američanom in tujcem, že če je bil slednji zgolj »razumno« osumljen terorizma.[46] Vse dejavnosti NSA so s tem dobile pravno podlago. Gre za člen 702 FISA, ki ostaja v veljavi do konca leta 2017, in za katerega Snowden pravi, da omogoča dejanja NSA, ki so v popolnem nasprotju z zapovedmi 4. amandmaja ameriške

[42] *Dragnet je eden izmed programov NSA za zbiranje podatkov.*
[43] *A. Byers, USA Freedom Act vs. USA PATRIOT Act. A look at how the two measures differ, 2015, http://www.politico.com/story/2015/05/usa-freedom-act-vs-usa-patriot-act-118469.html (zadnjič obiskano: 27. 12. 2015)*
[44] *Foreign Intelligence Surveillance Act of 1978 (50 U. S. C. ch. 36). S prevodom v slovenščino bi ta zakon poimenovali Zakon o nadzoru komunikacij tujcev.*
[45] *Tako je dejal Edward Snowden v enem svojih intervjujev. K. Sanders, Fact-checking John Oliver's interview with Edward Snowden about NSA surveillance, 2015, http://www.politifact.com/punditfact/statements/2015/apr/09/edward-snowden/fact-checking-john-olivers-interview-edward-snowde/ (zadnjič obiskano: 27. 12. 2015).*
[46] *L. Harding, Dosje Snowden: Zgodba najbolj iskanega človeka na svetu, 2014, str. 86.*

ustave in bi zato moral biti razveljavljen.[47] Omeniti velja še amandmaje k vsebini tako imenovanega »Executive Order 12333«[48] z dne 30. julija 2008. Ta med drugim dopušča možnost aktivnega tajnega delovanja za dosego ciljev agencije, med katere sodijo dejanja ozvočenja sistemov informacijske tehnologije, prebiranje e-pošte in drugi ter celo domnevni kibernetski napadi in sabotaže preko omrežij informacijske tehnologije.[49] Kot je bilo omenjeno, so bile pred kratkim določbe o hrambi osebnih podatkov s strani evropskih sodišč – Sodišča EU ter nacionalnih ustavnih sodišč, med njimi tudi USRS, razglašene za neveljavne, ker so v nasprotju z določbami o varstvu človekovih pravic, posebej pravice do zasebnosti. Tukaj pa so bile ravno takšne določbe sprejete z USA FREEDOM Act-om in se štejejo za milejši ukrep od prejšnje ureditve. Tako vidimo, da so ZDA, kar se tiče varstva pravice do zasebnosti in posegov vanjo, najmanj en korak za evropsko ureditvijo.

5. Informacijska družba in družbeni nadzor

Hiter razvoj informacijske tehnologije je prinesel nove tehnike družbenega nadzora. Sodobna družba je informacijska družba in prav tako lahko govorimo o sodobnem informacijskem nadzoru.[50] »Big brother is watching you!«[51] je slavni rek iz romana George Orwella, ki z leti vse bolj postaja resničnost. Veliki brat nas resnično opazuje na vsakem koraku. Tajne policije nekdanjih totalitarnih režimov si tovrstnega nadzora niso mogle niti predstavljati. Zanje je bilo značilno, da so zaradi potreb po večjem nadzoru uvedli sistem kartotek, kjer so zabeležili vse svoje objektivne sovražnike ter njihove prijatelje, znance, sorodnike, skratka vse osebe, s katerimi so ti kadarkoli prišli v stik ter poskušali ugotoviti samo naravo njihove povezave.[52] Dandanes, z vsem razvojem informacijske tehnologije, sodobne obveščevalno-varnostne agencije to počnejo na veliko bolj enostaven in eleganten način – zbrati jim uspe veliko večje količine podatkov, vse skupaj je veliko bolje organizirano

[47] *J. Ernst, USA Freedom Act vs expired Patriot Act provisions: How do the spy laws differ?, 2015, http://www.rt.com/usa/264005-freedom-patriot-act-surveillance/ (zadnjič obiskano: 27. 12. 2015).*
[48] *P. Margulies, The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism, Fordham Law Review, Iss. 5 (2014), str. 2142.*
[49] *J. Bamford, The Secret War, 2013, https://web.archive.org/web/20140125144725/http://www.wired.com/threatlevel/?p=58188 (zadnjič obiskano: 27. 12. 2015)*
[50] *Webster predlaga, da bi lahko namesto pojma informacijska družba uporabljali kar pojem družba nadzora. F. Webster v: M. Kovačič, Zasebnost na internetu, 2003, str. 23.*
[51] *»Veliki brat te opazuje!« G. Orwell, 1984, 1983, str. 1.*
[52] *H. Arendt, Izvori totalitarizma, 2003, str. 524–525.*

in na dosegu roke z enim samim klikom na gumb. Takratni totalitarni režimi o tovrstnem sistemu nadzora niso upali niti sanjati.[53] Če navedem primere, obveščevalno-varnostne agencije so nadzirale posameznikove objave na socialnih omrežjih, prisluškovale telefonskim pogovorom, uporabljale možnost geografske lokacije telefona za ugotovitev gibanja posameznika, brale e-pošto ter na splošno točno vedele, kdaj, kje in kaj je nekdo brskal po spletu.[54] Kadar to potrebujejo, vse skupaj zberejo v datoteko in si ustvarijo natančen profil te osebe, saj imajo na razpolago vpogled v praktično celotno življenje tega posameznika.[55] Razvoj tehnologije je omogočil pocenitev in večji obseg zbiranja in obdelave podatkov ter s tem razširitev samega nadzora. Prav tako je prišlo do globalizacije nadzora. Predvsem v zadnjem času je opaziti globalizacijo mednarodnih varnostnih in administrativnih sistemov, pa tudi globalizacijo komercialnega nadzorovanja.[56]

V današnji informacijski dobi gre za neke vrste moderen tip panoptikona, arhetipa družbenega nadzora, katerega gradbeni koncept je pred več kot dvesto leti postavil Jeremy Bentham.[57] Ta model je omogočal samodejno vzpostavitev in delovanje nadzora nad zaprto populacijo in je bil predviden najprej za zapor, nato pa še za tovarno, šolo, bolnišnico in norišnico. Bentham je bil mnenja, da je mogoče z njegovim izumom izboljšati moralo, ohraniti zdravje, okrepiti industrijo, utrditi ekonomijo ter še marsikaj.[58] Kasneje, v dvajsetem stoletju, je Foucault v svojem delu »Oko oblasti« to idejo razširil preko same arhitekturne razsežnosti ter jo predstavil kot koncept družbenega nadzora, kjer so posamezniki opazovani, brez da to vedó.[59] Slednje je največja posebnost in prednost. Kot je dejal Miller: »To, da oko vidi, ne da bi bilo videno – v tem

[53] *Kot navaja Arendt, so bile takratne »moderne« sanje policije (govorimo o 40-ih, 50-ih letih 20. stoletja) v primerjavi z današnjimi precej skromnejše, in sicer: »Moderne sanje totalitarne policije skupaj z njeno moderno tehnologijo so neprimerno grozljivejše. Zdaj policija sanja o tem, da bi že en sam pogled na orjaški zemljevid v vsakem trenutku zadoščal za ugotovitev, kdo je povezan s kom in v kolikšni meri; in te sanje, teoretično gledano, niso neuresničljive, čeprav je tehnična plat izvedbe nekoliko zahtevnejša.« H. Arendt, 2003, str. 524–525. Kot vidimo, so te neprimerljive z dosegom in s tem močjo, ki jo imajo tajne službe danes, saj tehnična plat izvedbe ni več problematična, niti za pridobitev bistveno večje količine informacij od prej omenjenih.*

[54] *Za več informacij o tem glej Surveillance Techniques: How Your Data Becomes Our Data, 2015, https://nsa.gov1.info/surveillance/ (zadnjič obiskano: 28. 12. 2015) in How the NSA's Domestic Spying Program Works, 2015, https://www.eff.org/nsa-spying/how-it- (zadnjič obiskano: 28. 12. 2015).*

[55] *L. Harding, 2014, str. 37 in 47–50.*

[56] *M. Kovačič, Nadzor in zasebnost v informacijski družbi: Filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu, 2006, str. 31.*

[57] *Natančneje leta 1791. M. Drev, 2010, str. 21–22.*

[58] *J. Bentham v: M. Kovačič, 2006, str. 24.*

[59] *M. Kovačič, 2006, str. 22–23.*

je največja zvijača Panoptikona. Če lahko razločim pogled, ki me zalezuje, lahko obvladam nadziranje, lahko ga tudi sam zalezujem, ugotovim njegove premore in slabosti, preučim njegovo regularnost, ga izsledim. Če pa je Oko skrito, potem me gleda tudi takrat, kadar ne vidi. Oko, ki je potuhnjeno v senci, pomnoži vse svoje moči ...«.[60] Ravno takšno opazovanje oziroma nadziranje posameznikov brez njihovega vedenja je značilno tudi za današnje čase, s tem da je veliko bolj dodelano. Dandanes namreč ni več potreben nadzor s fizično prisotnostjo opazovalca, ampak je dovolj to storiti preko medijev sodobne informacijske tehnologije v virtualnem prostoru. Opazovalec je tako lahko tisoče kilometrov stran in kljub temu izve o življenju in osebnih zadevah opazovanega posameznika mnogo več, kot je bilo to mogoče pred par desetletji s konstantnim fizičnim opazovanjem posameznika. Država postaja vse bolj omnipotentna, točno ve, kaj počneš, kje in kdaj to počneš. Prav tako ve, kje te najti ob vsakem trenutku. Lahko bi rekli, da je bila to največja vizija Benthama, ki pa se v tistem času še ni mogla uresničiti zaradi pomanjkanja tehnološkega napredka. Dolar je namreč dejal, da je bila njegova vizija o nadzoru »v naslednjem koraku, kako čim bolje izpostaviti pogledu celoten družbeni prostor, ga napraviti preglednega in dostopnega kontroli ...«.[61]

S sodobno tehnologijo (računalniki, mobilnimi telefoni, bančnimi karticami, RFID čipi, GPS napravami ipd.) se nenehno kopiči podatke in gradi profile celotnih populacij.[62] »Posameznik tako postaja sam svoj dosje in v sodobni družbi praktično ne more obstajati, ne da bi bil nadzorovan.«[63] Oziroma kot pravi Kovačič: » ... državljani živimo v svetu, v katerem se moramo nujno odpovedati delu svoje zasebnosti na račun večje funkcionalnosti in obvladovanja kompleksnosti življenja v sodobni družbi«.[64] Nadzor postaja problematičen, saj se mu podrejamo prostovoljno, za določene ugodnosti.[65] Prav tako puščamo za sabo tako imenovano elektronsko sled. Gre za informacije o dejavnostih nekega posameznika,

[60] *J. A. Miller v: M. Kovačič, 2006, str. 23.*
[61] *M. Dolar v: M. Kovačič, 2006, str. 24.*
[62] *M. Drev, 2010, str. 31.*
[63] *Isto.*
[64] *M. Kovačič, 2006, str. 34.*
[65] *O tem poroča tudi Rhoen, ki govori o tako imenovanem »Big Data« trendu, kjer zasebne družbe zbirajo ogromne količine podatkov iz posameznikovega zasebnega življenja za namene procesiranja in omogočanja boljše uporabniške izkušnje. Posamezniki velikokrat niti nimajo izbire, ali produkt uporabijo in izgubijo zasebnost ali pa ga ne in svojo zasebnost ohranijo. Druge izbire nimajo. M. Rhoen, Big Data and Consumer Participation in Privacy Contracts: Deciding who Decides on Privacy, Utrecht Journal of International and European Law, Iss. 80 (2015), str. 52–54.*

ki se samodejno shranjujejo. O njej je že leta 1983 pisal Burnham in opozoril, da avtomatski sistemi ali institucije vsakič zaznajo in zabeležijo dogodke, kot so prometni podatki, kadar: posameznik dvigne slušalko, uporabi bankomat ali plačilno kartico, gre na banko, obišče zdravnika, se poroči ipd.[66] Danes bi k temu lahko dodali še marsikaj, kot na primer kakršnakoli uporaba mobilnih telefonov, zgodovina brskanja po spletu, uporaba raznih navigacijskih sistemov, spletni piškotki itd.

Falkvinge je primerjal, kaj je pomenila beseda prisluškovanje nekoč (v 90-ih letih prejšnjega stoletja) in danes. Dejal je, da ko so 20 let nazaj prisluškovali našim staršem, so organi nadzirali telefonske klice in fizična pisma. »Ko nam »prisluškujejo« danes, s tem mislijo nadzor naslednjih stvari (le kratek in nepopoln seznam):[67] »telefonski klici; fizična pisma; elektronska pošta; neformalni pogovori; kakšno glasbo poslušamo, kakšne filme gledamo in s kom; katere časopise beremo, kakšne članke beremo v teh časopisih, kdaj, kako dolgo in v kakšnem vrstnem redu; kakšne knjige beremo in koliko nas ta tema zanima; kaj kupujemo; o katerih nakupih razmišljamo, a jih ne opravimo; kam gremo na počitnice; katera potovanja želimo rezervirati, a jih ne; na katere strani za zmenkarije hodimo in s kom se dobivamo; kako hodimo po mestih: v resoluciji, ki zajame vsak korak, vključno s hitrostjo hoje; vse slike, ki jih pokažemo prijateljem; vse slike, ki jih posnamemo, a jih ne pokažemo prijateljem; naša teža, delež telesne maščobe, krvni tlak in splošno zdravje; neposredni video prenos naše dnevne sobe, tudi ponoči; kdaj spimo in kako dobro se naspimo; vse, kar rečemo pred televizijo; vse ostalo, kar delamo na internetu in vse druge informacije, do katerih imajo dostop senzorji na kateri koli izmed naših naprav, med drugim na telefonih, kamerah, prenosnikih, avtih, urah in tako dalje, tudi če nikoli nismo vedeli, da ta senzor obstaja in ne poznamo aplikacije, ki bi analizirala prav ta podatek.«

V sklopu opravljanja obveščevalno-varnostne dejavnosti obveščevalne službe svojim programom dodeljujejo posebna imena. Med poznanimi in odmevnimi programi obveščevalnih agencij so predvsem programi NSA in GCHQ. Mnoge izmed njih je razkril Snowden. Obstaja možnost, da te obveščevalne agencije izvajajo

[66] *D. Burnham v: M. Kovačič, 2003, str. 27.*
[67] *R. Falkvinge, Prisluškovanje 21. stoletja ne enačite s tistim v 90. letih, 2015, https://piratskastranka.si/prisluskovanje-21-stoletja-ne-enacite-s-tistim-v-90-letih/ (zadnjič obiskano: 28. 12. 2015).*

še kakšne podobne programe, ki pa nam zaradi njihove tajnosti zaenkrat niso poznani. Med prvimi programi NSA, zagnanimi po 11. septembru 2001, je bil program STELLAR WIND, ki je omogočal množično »rudarjenje podatkov« ameriških državljanov in je zajemal internetne komunikacije, kot so elektronska sporočila (e-pošta), telefonske komunikacije, finančne transakcije, telefonske in internetne metapodatke ter samo internetno aktivnost.[68] Prav tako je takrat začel delovati program TRAILBLAZER, preko katerega je NSA analizirala podatke, ki so se prenašali preko različnih komunikacijskih omrežij, telefonije in interneta.[69] Oba programa sta kasneje prenehala delovati. Med najodmevnejšimi je program PRISM, ki določa tajno sodelovanje največjih tehnoloških družb in telekomunikacijskih operaterjev. Med njimi najdemo mnoge tehnološke »velikane« iz Silicijeve doline, kot so Google (od januarja 2009), Apple (od oktobra 2012), Microsoft (od septembra 2007), Facebook (od junija 2009) ter številne velike telekomunikacijske ponudnike, kot sta Verizon in AT & T ter številni drugi.[70] NSA je od njih zahtevala tako predajo metapodatkov kot same vsebine e-pošte, raznih spletnih pogovorov, videoposnetkov, slik in ostalih dokumentov.[71] Vsaka izmed omenjenih družb ima ogromno število uporabnikov (gledano v stotinah milijonov oz. milijardah) in možnost zbiranja velikega števila informacij. Tako je NSA s pomočjo naštetih tajnih sodelavcev pridobila neomejen dostop do praktično vseh podatkov na internetu, pa naj se sliši še tako neverjetno. Če vzamemo za primer Google, ki lahko pridobi in hrani ogromne količine podatkov od svojih uporabnikov, saj ponuja velik obseg storitev – od internetnega brskalnika, predvajalnika videoposnetkov YouTube, elektronske pošte Gmail do Google zemljevidov, klepetalnice Hangouts, hrambe podatkov v oblaku Google Drive ter socialnega omrežja Google + in številnih drugih. Vsak uporabnik interneta tako uporablja vsaj eno Googlovo storitev ter za seboj pušča elektronsko sled in informacije, ki jih posledično preko tajnega sodelovanja pridobijo agenti NSA. Internet je obširen virtualni prostor, kjer nobeno dejanje posameznika ni neopazno in anonimno, saj se vedno najde nekdo, ki bo opazoval oziroma beležil našo sleherno aktivnost na spletu. Temu

[68] *L. Harding, 2014, str. 81–83.*
[69] *Prav tam, str. 47–48.*
[70] *Freedom on the Net 2014, 2013, str. 890–891 in Luke Harding, 2014, str. 176.*
[71] *Freedom on the Net 2014, 2013, str. 891.*

je podoben GCHQ-jev program TEMPORA, s katerim so Britanci prestrezali promet, ki poteka preko podmorskih optičnih kablov ob kraju Bude v Veliki Britaniji in preko katerih poteka kar 25 % celotnega internetnega prometa na svetu.[72] Ta program med drugim določa tako imenovane »prestrezne partnerje« oziroma tajne sodelavce, ki GCHQ posredujejo podatke.

6. Primeri in praksa iz tujine

Razmere so najboljše v EU, kjer se zagotavlja še najvišja stopnja varstva. Pomembno vlogo pri tem ima Sodišče EU, kar je razvidno iz sodbe v zadevi Digital Rights Ireland v aprilu 2014, ko je za neveljavno razglasilo Direktivo 2006/24/ES o hrambi osebnih podatkov. Sodišče EU je s to odločbo pokazalo, da hramba osebnih podatkov krši temeljne človekove pravice, podeljene s pravom EU in da se mora te na ozemlju EU spoštovati. Pravica do zasebnosti državljanov EU je pomembna in posegi vanjo s strani države oziroma njenih obveščevalnih agencij so tukaj nedopustni. O programih množičnega nadzora obveščevalno-varnostnih agencij, kot je program PRISM, je odločalo v zadevi Max Schrems v. Data Protection Commissioner (C-362/14), kjer je 6. oktobra 2015 tudi razveljavilo dogovor Varni pristan (ang. »Safe Harbour«) o izmenjavi podatkov med EU in ZDA. Dejalo je namreč, da stopnja varstva pravic v EU ni enaka tisti v ZDA in je zato ogroženo varstvo pravice do zasebnosti državljanov EU. Pravica do zasebnosti je dobro varovana tudi v Republiki Sloveniji, saj je kmalu po sprejetju odločbe Sodišča EU Ustavno sodišče RS s sodbo v zadevi U-I-65/13 julija 2014 razveljavilo XIII. poglavje Zakona o elektronskih komunikacijah, ki je vseboval podobne določbe. Ustavno sodišče je glede omejevanja človekovih pravic v tem primeru dejalo naslednje: »V izhodišču je treba poudariti, da so boj proti hudim kaznivim dejanjem, še posebej organiziranemu kriminalu in terorizmu, obramba države in zagotavljanje nacionalne varnosti ter ustavne ureditve temeljnega pomena za delovanje pravne države. Vendar pa tak cilj, čeprav temeljnega pomena, sam po sebi ne more upravičevati neomejenega posega v človekove pravice.«[73]

Vendar pa ni bilo, oziroma ni, povsod v evropskih državah tako. Francija namreč postaja država vse večjega nadzora, saj je 25.

[72] *L. Harding, 2014, str. 139–142.*
[73] *USRS, 3. 7. 2014 – opr. št. U-I-65/13, http://odlocitve.us-rs.si/sl/odlocitev/US30439.*

junija 2015 sprejela zakonodajo, ki širi pooblastila obveščevalnim agencijam in dovoljuje vohunjenje v javnosti ter veča nadzor nad svojim prebivalstvom. Mnogi ji očitajo dvoličnosti, saj je v medijih odkrito kritizirala ameriško vohunjenje za njimi[74], medtem ko je kmalu zatem sama sprejela takšno zakonodajo.[75] Kritiki novo sprejetega zakona slednjega imenujejo kar »Francoski Patriot Act«.[76] Kontroverzni zakon je bil prvič predstavljen francoskemu parlamentu aprila 2015, in sicer kot posledica terorističnih napadov na Francijo januarja istega leta. Gre za napade na Charlie Hebdo. V luči ponovnih terorističnih napadov na Pariz, 13. novembra 2015, ki predstavljajo precej svežo rano francoski državi in njeni nacionalni varnosti, bo po vsej verjetnosti taka zakonodaja ostala v veljavi še kar nekaj časa. Primeri množičnega nadzora in deljenja informacij z NSA niso tuji niti Nemčiji. Maja 2015 se je namreč razvedelo o sodelovanju nemškega telekoma – Deutsche Telekom z nemškimi obveščevalnimi službami – Bundesnachrichtendienst (BND). Program je poznan pod imenom »Operacija Eikonal« in je deloval med leti 2004 – 2008.[77] 1. oktobra 2015 pa je slovenska javnost izvedela, da se je v sklopu te operacije prisluškovalo tudi določenim slovenskih telefonskim linijam, ki so potekale v tujino. Seveda ne moremo mimo Velike Britanije, ki je poleg ZDA, med najhujšimi kršiteljicami posameznikove pravice do zasebnosti. Njena obveščevalna agencija Government Communications Headquarters (slo. Vladni urad za komunikacije) oziroma GCHQ je najtesnejša partnerica NSA in je skupaj z njo izvajala množični nadzor svetovnega prebivalstva s prestrezanjem internetnih in telefonskih komunikacij. Snowden je celo dejal, da je GCHQ še hujša in bolj vsiljiva kot NSA.[78] V primerjavi z ZDA so imeli večjo svobodo pri delu, kar potrjujejo razkriti dokumenti, v katerih je GCHQ sama dejala: »V primerjavi z ZDA nam veliko manj gledajo pod prste.«[79] V Veliki Britaniji preiskovalna pooblastila obveščevalnih

[74] *Prisluškovanje francoskim predsednikom je 23. 6. 2015 z objavo obremenilnih dokumentov razkril WikiLeaks. Več o tem v Espionnage Élysée, 2015, https://wikileaks.org/nsa-france/ (zadnjič obiskano: 28. 12. 2015).*

[75] *M. Untersinger, If You Can't Beat'Em: France, Up In Arms Over NSA Spying, Passes New Surveillance Law, 2015, https://firstlook.org/theintercept/2015/06/24/france-protests-nsa-spying-passes-new-surveillance-law/ (zadnjič obiskano: 28. 12. 2015).*

[76] *Step closer to surveillance state? France passes new spying law, 2015, http://rt.com/news/269545-france-surveillance-spying-law (zadnjič obiskano: 28. 12. 2015).*

[77] *J. Baker, Choose Deutsche Telekom for all your bargain spying needs, 2015, http://www.theregister.co.uk/2015/05/21/deutsche_telekom_accused_helping_decade_long_nsa_spying_campaign/ (zadnjič obiskano: 28. 12. 2015).*

[78] *L. Harding, 2014, str. 100.*

[79] *Prav tam, str. 80.*

agencij ureja Regulation of Investigatory Powers Act[80], na kratko RIPA iz leta 2000 ter julija 2014, navkljub odločbi Sodišča EU, sprejela Data Retention and Investigatory Powers Act 2014 (DRIPA).[81] Britansko Višje sodišče je zakon julija 2015 razglasilo za nezakonit in določilo njegovo veljavnost še do marca 2016 ter s tem dalo vladi čas, da sprejme novo zakonodajo, tokrat v skladu s pravom EU.[82] Investigatory Powers Tribunal je ugotovil nezakonitost, ker so bile vladne določbe, ki so takšno izmenjavo dovoljevale, tajne. Na podlagi te sodne odločbe lahko sedaj vsak posameznik preveri, ali sta NSA in GCHQ zbirali podatke o njem na spletni povezavi: https://www.privacyinternational.org/illegalspying. Pred tem namreč posameznik ni mogel vedeti, ali sta ti dve agenciji prestrezali in zbirali tudi podatke, vezane nanj.

V svoji sodni praksi s področja ukrepov in državnih posegov v pravice posameznikov je ESČP določilo doktrino diskrecijske oblasti države, s katero se določa, da države same najbolje vedó, katere ukrepe izvesti v določenem primeru, saj te poznajo okolje, v katerem ga sprejmejo.[83] Vendar morajo pri tem upoštevati standarde in načela varstva človekovih pravic, ki izhajajo iz EKČP in sodne prakse ESČP. V zadevi Liberty v. United Kingdom[84] je sodišče dejalo, da GCHQ-jevo prestrezanje telefonskih klicev med Severno Irsko in Veliko Britanijo, temelječe na RIPA, pomeni kršitev 8. člena EKČP, saj podlaga za intervencijo ni bila javno dostopna ter s tem ni zagotavljala zadostnega varstva pred samovoljnim delovanjem.[85] Prva zadeva v zvezi z izvajanjem množičnega nadzora s strani obveščevalnih organizacij države, je zadeva Privacy International v. United Kingdom. Tu Privacy International zahteva razkritje tajnih dokumentov, ki vsebujejo dogovore o vohunjenju in deljenju teh informacij med petimi državami, in sicer med ZDA, Veliko Britanijo, Kanado, Avstralijo ter Novo Zelandijo. Gre za tako imenovano skupino »Five Eyes«. Privacy International v tožbi, vloženi v septembru 2014, navaja, da si te države med seboj delijo zasebne informacije posameznikov, ki so jih prestregle z operaci-

[80] *Regulation of Investigatory Powers Act, 2000 c. 23 iz leta 2000.*
[81] *Data Retention and Investigatory Powers Act 2014, 2014 c. 27.*
[82] *High Court of Justice, 17. 7. 2015 – opr. št. EWHC 2092: The Queen v. The Secretary of State for the Home Department-Defendant.*
[83] *R. Lampe, 2004, str. 399.*
[84] *ESČP, 1. 10. 2008 – opr. št. 58243/00: Liberty v. United Kingdom.*
[85] *I. Georgieva, The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR, Utrecht Journal of International and European Law (2015), Iss. 80, str. 120.*

jami množičnega nadzora, razkritimi s Snowdnovimi dokumenti.[86] Dodajajo, da je tajnost okoliščin in načinov, na podlagi katerih so posamezniki opazovani, nezakonita. Poleg tega imamo še eno tožbo proti Veliki Britaniji, vloženo aprila 2015, in sicer zadevo 10 Human Rights Organisations v. United Kingdom, kjer 10 organizacij za varstvo človekovih pravic zahteva prevzem odgovornosti britanske vlade glede množičnega prestrezanja, zbiranja, analiziranja, distribucije in zadržanja komunikacijskih podatkov na obsežni ravni brez primere.[87] Pravna podlaga so ponovno dokumenti, ki jih je Snowden razkril. ESČP v teh dveh zadevah še ni odločilo. Vendar kot lahko vidimo, igra ESČP pomembno vlogo pri varstvu zasebnosti posameznika. Tekom svoje sodne prakse se je velikokrat postavilo na stran pravice do zasebnosti in s tem postavilo precedense, ki imajo pomembno vlogo tudi v prihodnje. Po vsej verjetnosti bo kritično tudi do množičnega nadzora, ki so ga izvajale obveščevalno-varnostne agencije. V obeh omenjenih primerih, kjer se organizacije za človekove pravice borijo proti Veliki Britaniji, se bo tako postavilo na stran prvih in ugotovilo kršitev konvencije ter nezakonitost dejanj vladnih organizacij.

Na ameriških tleh je počasno izboljšanje razmer razvidno iz zamenjave USA PATRIOT Act-a z USA FREEDOM Act-om v začetku junija 2015. S slednjim se je omejilo množične posege v pravico do zasebnosti in določilo počasno omejevanje tovrstnih programov NSA, vendar še vedno ni povsem prepovedalo izvajanje nadzora. Takšna odločitev ameriškega zakonodajalca je odgovor v pravi smeri, saj v nasprotnem primeru ne moremo govoriti o učinkovitem delovanju pravne države oziroma načela »Rule of law« ter o temeljitem spoštovanju temeljnih človekovih pravic in svoboščin. Stanje, v katerem so bile ZDA pred tem, ko so imele obveščevalne agencije pravico samovoljno in množično posegati v zasebnost posameznika brez utemeljenega suma, ni daleč od ureditve totalitarnih režimov in tajne policije, ki jih je Hannah Arendt opisala v delu Izvori totalitarizma. Za dodaten napredek in približanje ureditvi, kot jo poznamo v večini evropskih držav,

[86] *Privacy International v. United Kingdom, 2015, https://www.privacyinternational.org/?q=node/83 (zadnjič obiskano: 28. 12. 2015).*

[87] *Te organizacije so American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre, Liberty, Privacy International. The European Court of Human Rights Application: 10 Human Rights Organisations v United Kingdom: Additional Submissions on the Facts and Complaints, 2015, https://www.amnesty.org/en/documents/ior60/1415/2015/en/ (zadnjič obiskano: 28. 12. 2015).*

bo kot kaže potrebna »pomoč« Vrhovnega sodišča ZDA. Primeri, v katerih so obravnavali operacije, podobne tistim, ki so jih obveščevalne agencije izvajale v skladu z množičnim nadzorom, so bili v večini primerov kritizirani in razglašeni za neskladne z določbami četrtega amandmaja ameriške ustave, ki ureja pravico do zasebnosti. Argumentacije vrhovnih sodnikov ZDA v zvezi z zaščito pravice do zasebnosti na podlagi četrtega amandmaja so bile v večini primerov pozitivne. Kritično so se odzvali na primere nadziranja in beleženja lokacije GPS-sistemov in s tem posameznika (sodnik Alito v zadevi Jones) ter na primere zbiranja podatkov in metapodatkov iz pametnih telefonov, ki s tem razkrijejo veliko informacij iz zasebnega življenja posameznika (sodnik Roberts v zadevi Riley). Poudariti je potrebno, da se te odločitve nanašajo na ozko področje delovanja organov pregona in ne na izvajanje množičnega nadzora s strani NSA. Vsekakor bo vredno slediti zadevam, ki se zaenkrat odvijajo pred ameriškimi sodišči nižjih instanc in kjer posamezniki ter razne organizacije za človekove pravice tožijo vlado ZDA v zvezi z množičnim nadzorom. Počakati je potrebno, da ena izmed teh zadev[88] končno pride do Vrhovnega sodišča ZDA. Ko se bo to zgodilo, bomo dobili dokončen odgovor na vprašanje, ki ga vsi pričakujemo – ali bodo v ZDA državne posege v zasebnost posameznika na področju informacijske tehnologije obsodili in razglasili za protiustavne ali ne. Glede na dosedanjo sodno prakso Vrhovnega sodišča ZDA in pomembnost vloge, ki jo je imelo za varstvo ustavnih pravic posameznikov skozi svojo celotno zgodovino, bo imela odločitev zelo pomembne in daljnosežne posledice. O izidu lahko zgolj ugibamo, vendar bi moralo Vrhovno sodišče ZDA ob upoštevanju mnenja predsedujočega sodnika Robertsa in sodeč po nedavnih odločitvah ugotoviti kršitev. Roberts je namreč v zadevi Riley poudaril, da predstavlja razumnost temeljni kriterij četrtega amandmaja. Nepravilna uporaba slednje vodi v nerazumnost, ki pušča dvome glede mejá legitimnih državnih interesov in nedopustnih posegov v zasebnost.

[88] *Tožbe zoper NSA in ameriško vlado zaradi izvajanja množičnega nadzora so številne. Med njimi najdemo zadeve: ACLU v. NSA (zavržena 2007); Shubert v. Obama; First Unitarian Church of Los Angeles v. NSA; Wikimedia v. NSA (zavržena 23.10.15); Jewel v. NSA; ACLU v. Clapper; Smith v. Obama. Vse so bodisi zavržene bodisi zavrnjene ali pa so še v fazi odločanja. Izjema je zadeva Klayman v. Obama, kjer je sodnik 9.11.2015 ugotovil neustavnost množičnega nadzora NSA z ameriško ustavo. Gre za prvi primer na nižji sodni instanci v ZDA, kjer je sodišče ugotovilo tovrstno neskladnost z ustavo.*

7. Priporočila in ureditev v prihodnosti

Po natančnem in obsežnem pregledu teorije in prakse ter same zakonske ureditve in sodne prakse mednarodnih in nacionalnih sodišč lahko povem, da je potrebno še kar nekaj dela, če želimo stvari urediti in doseči ponovno upoštevanje načel demokratične in pravne države ter pomagati ljudem pridobiti nazaj zaupanje v pravo in učinkovito varstvo njihov pravic. Glede na zakonodajo in sodno prakso najvišjih sodišč, tako ZDA kot evropskih držav in Sodišča EU, je razvidno, da se stvari počasi normalizirajo in vračajo nazaj na stare tire. Vendar je zaupanje, ko se ga enkrat izgubi, veliko težje pridobiti nazaj. Z opravljeno anketo je razvidno, da je velika večina anketiranih izgubila zaupanje v učinkovito pravno varstvo pravice do zasebnosti na področju informacijske tehnologije.

Zato predlagam naslednje izboljšave in spremembe, za katere menim, da lahko pomagajo pri obstoječi situaciji in na podlagi katerih se lahko sčasoma med ljudmi povrne zaupanje v pravo in učinkovito varstvo človekovih pravic. Menim, da je potrebna 1) večja transparentnost delovanja, ki omogoča nadzor javnosti nad oblastjo in s tem zagotavlja varstvo pred njihovim samovoljnim delovanjem; 2) sprejetje ustreznejše zakonodaje, ki bo čim boljše opredelila pravice posameznikov v povezavi z informacijsko tehnologijo in ki ne bo širila pristojnosti obveščevalno-varnostnih organizacij, ampak jih omejila ter ob tem upoštevala ustavne določbe o varstvu temeljnih človekovih pravic in svoboščin; 3) višja stopnja varstva človekovih pravic, predvsem pravice do zasebnosti, saj je bila ta v zadnjem desetletju izredno slabo varovana, še posebej s strani nižjih sodnih instanc, ki preprosto niso želele inkriminirati dejanj vladnih organizacij, kar je samo zmanjševalo varstvo človekovih pravic ter zaupanje posameznikov v učinkovit sistem sodnega varstva; 4) potreba po utemeljenem sumu in sodnem nalogu ter z zakonom in ustavo skladnim izvajanjem dejavnosti nadzora, kar so najvišja nacionalna sodišča ter Sodišče EU že navedli, samo ne še pri množičnem nadzoru; 5) morda upoštevanje sodne prakse mednarodnih sodišč z zadevnega področja, čeprav ta določeno nacionalno sodišče ne zavezuje (v mislih imam predvsem ameriška sodišča nižjih sodnih instanc); 6) skrb za nacionalno varnost, vendar ne za vsako ceno in ne z vsesplošnim kršenjem pravice do zasebnosti ter ne zgolj kot izgovor za izvajanje množičnega

nadzora posameznikov; 7) doslednejše upoštevanje načela sorazmernosti, saj je le z uspešno prestanim testom sorazmernosti moč omejiti pravico do zasebnosti oziroma sprejeti zakonodajo, ki bi bila skladna z ustavo ter v povezavi s slednjim; 8) drugačni, milejši ukrepi za dosego tovrstnih ciljev – izvajanje ciljnega in ne vsesplošnega nadzora.

8. Zaključek

Vedno hitreje prehajamo iz informacijske dobe »Age of Information« v dobo interneta stvari »Internet of Things« (IoT). Tako so jo poimenovali, saj je vedno več naprav in osebnih pripomočkov povezanih z internetom. In vedno več jih bo. Če neka naprava ni povezana z internetom, vdor iz daljave brez fizične prisotnosti oziroma fizičnih pripomočkov ni mogoč. Nekoč je bil z internetom povezan samo računalnik, kar pomeni, da so drugi lahko vanj vdrli in tako dostopali do naših osebnih podatkov ter drugih informacij samo preko tega medija. Vendar se to hitro spreminja. Telefoni so bili nekoč namenjeni zgolj klicanju, nato so dodali možnost pisanja SMS-sporočil in počasi smo prišli do pametnih telefonov, ki jih posedujemo danes in katere neprestano nosimo s seboj. Ti so zelo sposobni in nam omogočajo marsikaj, od telefonskih pogovorov do pregledovanja e-pošte, brskanja po spletu in skoraj neskončnega števila raznolikih aplikacij, ki nam olajšujejo življenje. Ker so ti sedaj povezani z internetom, so možni tudi vdori vanje in s tem kraja osebnih podatkov ter omogočanje sledenja, saj imajo vgrajen GPS-oddajnik. Prav tako je dandanes z internetom povezan že marsikateri drugi osebni pripomoček. Trenutno so popularne tako imenovane pametne ure, pametna očala (Google Glass) ipd. Načrti za bližnjo prihodnost in bistvo IoT je povezati vse domače pripomočke in ustvariti nekakšen »Smart Home«, kjer je vse povezano z internetom in omogoča lažje življenje posameznikom, s tem pa tudi večjo nevarnost, ki se je mnogi niti ne zavedajo. Kmalu bomo namreč imeli pametne hladilnike, ki nam bodo povedali, kaj imamo v hladilniku, kdaj stvari poteče rok in kdaj moramo kaj kupiti. Pametne televizije, pametne klimatske in grelne naprave (razne toplotne črpalke ipd.) ter pametne varnostne naprave (kot je tista od podjetja Nest) že imamo in jih lahko upravljamo na daljavo preko pametnega telefona. Vse to res lajša življenje posamezniku, dopušča pa tudi možnost veliko večjega in

poenostavljenega posega v njegovo zasebnost. Če lahko namreč mi na daljavo dostopamo do teh informacij, lahko to storijo tudi drugi – tisti, ki imajo določeno znanje in sredstva. Mednje sodijo med drugimi tudi obveščevalne agencije. Z vidika nadaljnjega razvoja in napredka človeštva je hiter razvoj tehnologije čudovit, vendar grozljiv z vidika prava in varovanja temeljnih pravic, saj dopušča veliko hujše kršitve.

Sem velik ljubitelj tehnologije in z velikim občudovanjem gledam na marsikatere stvaritve, ki danes nastajajo dnevno. Vendar je pri tem potrebno biti previden in zlasti delovati v skladu z zakonitostjo in ustavnostjo, še posebej kadar imamo opravka s tehnologijo, saj ima ta veliko večje in daljnosežne posledice kot druga področja, predvsem zaradi velike razširjenosti in hitrosti same širitve. Pravo razvoja ne sme zavirati, vendar hkrati za njim ne sme zaostajati. Zato mora biti zakonodajalec pri hitrem razvoju informacijske tehnologije dosleden in v koraku s časom. Kot je dejal Zobec: »Pravo [...] raste iz dejstev, iz nenehno spreminjajoče se življenjske prakse – tudi vse velike kodifikacije niso nič drugega kot abstrahiran odgovor na življenje.«[89] Ker tehnologija med drugim omogoča nove načine ogrožanja človekovih pravic, je naloga prava, da zagotovi njihovo varstvo. Ob tem je potrebno paziti, da je sprejeta zakonodaja pravična. Neka zakonodaja je lahko legalna, ni pa nujno, da je tudi pravična. Pravni akti, kot je na primer ameriški PATRIOT Act, so lahko legalni, ampak daleč od tega, da bi bili tudi pravični. Ne smemo pozabiti, da pravo stremi k pravičnosti, sprejeta zakonodaja mora biti pravična za vse in ne zgolj za privilegirane posameznike.

Težava se pojavi, ko države in njene organizacije tega ne zagotavljajo oziroma ko se zakonov same ne držijo. Ravno one so dolžne postopati z integriteto, saj so drugim za zgled. Ključni problem sedanje družbe je ravno v pomanjkanju integritete, ki se kaže od ravnanja otrok samih pa do posameznikov na oblasti. Vedno manj ljudi ima v sebi čut za spoštovanje in čast[90], ki sta bila nekoč značilna in temu primerno se kaže stanje današnjih držav. Ljudje so vedno bolj pokvarjeni, družba propada, vse skupaj gre samo navzdol. Vsepovsod je vidna korupcija, zločini in taki ali

[89] *J. Zobec v: M. Avbelj (urednik): Izzivi moderne države, 2012, str. 100.*
[90] *Tsunetomo je v Hagakure dejal: »Life is not so important when forced to choose between life and integrity.« Kar bi v slovenščino prevedli kot: »Življenje ni več toliko pomembno, kadar si prisiljen izbirati med življenjem in integriteto.« Y. Tsunetomo, The Hagakure, 2002, str. 3.*

drugačni prekrški ter posegi v človekove pravice. V tej smeri je potrebno nekaj korenito spremeniti. In to čim prej. V nasprotnem primeru je družba, kot jo poznamo danes, na dolgi rok, obsojena na propad. Zgodovina nas uči, da razni totalitarni režimi in družbe, kjer primanjkuje integritete med ljudmi, ne morejo obstati za dolgo. Potrebno je upoštevati Avbljevo integralno teorijo prava in razumevanja integritete kot povezave morale in koherentnosti.[91] Slednja je bistvena za družbo. Zaradi pomanjkanja integritete pridemo v stanje, v kakršnem smo sedaj – zaradi pomanjkanja integritete pri posameznikih ti posegajo v pravice drugih posameznikov, posledično države sprejmejo zakone, ki posegajo v pravice vseh. Vrtimo se v začaranem krogu, kjer pridemo do države, ki ni več utemeljena na vladavini prava in kjer prihaja do pomanjkanja integritete pri delovanju njenih institucij, ki tako delujejo na nedemokratičen način. Če institucije delujejo s pomanjkanjem integritete, pravna država ne bo delovala. Manj kot bodo pravo spoštovali institucionalni akterji, toliko manj ga bodo spoštovali navadni državljani, kar posledično popelje do razkroja in dekadence družbe.

Za ideale pravične in demokratične družbe, utemeljene na vladavini prava, kjer se svobodo in pravico do zasebnosti spoštuje in dosledno upošteva, se je potrebno aktivno zavzemati in bojevati, saj se le tako lahko prepreči, da ta postane zgolj mrtva črka na papirju. Podbregar je dejal, da smo kot družba zelo občutljivi na omejitve človekovih pravic in zasebnosti posameznika, vendar smo za tiste, ki se dogajajo v naši bližini, navadno povsem neobčutljivi.[92] Kar želi s tem povedati, je, da v teoriji sicer kažemo interes za človekove pravice in želimo, da se te spoštuje, v praksi pa za to ne storimo ravno veliko. Še posebej, če nas njihove omejitve ne zadevajo direktno. Kršitev se lahko dogaja prav v naši bližini, pa se sploh ne bomo odzvali. To velja tudi za operacije obveščevalno-varnostnih organizacij – sumili smo, da to počnejo, pa nismo ničesar storili. Podobno bi lahko rekli za korupcijo – vsi vemo, da ta obstaja, običajno pa ne storimo ravno veliko, da bi to preprečili. Velika večina se proti temu odzove le verbalno, pa še to zgolj, kadar so v ožjem krogu prijateljev in znancev. Vsem je všeč predvsem pasivno delovanje – verbalno negodovanje, podpis kakšne

[91] *M. Avbelj v: M. Avbelj (urednik): Izzivi moderne države, 2012, str. 140–145.*
[92] *I. Podbregar v: I. Podbregar (urednik): Obveščevalno-varnostna dejavnost: procesi, metode, nadzor, 2012, str. 30.*

peticije iz udobja domačega fotelja ali kaj podobnega. Taka dejanja nam dajejo uteho, da nekaj smo pa le storili za nas in za svet okoli nas. Čeprav dejansko ni tako. Aktivno pa se noben ne želi s tem ubadati ter s tem »izgubljati časa« in si »mazati rok«. To je pokazala tudi analiza opravljene ankete, kjer se je le manjši odstotek pripravljen aktivno zavzemati za svoje pravice. Kar seveda ni prav, če želimo biti deležni sprememb in izboljšanja našega življenjskega standarda. Velikokrat je potrebno vzeti stvari v svoje roke in se sami lotiti nečesa, ne pa čakati, da to stori kdo drug. To je tudi eden večjih problemov današnje družbe. Drugi problem je, da se veliko stvari dogaja virtualno in tako ne čutimo neke povezanosti s tem. Ravno zaradi tega se mogoče nismo kot javnost burneje odzvali na ta dejanja. Podobno kot pri plačilu s kreditno kartico nimamo občutka, koliko smo porabili, ker nismo imeli denarja fizično v roki in ga nato z nakupom »izgubili«. Mogoče (verjetno) bi se drugače odzvali, če bi kot primer posega v našo zasebnost obveščevalno-varnostne agencije v naše domove namestile kamere za nadzor vsakega našega giba. Pa tovrstna dejanja niso veliko drugačna od posegov, ki smo jih bili deležni v naše pravice virtualno – preko medijev sodobne informacijske tehnologije. Zato se moramo aktivno zavzemati za svoje pravice in svojo zasebnost. Vprašati se moramo: »Če ne jaz, kdo pa?«, »Če ne danes, kaj pa v prihodnosti?«

Kljub temu lahko zaključim s pozitivno noto, saj obstajajo posamezniki in organizacije, ki so pripravljeni nekaj storiti za temeljne pravice in svoboščine vseh nas. Njim gre zahvala, da so bile vložene številne tožbe proti dejavnostim množičnega nadzora, da so bili protesti zoper takšna dejanja deležni množične udeležbe. Taki posamezniki so zasluženi, da se sedaj stvari obračajo na bolje. Vrhovno sodišče ZDA in evropska nacionalna ustavna sodišča, s Sodiščem EU na čelu, namreč postopoma, primer za primerom, rešujejo načeli demokratične in pravne države, ki sta bili v zadnjem desetletju ujetnika nacionalne varnosti in tako očitno zapostavljeni. Morda pa prihodnost le ne bo tako slaba, kot je to nakazovala sedanja praksa in še obstaja upanje za ponovno vzpostavitev harmonije in zaupanja v pravo. Vsaj kar zadeva nacionalno varnost in posameznikovo pravico do zasebnosti.