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

Pravica do zasebnosti in mobilna telefonija
David Dolinar

Article information:
To cite this document:
Dolinar, D. (2013). Pravica do zasebnosti in mobilna telefonija, Dignitas, št. 57/58, str. 70-97.

Permanent link to this doument:
https://doi.org/ 10.31601/dgnt/57/58-6

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

For Authors:
Please visit http://revije.nova-uni.si/ or contact Editors-in-Chief on publishing@nova-uni.si for more information.

Pravica do zasebnosti in mobilna telefonija

David Dolinar

1. Uvod

V današnjem času pravzaprav ne poznamo človeka, ki ne bi imel mobilnega telefona, poznamo pa jih kar nekaj, ki imajo dva telefona ali celo več. Pri nekaterih so dodatni mobilniki prevzeli funkcijo službenega telefona in zamenjali stacionarne telefone. Nekateri imajo več mobilnikov kar tako, ker jih pač lahko imajo. Vnela se je prava tekma, kdo ima boljšega, novejšega, kdo takega s štirijedrnim procesorjem in kdo lahko nanj spravi večjo količino podatkov. V dobi pametnih telefonov so poleg navadnih sporočil in klicev ti podatki tudi različne fotografije, datoteke z besedilom, videi, knjige, elektronska sporočila, glasba, različne aplikacije, filmi itd.

Tu pa nastopi pravica do zasebnosti. V času običajnih stacionarnih telefonov je bila stvar razmeroma enostavna, pogledali smo po sobi, v kateri je bil telefon, oziroma smo dobro zaprli vrata telefonske govorilnice in tako smo imeli zagotovljeno zasebnost. Z mobilnimi telefoni, predvsem pa z razvojem pametnih telefonov, na spisek možnih posegov v zasebnost poleg prisluškovanja, prestrezanja besedilnih sporočil ali kraje telefona dodajamo še cel kup drugih možnih prevar in nevšečnosti. Glede na to, da so pametni telefoni prek brezžičnega omrežja neprestano povezani s spletom, ki ga, kjer ni dostopen, zamenja mobilno omrežje, in da se tehnologija v tej panogi izredno hitro razvija, se ta spisek nenehno daljša.

Prek mobilnega telefona vsak dan prenesemo ogromne količine podatkov. O vdoru v zasebnost ne govorimo samo v primerih, ko nam kdo neposredno prisluškuje ali kako drugače očitno posega v zasebnost. O našem življenju, razmišljanju, hobijih, navadah in celo še bolj osebnih stvareh bi danes lahko veliko povedalo že

povsem nedolžno brskanje po spletu ali nalaganje izbrane aplikacije na mobilni telefon, če bi podatke o tem kdo prestregel.

Zdi se torej, da se mobilni telefoni, s tem ko postajajo vse bolj vsestranski in vsebujejo različne funkcije, vedno manj uporabljajo za klicanje in vedno bolj za brskanje po spletu, obiskovanje družabnih omrežij, slikanje itd. Prav tako se v sodobnem življenju ob popularnosti družabnih omrežij, resničnostnih oddaj ipd. zdi, da zasebnost postavljamo na stranski tir ter se ji zaradi lastnega udobja pravzaprav odpovedujemo oziroma dobiva nov pomen. Tako moramo danes vsi živeti neke vrste »reality show«. Pravica do zasebnosti je tako ena izmed bolj ogroženih človekovih pravic, in če je včasih veljala za nekaj samoumevnega, je danes (redka) dobrina.

2. Pravica do zasebnosti

2.1. Opredelitev pojma zasebnosti

Enotne definicije pravice do zasebnosti pravzaprav ni, vsak posameznik si jo namreč razlaga drugače, glede na svoje stališče, čas, prostor, družbeno vlogo, razmišljanje, situacijo, v kateri se je znašel, itd.

Zaradi pomembnosti 8. člena EKČP in Konference nordijskih pravnikov bomo uporabili definicijo pravice do zasebnosti, sprejeto v dokumentu, imenovanem Zaključki. Ta povzema ugotovitve pravnikov članic Sveta Evrope, ki so se zbrali na omenjeni konferenci.[1]

Leta 1967 je potekala Konferenca nordijskih pravnikov, kjer so se zaradi nejasne formulacije 8. člena EKČP zbrale delegacije pravnikov članic Sveta Evrope in drugih držav ter razglabljale o pravici do zasebnosti. Sprejet je bil sklepni dokument, imenovan Zaključki. »Zaključki so pomembni zato, ker se je prav na podlagi teh smernic, katerih se sodišče (ESČP) drži še danes, izoblikovala praksa ESČP glede pravice do zasebnosti na podlagi 8. člena EKČP. Zaključki nam služijo kot orodje v klasifikaciji pravice do zasebnosti, njenega razumevanja in samega definiranja. Tako še danes večina avtorjev (Wildhaber, Van Dijk, Breitenmoser itd.) uporablja definicijo pravice do zasebnosti, ki so jo sprejeli prav v Zaključkih konference, ali

[1] R. Lampe, Sistem pravice do zasebnosti, Bonex, Ljubljana, 2004, 377.

njeno izpeljanko.«[2] V Zaključkih so pravico do zasebnosti definirali kot »enega izmed nepogrešljivih elementov človekove sreče, ki je pravica (biti) sam, živeti svoje življenje z minimalnim vmešavanjem. Človeka varuje pred državno oblastjo, javnostjo na splošno in drugimi posamezniki. Priznana naj bo kot temeljna človekova pravica (temeljna pravica človeštva). Tako naj bi bila varovana pred posegi v družinsko življenje, dom in dopisovanje.«[3]

2.2. Pravna ureditev pravice do zasebnosti

2.2.1. Ustava RS

Kot ugotavljata Kavčič in Grad, se je »potreba po ustavnem varstvu pravice do zasebnosti povečala zlasti v zadnjih dveh desetletjih zaradi čedalje večje uporabe elektronskih tehničnih pripomočkov za neopazno poseganje v človekovo zasebnost in zbiranje informacij o njem«. Poleg 35. člena pravico do zasebnosti zagotavljajo tudi posebne določbe 36., 37. in 38. člena Ustave RS.[4]

35. člen Ustave RS

Na splošno pravico do zasebnosti zagotavlja 35. člen Ustave RS, ki ureja varstvo pravic zasebnosti in osebnostnih pravic ter določa: »Zagotovljena je nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic.«[5]

Orehar Ivanc poudarja, da je s 35. členom ustave »zagotovljeno celovito varstvo vseh pravic osebnosti, ne glede na to, ali so z ustavo izrecno urejene ali ne. Te pravice so zagotovljene vsem fizičnim osebam ne glede na to, ali so državljani RS ali tuji državljani oziroma osebe brez državljanstva in ne glede na to, ali so poslovno sposobni ali ne.«[6]

35. člen spada v poglavje človekovih pravic in temeljnih svoboščin, ki jih določa ustava, iz česar sledi, da se tudi pravica do zasebnosti (kot vse druge ustavne človekove pravice in temeljne svoboščine) po določbah 15. člena ustave uresničuje neposredno na podlagi ustave,[7] »kar pomeni, da pravica do zasebnosti tudi v sistemu civilnega prava temelji na ustavnem določilu – 35. členu,

[2] Prav tam.
[3] Prav tam. 377, 378.
[4] I. Kaučič in F. Grad, 2007, 119.
[5] Ustava RS 1991, 35. člen.
[6] M. Orehar Ivanc v L. Šturm in drugi 2002, 370 in 371.
[7] Ustava RS 1991, 15. člen.

ki samo pravico do zasebnosti v pravu nasploh tudi garantira«.[8] Prav tako ustava zagotavlja sodno varstvo človekovih pravic in temeljnih svoboščin,[9] »zagotovljeno je torej tudi civilnopravno (sodno) varstvo človekovih in s tem tudi osebnostnih pravic«.[10]

Iz povedanega izhaja, da je za pravico do zasebnosti značilen dualistični koncept njenega obravnavanja. »Dualistični zato, ker se pravica do zasebnosti v pravu pojavlja v dveh oblikah: kot osebnostna pravica (zasebnega značaja) in človekova pravica (javnopravnega značaja).«[11] Tako je dvojno varovana, saj jo obravnavamo »kot osebnostno pravico, ki je varovana z instrumenti civilnega prava, ter kot človekovo pravico (javnopravnega značaja), ki je varovana z ustavo in mednarodnopravnimi dokumenti«.[12] V smislu zasebnega prava je varovana neposredno na podlagi ustave, v javnopravnem pojmovanju pa je samostojna pravica tako ustavnega kot evropskega (mednarodnega) prava na podlagi 8. člena EKČP.[13]

36. člen Ustave RS

36. člen ureja nedotakljivost stanovanja in določa: »Stanovanje je nedotakljivo. Nihče ne sme brez odločbe sodišča proti volji stanovalca vstopiti v tuje stanovanje ali v druge tuje prostore, niti jih ne sme preiskovati. Pri preiskavi ima pravico biti navzoč tisti, čigar stanovanje ali prostori se preiskujejo, ali njegov zastopnik. Preiskava se sme opraviti samo v navzočnosti dveh prič. Pod pogoji, ki jih določa zakon, sme uradna oseba brez odločbe sodišča vstopiti v tuje stanovanje ali v tuje prostore in izjemoma brez navzočnosti prič opraviti preiskavo, če je to neogibno potrebno, da lahko neposredno prime storilca kaznivega dejanja ali da se zavarujejo ljudje in premoženje.«[14]

Zaradi napredovanja prisluškovalne in druge nadzorovalne tehnologije je teritorialno varstvo zasebnosti danes postalo bistveno manj pomembno, saj je prostorski vidik varstva zasebnosti povsem podrejen splošnemu vidiku.[15]

[8] R. Lampe 2004, 264.
[9] Ustava RS 1991, 15. člen.
[10] R. Lampe 2004, 265.
[11] L. Toplak v L. Šturm in drugi 2002, 369.
[12] L. Toplak v L. Šturm in drugi 2002, 368.
[13] L. Toplak v L. Šturm in drugi 2002, 369, 370.
[14] Ustava RS 1991, 36. člen.
[15] B. M. Zupančič v L. Šturm in drugi 2002, 387.

37. člen Ustave RS

37. člen ureja varstvo tajnosti pisem in drugih občil ter določa: »Zagotovljena je tajnost pisem in drugih občil. Samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države.«[16]

37. člen Ustave RS je za pričujoče delo še posebej pomemben, saj ustava z njim zagotavlja pravico do komunikacijske zasebnosti. Omenjena pravica »predstavlja varstvo posameznikovega interesa, da se država ali nepovabljeni tretji ne seznanijo z vsebino sporočila, ki ga posreduje preko kateregakoli sredstva, ki omogoča izmenjavo oz. posredovanje informacij (na daljavo); kot tudi posameznikovega interesa, da ima nadzor (in svobodo) nad tem, komu, v kakšnem obsegu, na kakšen način in pod kakšnimi pogoji bo posredoval določeno sporočilo«.[17]

»Tako kot nedotakljivost stanovanja predstavlja pravica do komunikacijske zasebnosti življenjsko pomemben del splošne pravice do zasebnosti, brez katere ni mogoče govoriti o demokratični družbi, svobodi in osebni avtonomiji posameznikov.«[18]

38. člen Ustave RS

38. člen ureja varstvo osebnih podatkov in določa: »Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Vsakdo se ima pravico seznaniti z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.«[19]

Gre za informacijsko zasebnost, katere bistvo je posamezniku zagotoviti, da obdrži informacije o sebi, ker noče, da bi bili drugi seznanjeni z njimi. Ker gre za osebne podatke, so upravičenci te pravice samo fizične osebe, ne pa tudi pravne osebe.[20]

Razumno pričakovanje zasebnosti

Pomembno je omeniti tudi test razumno pričakovane zasebno-

[16] Ustava RS 1991, 37. člen.
[17] G. Klemenčič v L. Šturm in drugi 2002, 391.
[18] G. Klemenčič v L. Šturm in drugi 2002, 391.
[19] Ustava RS 1991, 38. člen.
[20] J. Čebulj v L. Šturm in drugi 2002, 409, 410.

sti (reasonable expectation of privacy). Gre za doktrino, ki izhaja iz sodne prakse. Prvič jo je leta 1967 uporabilo vrhovno sodišče ZDA v zadevi Katz. Trideset let kasneje je test uporabilo ESČP v zadevi Halford proti Združenemu kraljestvu, prevzelo pa ga je tudi naše ustavno sodišče (Odl. US VI, 158). Pri testu gre za tehtanje med dvema elementoma: pričakovanjem zasebnosti in upravičenostjo pričakovanja.[21]

Če za primer vzamemo komunikacijsko zasebnost, torej 37. člen Ustave RS, gre za poseg v zasebnost po navedenem konceptu takrat, ko posameznik pri posredovanju svojega sporočila razumno upravičeno pričakuje, da bo njegova komunikacija nenadzorovana.[22] Konkreten primer upravičenega in razumnega pričakovanja zasebnosti bi bil telefonski pogovor v javni telefonski govorilnici.[23]

»Iz tega sledi tudi ključna maksima ustavnega varovanja zasebnosti: Pravo (ustava) ne ščiti zgolj prostorov, lastnine ali lastnikov, temveč posameznike, ki v določenem trenutku, v določenem prostoru ali pri določenem ravnanju (upravičeno) pričakujejo svojo zasebnost!«[24]

2.2.2. Splošna deklaracija človekovih pravic

Splošna deklaracija človekovih pravic je bila z resolucijo št. 217 A (III) sprejeta in razglašena 10. decembra 1948. Sprejela in razglasila jo je Generalna skupščina Združenih narodov.[25] V njej so očrtane osnovne človekove pravice. »Deklaracija ni pravno zavezujoč dokument, kljub temu pa je osnova za vse mednarodnopravno zavezujoče instrumente o človekovih pravicah.«[26]

12. člen deklaracije določa: »Nikogar se ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi.«[27]

»12. člen SDČP tako predstavlja splošen pozitivnopravni temelj obstoja in priznavanja pravice do zasebnosti posameznika ter na

[21] G. Klemenčič v L. Šturm in drugi 2002, 401.
[22] G. Klemenčič v L. Šturm in drugi 2002, 401.
[23] I. Kaučič in F. Grad 2007, 121.
[24] G. Klemenčič v L. Šturm in drugi 2002, 401.
[25] Splošna deklaracija človekovih pravic, 1948.
[26] mzz.gov.si, 26. 11. 2012.
[27] Splošna deklaracija človekovih pravic 1948, 12. člen.

drugi strani obveznost obstoječega pravnega reda po spoštovanju in zagotovitvi pravnega varstva pred vmešavanjem v pravico do zasebnosti.«[28]

2.2.3. Evropska konvencija o varstvu človekovih pravic (EKČP)

EKČP je bila 4. novembra 1950 podpisana v Rimu, veljati pa je začela šele 3. septembra 1953 (Slovenija jo je ratificirala leta 1994)[29] in velja za največji dosežek Sveta Evrope.[30] Upoštevajoč Splošno deklaracijo o človekovih pravicah (1948) in cilj Sveta Evrope, »si ta deklaracija prizadeva zagotoviti splošno in učinkovito priznavanje in spoštovanje v njej razglašenih pravic«.[31] Namen konvencije je torej garancija človekovih pravic, navedenih v deklaraciji, ter njihovo institucionalno varstvo na mednarodni ravni. »Konvencija in njen mednarodni instrumentarij varstva velja v mednarodnem pravu za pionirskega ter danes za najučinkovitejši instrumentarij varstva človekovih pravic.«[32]

Konvencija v 8. členu (Pravica do spoštovanja zasebnega in družinskega življenja) določa:[33]

1. »Vsakdo ima pravico do spoštovanja njegovega zasebnega in družinskega življenja, doma in dopisovanja.«

2. »Javna oblast se ne sme vmešavati v izvrševanje te pravice, razen če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato da se prepreči nered ali kaznivo dejanje, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi.«

Na podlagi EKČP je bilo ustanovljeno Evropsko sodišče za človekove pravice[34] (ESČP). ESČP je na podlagi 8. člena EKČP prvič odločilo šele leta 1978, kar kaže na to, da strasburški organi (takrat še Komisija in Sodišče)[35] do poznih 70. let niso priznavali pravice

[28] R. Lampe 2004, 46.
[29] Slovenija EKČP ratificira z Zakonom o ratifikaciji Konvencije o varstvu človekovih pravic.
[30] R. Lampe 2004, 374.
[31] EKČP 1994, preambula.
[32] R. Lampe 2004, 374.
[33] EKČP 1994, 8. člen.
[34] »Naloga ESČP je v prvi vrsti zagotavljati, da države spoštujejo in zagotovijo spoštovanje človekovih pravic in temeljnih svoboščin iz EKČP svojim državljanom kot tudi vsakomur znotraj njihove jurisdikcije, ne glede na spol, raso, državljanstvo, etnični izvor ali drugo okoliščino« (mzz.gov.si, 28. 11. 2012).
[35] »Protokol št. 11, ki je v veljavi od 1. novembra 1998, je ukinil do tedaj delujočo Evropsko komisijo za človekove pravice, ki je bila zadolžena za predhodno selekcijo pritožb. Od uvedbe tega protokola se lahko posameznik s pritožbo obrne neposredno na Evropsko sodišče za človekove pravice (ESČP)« (mzz.gov.si, 28. 11. 2012).

do zasebnosti kot človekove pravice in je tudi niso ustrezno varovali, in sicer zaradi prevelike abstraktnosti pojmovanja 8. člena EKČP.[36]

Kljub začetnim težavam z abstraktnostjo in nejasnostmi s formulacijo je 8. člen EKČP danes izjemno pomemben. Ne samo da pravica do zasebnosti iz omenjenega člena igra pomembno vlogo v samem sistemu človekovih pravic, ampak je povezana tudi z drugimi pravicami oziroma se te pojmovno navezujejo nanjo.[37]

2.2.4. Direktive EU

Za naše obravnavanje so pomembne predvsem tri direktive:

• Direktiva 95/46/ES Evropskega parlamenta in Sveta EU o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov: »1. V skladu s to direktivo države članice varujejo temeljne pravice in svoboščine fizičnih oseb in predvsem njihovo pravico do zasebnosti pri obdelavi osebnih podatkov.«

»2. Države članice ne omejujejo niti ne prepovedujejo prostega prenosa osebnih podatkov med državami članicami zaradi razlogov, povezanih z varstvom, ki je zagotovljeno na podlagi odstavka 1.«[38]

• Direktiva 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah): »Ta direktiva določa uskladitev določb držav članic, ki je potrebna za zagotovitev enakovredne ravni varstva temeljnih pravic in svoboščin ter zlasti pravice do zasebnosti in zaupnosti v zvezi z obdelavo osebnih podatkov na področju elektronskih komunikacij in za zagotovitev prostega pretoka takih podatkov ter elektronske komunikacijske opreme in storitev v Skupnosti.« Ta direktiva pomeni nadaljevanje Direktive 95/46/ES, njene določbe omenjeno direktivo podrobneje opredeljujejo in dopolnjujejo.[39]

• Direktiva 2006/24/ES o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in o spremembi Direktive 2002/58/ES: »Namen te direktive je uskladiti

[36] R. Lampe 2004, 375.
[37] R. Lampe 2004, 375.
[38] Direktiva 95/46/ES 1995, 1. člen.
[39] Direktiva 2002/58/ES 2002, 1. člen.

določbe držav članic glede obveznosti ponudnikov javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij glede hrambe določenih podatkov, ki jih pridobivajo ali obdelujejo, da se zagotovi dostopnost podatkov za namen preprečevanja, preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, kakor jih opredeljuje nacionalna zakonodaja vsake od držav članic.«[40]

3. Mobilna telefonija

3.1. Razvoj mobilne telefonije

Prvi mobilni telefonski klic je bil izveden leta 1946, izvedli so ga pri podjetju AT&T v ZDA. Letnica velja za začetek mobilne telefonije, čeprav tedanji mobilni telefon ni bil ravno mobilni, podoben je bil današnjim mobilnikom, tehtal je kar 36 kg, vgrajen pa je bil v avtomobil. Prvi približek današnjim mobilnim telefonom je leta 1973 izdelala Motorola. Mobilni telefon z imenom Motorola Dynatac je tehtal skoraj en kilogram, brez polnjenja je deloval pol ure, polnil se je 10 ur, zaradi svoje oblike pa si je zaslužil vzdevek opeka.[41] Po letu 1982 se je pojavilo veliko podjetij, ki so proizvajala mobilne aparate, kar je povzročilo pravo mobilno revolucijo in pripeljalo do razvoja mobilnih telefonskih naprav, kakršne poznamo danes.

Razvijala pa so se tudi mobilna telefonska omrežja, ki so na začetku omogočala zgolj telefonske pogovore, medtem ko danes omogočajo videotelefonijo, dostop do svetovnega spleta praktično kjerkoli, izjemno hitre prenose podatkov in še marsikaj. Razvoj mobilnih telefonskih omrežij se trenutno deli na štiri generacije.

3.2. Zaupanje v mobilno omrežje

Eden ključnih dejavnikov za zaupanje v mobilno omrežje je prav gotovo njegova varnost. Tako je bila letos opravljena varnostna analiza slovenskih GSM-omrežij. Rezultati analize so pri slovenskih mobilnih operaterjih pokazali zaskrbljujoče varnostne pomanjkljivosti. Avtorji omenjene analize so namreč ugotovili, da bi z izrabo odkritih ranljivosti »napadalec lahko nepooblašče-

[40] Direktiva 2006/24/ES 2006, 1. člen.
[41] J. Hudoklin in drugi 2012, https://slo-tech.com/clanki/12003/, 29. 11. 2012.

no, predvsem pa nezaznavno prestrezal vsebino SMS-sporočil in pogovorov v 2G-omrežju, izvajal sledenje uporabnikom ali s pomočjo kraje identitete mobilnega uporabnika le-temu povzročal neupravičene stroške ali ga spravil v kazenski pregon«. Po mnenju avtorjev analize odkrite varnostne pomanjkljivosti »v slovenskih GSM-omrežjih omogočajo nepooblaščeno prestrezanje komunikacij tako s strani kriminalnih združb kot tudi tujih ter domačih varnostno-obveščevalnih organov«. Namen varnostne analize je bil delno dosežen, saj so po objavi rezultatov na spletu nekateri operaterji najhujše pomanjkljivosti že uspešno odpravili.[42]

V nadaljevanju predstavljamo dve možnosti zlorab omrežja, ki jih avtor v članku, v katerem jih opisuje, tudi dejansko izvede in podrobno opiše. Za obravnavano temo natančen opis izvedbe ni potreben, zato podajamo samo pomembna dejstva in zaključke.

3.2.1. Pošiljanje besedilnih sporočil s poljubno identifikacijo pošiljatelja

Gre za pošiljanje SMS-sporočil s spremenjeno identifikacijo pošiljatelja ali, povedano drugače, za pošiljanje SMS-sporočil s poljubne številke. Naslovniku je namreč možno poslati besedilno sporočilo (SMS) tako, da ta ne bo vedel, kdo mu ga je poslal oziroma se bo na njegovem mobilniku kot pošiljatelj izpisal kdo drug ali druga številka. Kot v svojem članku pravi Kovačič, je to celo »otročje lahko, saj za to praktično ni potrebno nikakršno poznavanje tehnologije. Vse, kar mora potencialni napadalec narediti, je, da na spletu poišče ustreznega ponudnika pošiljanja SMS-sporočil.« Obstajajo namreč ponudniki pošiljanja SMS-sporočil, ki prek preprostega spletnega servisa omogočajo avtomatizirano pošiljanje večjega števila besedilnih sporočil. Tovrstne storitve so, če se ne zlorabljajo, nekaj povsem običajnega, praviloma pa jih uporabljajo podjetja, ki prek sporočil strankam in drugim pošiljajo obvestila, reklame itd. Kovačič v članku celoten postopek razloži in prikaže ter zaključi: »Pošiljanje SMS-sporočil s poljubno identifikacijo pošiljatelja je torej povsem enostavno, z malce truda pa ga je mogoče izvesti tudi povsem anonimno.«[43]

[42] M. Kovačič 2012, http://hr-cjpc.si/pravokator/index.php/2012/06/16/varnost-slovenskih-gsm-omrezij/, 17. 12. 2012.
[43] M. Kovačič 2012, http://hr-cjpc.si/pravokator/index.php/2012/03/18/ko-poklicejo-hekerji-spreminjanje-klicne-identifikacije-telefonskih-klicev/, 17. 12. 2012.

3.2.2. Klicanje s poljubno klicno identifikacijo

Gre za podoben koncept, kot je opisan zgoraj, le da tu ne gre za besedilna sporočila, ampak za govorne klice. Zanimivo je tudi, da »spreminjanje klicne identifikacije samo po sebi ni prepovedano in se ta tehnologija v praksi tudi razmeroma pogosto uporablja. Tipičen primer so različni klicni centri, kjer so telefoni posameznih operaterjev v centru nastavljeni tako, da se kot njihova klicna identifikacija prikazuje telefonska številka centrale ali npr. vodje centra.«[44]

Klicanje s poljubno klicno identifikacijo na srečo ni tako preprosto kot pošiljanje besedilnih sporočil. Kljub temu je tako klicanje možno in tehnično povsem izvedljivo. »Kličemo lahko s poljubne številke, tudi iz lastne ali celo povsem izmišljene, npr. 1116.« Še bolj zaskrbljujoče je, kot ugotavljajo avtorji prispevka na spletni strani Dispatch Magazine On-Line, da »tehnični ukrepi proti spreminjanju klicne identifikacije niso mogoči, je pa včasih mogoče naknadno ugotavljati izvor klica«.[45]

Tovrstne zlorabe so nepridipravi že uporabljali. Pred kratkim se je to zgodilo v Veliki Britaniji, kjer so »neznani napadalci s pomočjo spremenjene klicne identifikacije izvajali masovno klicanje posameznikov (tudi do 1000 klicev na uro). Napadalci so uporabljali klicne identifikacije obstoječih podjetij ter klicne identifikacije neobstoječih številk (kar je številne klicane osebe prestrašilo), zvezo pa so vzpostavili le toliko, da je klicana številka pozvonila, nato so prekinili. Domnevno naj bi bil razlog takega početja preverjanje, katere telefonske številke sploh obstajajo (tim. *pinging*), te podatke pa bi napadalci nato lahko prodali marketinškim podjetjem za potrebe nelegalnega oglaševanja.«[46]

3.2.3. Zakonska ureditev

Pri opisanem gre torej za varnost omrežja oziroma varnost storitev, ki jih ponudniki ponujajo, ter za pravilnost delovanja, za kar morajo tudi ustrezno poskrbeti. To ureja Zakon o elektronskih

[44] M. Kovačič 2012, http://hr-cjpc.si/pravokator/index.php/2012/03/18/ko-poklicejo-hekerji-spreminjanje-klicne-identifikacije-telefonskih-klicev/, 17. 12. 2012.
[45] M. Kovačič 2012, http://hr-cjpc.si/pravokator/index.php/2012/03/18/ko-poklicejo-hekerji-spreminjanje-klicne-identifikacije-telefonskih-klicev/, 17. 12. 2012.
[46] M. Kovačič 2012, http://hr-cjpc.si/pravokator/index.php/2012/03/18/ko-poklicejo-hekerji-spreminjanje-klicne-identifikacije-telefonskih-klicev/, 17. 12. 2012.

komunikacijah ZEKom-1.[47] V 145. členu natančneje določa: »Izvajalci javnih komunikacijskih storitev morajo sprejeti ustrezne tehnične in organizacijske ukrepe za zagotovitev zavarovanja svojih storitev. Če je potrebno, za zagotovitev zavarovanja svojih storitev v delu, ki se nanaša na varnost omrežja, sprejmejo ustrezne tehnične in organizacijske ukrepe skupaj s ponudnikom javnega komunikacijskega omrežja.« Ti ukrepi »morajo ob upoštevanju tehnološkega razvoja in stroškov njihove izvedbe zagotoviti takšno raven varnosti in zavarovanja, ki ustreza predvidenemu tveganju. Tveganje predstavlja vsako dejanje, vsaka storitev ali vsak izdelek, ki posega v tajnost, zaupnost in varnost elektronskega komunikacijskega omrežja ali elektronske komunikacijske storitve, medtem ko spremeni dostopnost, vsebino, ceno ali kakovost storitve, in ki ga lahko operater sam ali skupaj z drugimi operaterji učinkovito onemogoči.«[48]

Če pride do posebnega tveganja za varnost omrežja, morajo biti uporabniki o tem obveščeni. Zakon namreč v 1. odstavku 146. člena določa: »Pri posebnem tveganju za varnost omrežja mora izvajalec javnih komunikacijskih storitev takoj, ko izve za tveganje, z objavo na svojih spletnih straneh in na drug primeren način obvestiti naročnike o takem tveganju. Če tveganje presega obseg ukrepov, ki jih izvajalec storitve lahko sprejme, mora hkrati obvestiti naročnike o vseh možnih sredstvih za odpravo tveganja, vključno z navedbo verjetnih stroškov, ter jim omogočiti hiter in učinkovit dostop do zaščitnih ukrepov.« Glede stroškov 2. odstavek istega člena določa: »Pri zlorabah, ki jih storijo tretje osebe in ki niso nastale po krivdi naročnikov ali uporabnikov, izvajalci javnih komunikacijskih storitev prevzamejo stroške zagotavljanja javnih komunikacijskih storitev, ki jim nastanejo kot posledica teh zlorab.«[49]

Spremenjene identitete oziroma, kot omenjamo zgoraj, poljubne identifikacije zakon neposredno ne ureja. Omogoča samo preprečitev prikaza identitete priključka, s katerega klicatelj kliče. ZEKom-1 v 1. odstavku 154. člena tako določa: »Če izvajalec storitve nudi prikaz identitete kličočega priključka, mora imeti kličoči uporabnik pred vsakim klicem možnost, da sam z enostavnimi sredstvi in brezplačno prepreči prikaz identitete priključka, s katerega kliče. Naročnik od izvajalca elektronskih komunikacijskih storitev lahko

[47] Ur. l. RS, št. 109/2012.
[48] ZEKom-1 2012, 145. člen.
[49] ZEKom-1 2012, 146. člen.

to zahteva avtomatično in brezplačno za vse klice s svojih priključkov.« Preprečitev prikaza omenjene identitete morajo operaterji brezplačno razveljaviti pri klicih na številko za klic v sili.[50]

Pri tem za primere zlorab in nadlegovanj 155. člen določa: »Če naročnik pisno zahteva od operaterja, da izsledi zanj zlonamerne ali nadležne klice, sme operater začasno, vendar največ tri mesece, beležiti izvor vseh klicev, ki se zaključijo v omrežni priključni točki tega naročnika, tudi tistih, za katere se zahteva preprečitev prikaza identitete kličočega priključka.«[51]

Prav tako je »uporaba samodejnih klicnih in komunikacijskih sistemov za opravljanje klicev na naročnikovo telefonsko številko brez človekovega posredovanja (npr. klicni avtomati, SMS-i, MMS-i), telefaksov ali elektronske pošte za namene neposrednega trženja dovoljena samo na podlagi naročnikovega ali uporabnikovega predhodnega soglasja.«[52]

3.3. Pametni telefon

Pametni telefon je pojem, ki ga je zaradi hitrega napredka težko definirati. Današnji pametni telefoni bodo čez nekaj let le še običajni telefoni. Opredelitev, ki bi nekako ustrezala današnjemu času, je, da je pametni telefon naprava, ki omogoča običajno telefonsko klicanje, hkrati pa ima funkcije, ki smo jih lahko v preteklosti zasledili zgolj pri dlančnikih in računalnikih, torej pošiljanje elektronskih sporočil, urejanje dokumentov, nalaganje programov oziroma aplikacij itd.[53]

Pametni telefoni so znani po svoji vsestranskosti. Naprava, ki se lahko uporablja kot plačilno sredstvo, čitalec črtnih kod in satelitska navigacija, omogoča pošiljanje elektronskih sporočil ter dostop do socialnih omrežij in spleta prek brezžične spletne povezave; poleg tega lahko z njo opravimo tudi telefonski klic. Nekateri srčni bolniki pametne telefone uporabljajo kot pametne zdravstvene senzorje (»smart-health sensors«), ki jim omogočajo, da živijo varno tudi zunaj bolnišnice, saj zdravniki njihovo bolezen opazujejo in nadzorujejo prek senzorjev.[54]

Tovrstni telefoni s svojimi funkcijami igrajo vedno pomemb-

[50] ZEKom-1 2012, 154. člen.
[51] ZEKom-1 2012, 155. člen.
[52] ZEKom-1 2012, 158. člen.
[53] L. Cassavoy, http://cellphones.about.com/od/smartphonebasics/a/what_is_smart.htm, 5. 11. 2012, prevedel Dolinar.
[54] ENISA 2010, 10, prevedel Dolinar.

nejšo vlogo v življenju uporabnika in vdirajo v vedno več segmentov njegovega delovanja. Razvoj v tem segmentu je izjemno hiter in ne kaže, da bi se kaj kmalu ustavil. Nekateri celo napovedujejo, da bodo v prihodnosti pametni telefoni, tablični računalniki in druga elektronika povezovali praktično vse, od avtomobilov in zdravstvenih storitev do celotnih mest.[55]

Omeniti je še treba, da se mobilni telefoni vedno bolj pogosto uporabljajo za obiskovanje spletnih strani, družabnih omrežij ipd., kar na seznam možnih nevarnosti za poseg v zasebnost na pametnih mobilnikih dodaja še nevarnosti, ki izhajajo iz samega svetovnega spleta.

Kot primer naj navedemo, da, sodeč po raziskavah v ZDA, kar 17 odstotkov uporabnikov mobilnih telefonov večino brskanja po spletu opravi prav prek telefona.[56] Poleg tega naj bi po mnenju podjetja Gartner[57] do leta 2013 mobilni telefoni postali najpogosteje uporabljena naprava za dostop do spleta, prehiteli naj bi celo običajne računalnike.[58]

3.4. Podatki o prometu

Kaj besedna zveza podatki o prometu sploh pomeni, nam razloži 45. točka 3. člena ZEKom-1, ki pravi: »Podatki o prometu so katerikoli podatki, obdelani za namen prenosa komunikacije po elektronskem komunikacijskem omrežju ali zaradi njegovega zaračunavanja.«[59]

ZEKom-1 hrambo podatkov o prometu sicer ureja v poglavju hramba podatkov (od 162. do vključno 169. člena ZEKom-1), vendar je treba še prej omeniti nekaj določb.

V 147. členu zakon opredeljuje zaupnost komunikacij in določa: »S tem zakonom se zaupnost komunikacij zagotavlja z namenom varovanja pričakovane zasebnosti na področju uporabe elektronskih komunikacij, zagotavljanja svobode komuniciranja in svobode izražanja.« Zaupnost komunikacij zajema tako vsebino komunikacij kot tudi podatke o prometu in lokaciji, ki so povezani z njo.[60]

[55] M. O Hara v A. Andrenšek 2012, http://www.dnevnik.si/objektiv/vec-vsebin/1042513900, 5. 11. 2012.
[56] ris.org 2012, 17. 12. 2012.
[57] Gartner, Inc. je vodilno svetovno podjetje, ki se ukvarja s svetovanjem in z raziskavami na področju informacijske tehnologije (gartner.com, 5. 1. 2013).
[58] Gartner v ISACA 2010, 4, prevedel Dolinar.
[59] ZEKom-1 2012, 3. člen.
[60] ZEKom-1 2012, 147. člen.

2. odstavek istega člena še dodaja, da mora operater oziroma vsakdo, ki sodeluje pri zagotavljanju in izvajanju njegove dejavnosti, varovati zaupnost komunikacij tudi po prenehanju opravljanja dejavnosti, pri kateri je bil zavezan k varovanju zaupnosti.[61]

Po 151. členu ZEKom-1 morajo, razen v primeru podatkov, za katere je po tem zakonu določen daljši čas hrambe, biti podatki o prometu, ki se nanašajo na naročnike in uporabnike ter jih je operater obdelal in shranil, izbrisani ali spremenjeni takoj, ko niso več potrebni za prenos sporočil, in to tako, da jih ni mogoče povezati z določeno ali določljivo osebo. Isti člen v nadaljnjih odstavkih opredeljuje še nekatere izjeme in pogoje, ki jih morajo izvajalci upoštevati ob rokovanju s tovrstnimi podatki.[62]

Obvezno hrambo prometnih podatkov nalaga 163. člen ZEKom-1: »Operater mora za namene pridobivanja podatkov[63] v javnem komunikacijskem omrežju, ki jih določa zakon, ki ureja kazenski postopek, za namene zagotavljanja nacionalne varnosti in ustavne ureditve ter varnostnih, političnih in gospodarskih interesov države, kakor jih določa zakon, ki ureja slovensko obveščevalno-varnostno agencijo, in za obrambo države, kakor jih določa zakon, ki ureja obrambo države, hraniti podatke iz 164. člena tega zakona, če jih ustvari ali obdela pri zagotavljanju z njimi povezanih javnih komunikacijskih storitev.« Omenjeni podatki se hranijo za določen čas, in sicer za čas 14 mesecev od dneva komunikacije, če gre za podatke v zvezi z javno dostopnimi telefonskimi storitvami, in 8 mesecev, če gre za druge podatke. Ob koncu hrambe morajo operaterji uničiti vse podatke, hranjene v skladu z določbami poglavja o hrambi podatkov, razen tistih, ki so bili na podlagi odredbe za dostop posredovani pristojnemu organu.[64]

Katere podatke oziroma vrste podatkov je treba hraniti, natančno opredeljuje in našteva 164. člen.[65]

Glede zaščite hranjenih podatkov zakon določa, da so operaterji dolžni sprejeti ukrepe za zaščito teh podatkov pred uničenjem, izgubo, spremembo ter nepooblaščenimi ali nezakonitimi oblikami hrambe, obdelave, dostopa ali razkritja in zagotoviti varovanje

[61] ZEKom-1 2012, 147. člen.
[62] ZEKom-1 2012, 151. člen.
[63] Ne glede na 3. člen in njegovo opredelitev podatkov o prometu podatki za potrebe tega poglavja (od 162. do 169. člena ZEKom-1) po 162. členu »pomenijo podatke o prometu in lokaciji ter povezane podatke, potrebne za določitev naročnika ali uporabnika« (ZEKom-1 2012, 162. člen).
[64] ZEKom-1 2012, 163. člen.
[65] ZEKom-1 2012, 164. člen.

hranjenih podatkov v skladu z zakonom, ki ureja varstvo osebnih podatkov.[66]

Kar se tiče posredovanja podatkov, mora operater hranjene podatke takoj in brez nepotrebnega odlašanja posredovati pristojnim organom na način in v obsegu, kot je določeno v odredbi.[67]

S sprejetjem Direktive 2006/24/ES je bila uveljavljena obvezna hramba prometnih podatkov. Pred njenim sprejetjem je veljala Direktiva 2002/58/ES, na podlagi katere se prometnih podatkov (razen za določene potrebe) ni smelo shranjevati brez soglasja uporabnika oziroma naročnika. Enako je določal tudi Zakon o elektronskih komunikacijah (ZEKom[68]), ki je bil sprejet na podlagi Direktive 2002/58/ES – kasneje ga je spremenila Direktiva 2006/24/ES.

3.4.1. Kritika obvezne hrambe podatkov o prometu

Sprejemanje Direktive 2006/24/ES so spremljali številni protesti in zapleti. Nasprotovala ji je namreč tako posebna komisija Evropskega parlamenta,[69] ki je predlog zavrnila,[70] kot tudi Evropski parlament.[71] Pomisleke je imela tudi delovna skupina za varstvo podatkov iz člena 29[72], ki jih je v zadnjem mnenju DS 113 z dne 21. oktobra 2005 o tedanjem osnutku direktive tudi izrazila in zapisala, da »bodo imele določbe direktive daljnosežne posledice za vse evropske državljane in njihovo zasebnost. Odločitev o hrambi komunikacijskih podatkov za namen boja proti hudim kaznivim dejanjem je prvi takšen primer in ima zgodovinski pomen. Posega v vsakdanjik vsakega državljana in lahko ogrozi temeljne vrednote in svoboščine, ki jih uživajo in cenijo vsi evropski državljani.«[73]

Po Kovačičevem mnenju gre pri obveznem shranjevanju prometnih podatkov »za načelno vprašanje beleženja osebnih po-

[66] ZEKom-1 2012, 165. člen.
[67] ZEKom-1 2012, 166. člen.
[68] Ur. l. RS, št. 43/2004.
[69] Gre za Alvarovo komisijo. Ime je dobila po vodji komisije, sicer evropskemu poslancu, poročevalcu komiteja evropskega parlamenta za civilne svoboščine, pravosodje in notranje zadeve Alexandru Alvaru (Kovačič 2007, 251).
[70] A. Alvaro v M. Kovačič 2007, 251.
[71] M. Kovačič 2007, 251.
[72] »Ta delovna skupina je bila ustanovljena v skladu z 29. členom Direktive 95/46/ES. Je neodvisen evropski svetovalni organ na področju varstva podatkov in zasebnosti. Njene naloge so opisane v 30. členu Direktive 95/46/ES in členu 15 Direktive 2002/58/ES« (Delovna skupina za varstvo podatkov iz člena 29, 2006, 1).
[73] Delovna skupina za varstvo podatkov iz člena 29, 2006, 2.

datkov oseb, ki niso ničesar osumljene, ob dejstvu, da je mogoče te podatke kdaj kasneje uporabiti v postopku proti njim«. Kot ugotavlja Kovačič, je bil tovrsten elektronski nadzor »do sprejema omenjene direktive mogoč le kot nekakšen skrajni ukrep, uperjen proti osumljencem najhujših kaznivih dejanj. S sprejemom direktive tarče tega ukrepa postajamo vsi uporabniki komunikacijskih sredstev.«[74]

Nemško ustavno sodišče je leta 2010 na Direktivi 2006/24/ES temelječ nemški zakon o obvezni hrambi prometnih podatkov celo razveljavilo in odredilo, da je treba vse shranjene prometne podatke nemudoma izbrisati. »Po mnenju sodišča namreč nemški zakon ne vsebuje ustreznih mehanizmov za preprečevanje neupravičenih posegov v zasebnost in je v neskladju tako z nemško ustavo kot tudi z 8. in 10. členom Evropske konvencije o človekovih pravicah, ki zagotavljata pravico do zasebnosti in svobodo izražanja.«[75]

Sodišče dodaja, da obvezna hramba prometnih podatkov, ki jo narekuje Direktiva 2006/24/ES, sama po sebi sicer ni neustavna, problem predstavlja le njena zakonodajna implementacija. Po mnenju sodišča bi »morala biti uporaba shranjenih prometnih podatkov omejena le na zločine, ki neposredno ogrožajo življenje ali telo posameznikov, ter zločine, ki predstavljajo neposredno nevarnost za varnost države«, podatkov pa, kot še dodaja, »ne bi smeli uporabljati v »splošne« varnostno-obveščevalne namene«.[76]

Pravilnost razsodbe nemškega ustavnega sodišča je posredno potrdil nemški Inštitut Max Planck, ki je leta 2011 opravil raziskavo o vplivu hrambe prometnih podatkov na boj proti kriminalu. »Odkrili so, da ukrepi hranjenja prometnih podatkov ne pripomorejo k večji preiskanosti ali preventivi pred kriminalnimi dejanji, zato niso smiselni.«[77]

Na drugi strani po mnenju zagovornikov hrambe prometnih podatkov ne gre za hud poseg v zasebnost, kot je na primer prisluškovanje, prometni podatki pa so nujni za preganjanje novih oblik kriminala. Kot ugotavlja Kovačič: »Vsekakor drži, da je brez prometnih podatkov odkrivanje kakršnegakoli kiberkriminala bistveno

[74] M. Kovačič 2007, 252.
[75] B. Kvas 2010, http://www.e-demokracija.si/2010/03/08/nemcija-sodisce-razveljavilo-zakon-o-obvezni-hrambi-prometnih-podatkov/, 9. 11. 2012.
[76] B. Kvas 2010, http://www.e-demokracija.si/2010/03/08/nemcija-sodisce-razveljavilo-zakon-o-obvezni-hrambi-prometnih-podatkov/, 9. 11. 2012.
[77] M. Huš 2012, https://slo-tech.com/novice/t504584, 9. 11. 2012.

oteženo, morda celo nemogoče. Kljub temu je mogoče analizo prometnih podatkov uporabiti (zlorabiti) za iskanje vzorcev »sumljivih« dejavnosti ter predvidevanje, kar pomeni hud poseg v človekovo zasebnost in svobodo. Tovrstni podatkovni nadzor je mogoče izvajati v velikem obsegu in povsem nezaznavno, predvsem pa ga je moč avtomatizirati. Prometne podatke je namreč za razliko od prisluhov vsebine glasovne komunikacije mogoče analizirati z metodami izkopavanja podatkov, zato hramba prometnih podatkov v mobilni telefoniji predstavlja veliko grožnjo zasebnosti.«[78]

Kljub vsemu je bila decembra 2005 direktiva o obvezni hrambi prometnih podatkov sprejeta, aprila 2006 pa tudi objavljena v uradnem listu EU.[79]

3.4.2. Podatki o lokaciji

Podatki o lokaciji so podatki o lokaciji mobilnega telefona ali druge naprave. Po Zakonu o elektronskih komunikacijah so to »vsakršni podatki, obdelani v elektronskem komunikacijskem omrežju ali v okviru elektronske komunikacijske storitve, ki kažejo na zemljepisni položaj terminalske opreme uporabnika javno dostopne elektronske komunikacijske storitve«.[80]

Lokacijski podatki spadajo pod podatke o prometu, vendar pa zakon pozna tudi lokacijske podatke, ki niso hkrati podatki o prometu. V zvezi z njimi v 152. členu določa, da se sme tovrstne podatke obdelovati le v takšni obliki, da jih ni možno povezati z določeno ali določljivo osebo, ali na podlagi soglasja uporabnika ali naročnika v obsegu in trajanju, potrebnem za izvedbo storitve z dodano vrednostjo. To soglasje lahko uporabnik ali naročnik kadarkoli prekliče.[81]

Tudi če je uporabnik ali naročnik zavrnil obdelavo podatkov ali ni izdal soglasja za njihovo obdelavo, mora operater lokacijske podatke posredovati pristojnim organom v primeru klicev na enotno evropsko številko za klice v sili 112 ali številko policije 113.[82]

Podatki o lokaciji mobilnega telefona so precej kočljiva zadeva, saj lahko njihova zloraba pomeni hud poseg v zasebnost, medtem

[78] M. Kovačič 2007, 254.
[79] M. Kovačič 2007, 251.
[80] ZEKom-1 2012, 3. člen.
[81] ZEKom-1 2012, 152. člen.
[82] ZEKom-1 2012, 152. člen.

ko se po drugi strani na njihovi podlagi rešujejo življenja. To predvideva tudi ZEKom-1, ki v 153. členu določa posredovanje prometnih in lokacijskih podatkov v primerih varovanja življenja in telesa. Tako določa, da mora operater v primerih, ko gre za varstvo življenjskih interesov posameznika, policiji posredovati podatke, ki so potrebni za ugotovitev zadnje lokacije opreme za mobilno komunikacijo, če je to glede na okoliščine nujno, pri čemer v nadaljevanju istega člena našteva tudi primere oziroma okoliščine, v katerih je posredovanje teh podatkov nujno.[83]

Na eni strani se torej lokacijski podatki uporabljajo v primerih, ko je lahko ogroženo življenje, kot bi se lahko na primer pri poplavah v Železnikih, kjer je policija iskala tri pogrešane osebe. Operativni štab policijske uprave Kranj je operaterja mobilne telefonije zaprosil, naj mu posreduje podatke o lokaciji mobilnega telefona ene izmed oseb. V tem primeru operater zaradi zakonskih pomislekov podatkov sicer ni posredoval, pogrešana oseba pa je bila kasneje najdena mrtva nekaj sto metrov od bivališča.[84]

Kljub temu lahko tovrstni podatki omogočajo tudi njihovo zlorabo v nezakonite namene, kar je počel britanski mobilni operater Virgin Mobile, ki je leta 2001 priznal, da je hranil podatke o prometu in lokaciji uporabnikov za neomejen čas. Podatke je potreboval za opravljanje analize o obremenjenosti omrežja.[85]

3.5. Komunikacijska zasebnost na delovnem mestu

ISACA[86] v svojem poročilu ugotavlja, da z vpeljavo mobilnih naprav[87] v poslovni svet podjetja opažajo večanje produktivnosti zaposlenih.[88] Študija raziskovalne skupine Aberdeen Group je pri najboljših podjetjih pokazala celo 40-odstotno rast stopnje produktivnosti.[89]

S tega naslova je komunikacijska zasebnost na delovnem mestu vsekakor eden izmed pomembnejših vidikov obravnavanja pravice do zasebnosti. Pri tej temi gre za vprašanje, kaj zaposleni

[83] ZEKom-1 2012, 153. člen.
[84] B. Mekina 2008, http://www.mladina.si/92678/vse-pod-nadzorom/, 13. 11. 2012.
[85] G. Wearden v M. Kovačič 2007, 254.
[86] »Neprofitno, neodvisno člansko združenje ISACA je vodilni globalni ponudnik znanja, certifikacij, skupnosti, zagovorništva in izobraževanja o zagotavljanju, nadzoru in varnosti informacijskih sistemov, vodenju IT v podjetjih ter z IT povezanih tveganjih in skladnostjo« (isaca.si, 3. 1. 2013).
[87] V poročilu so kot mobilne naprave mišljeni pametni telefoni, prenosni in tablični računalniki, digitalne kamere, naprave z infrardečo povezavo in še nekatere druge.
[88] ISACA 2010, 4, prevedel Dolinar.
[89] Aberdeen Group v ISACA 2010, 4, prevedel Dolinar.

dela med delovnim časom, vprašanje zlorabe delodajalčeve opreme v zasebne namene in na drugi strani za vprašanje zasebnosti zaposlenega.[90]

V svetovnem merilu ločimo dva različna pristopa, tako imenovani »ameriški« in »evropski« pristop. »Ameriški pristop zaposlenega na delovnem mestu vidi predvsem kot delojemalca, ki uporablja opremo, ki je last delodajalca, v delovnem času je plačan s strani delodajalca in zato službenih komunikacijskih sredstev in službenega časa ne sme »zlorabljati« v zasebne namene«, medtem ko »evropski pristop zaposlenega na delovnem mestu ne vidi samo kot delavca, pač pa tudi kot človeško bitje, ki ima kot tako tudi določene (človekove) pravice«. Poleg tega je pri tem pomembno varovanje pravic tretjih oseb (»z nadzorom komunikacij zaposlenega nadzorujemo tudi komunikacije njegovih zunanjih komunikacijskih partnerjev«) in vprašanje sorazmernosti, »se pravi kolikšen obseg nadzora je sprejemljiv in še opravičljiv oziroma ali zaželenega cilja ni mogoče doseči z blažjimi sredstvi«.[91]

3.5.1. Komunikacijska zasebnost na delovnem mestu v Evropi

ESČP je v primeru Halford proti Veliki Britaniji izrecno poudarilo, da zaposleni na delovnem mestu upravičeno pričakuje zasebnost.[92]

Pomembna je tudi odločitev ESČP v primeru Copland proti Veliki Britaniji (Application no. 62617/00), kjer je sodišče presodilo, »da varstvo zasebnosti velja tako za telefonske komunikacije kot tudi za elektronsko pošto in uporabo interneta in da je s stališča varstva zasebnosti irelevantno, ali gre za zasebno ali za službeno komunikacijsko sredstvo«.[93] Sodišče je presodilo, da kršitev zasebnosti ni samo vpogled v vsebino komunikacij, temveč tudi vpogled v prometne podatke. Kot nadaljuje sodišče, »je s stališča varstva zasebnosti irelevantno, ali so bili podatki »zgolj« zbrani ali pa so bili tudi razkriti tretjim osebam oziroma uporabljeni proti pritožnici«.[94]

To seveda ne pomeni, da delodajalec nima nikakršnih pravic in da lahko zaposleni njegovo opremo uporablja, kakor želi in za ka-

[90] M. Kovačič 2010, http://hr-cjpc.si/pravokator/index.php/2010/09/22/komunikacijska-zasebnost-na-delovnem-mestu/, 8. 1. 2013.
[91] M. Kovačič 2010, 55.
[92] M. Kovačič 2010, 59.
[93] M. Kovačič 2010, 59.
[94] M. Kovačič 2010, 60.

terikoli namen. Oprema je last delodajalca in ta lahko določa pravila njene uporabe, saj je zaposleni še vedno zgolj njen uporabnik. Upoštevati pa je treba, da mora biti zaposleni vnaprej seznanjen s pravili uporabe telefona in druge opreme ter da si delodajalec ne more privoščiti pretiranega omejevanja pravice do zasebnosti in pravice do komunikacije z zunanjim svetom. Načeloma se mora zaposleni z nadzorom strinjati oziroma mora biti ta objektivno opravičljiv in sorazmeren. Zaposleni je v razmerju do delodajalca v podrejenem položaju, zato mora biti to strinjanje prostovoljno in brez prisile.[95]

3.5.2. Komunikacijska zasebnost na delovnem mestu v Sloveniji

Komunikacijsko zasebnost v Sloveniji zagotavlja 37. člen Ustave RS. Po Kovačičevem mnenju gre za specifiko slovenskega pravnega reda. Na podlagi tega člena je tako komunikacijska zasebnost v Sloveniji bolj zaščitena, kot je sicer na splošno v Evropi, saj Ustava RS za poseg v komunikacijsko zasebnost zahteva ustrezno zakonsko podlago in predvsem sodno odredbo.[96]

To potrjuje tudi Ustavno sodišče RS v odločitvi o ustavni pritožbi Up-106/05, kjer natančno razdeli in obrazloži dopustnost posega v svobodo komuniciranja, ko pravi, da je poseg dopusten samo, »če so izpolnjeni naslednji pogoji: 1) da je poseg določen v zakonu, 2) da poseg s svojo odločbo dovoli sodišče, 3) da je določno omejen čas izvajanja posega in 4) da je poseg nujen za uvedbo ali potek kazenskega postopka ali za varnost države«, in v naslednjem odstavku še enkrat poudari: »Po drugem odstavku 37. člena ustave torej poseg v svobodo komuniciranja ni dovoljen brez predhodnega dovoljenja sodišča.« Podobno kot ESČP v primeru Copland proti Veliki Britaniji tudi Ustavno sodišče RS ugotavlja, da ni varovana samo vsebina komunikacije, pač pa »je treba predmet varstva komunikacijske zasebnosti razlagati širše, tako da ta vključuje tudi tiste podatke o telefonskih klicih, ki so sestavni del komunikacije«.[97]

Kot ugotavlja Klemenčič, se sodna praksa v Sloveniji praviloma postavlja na stran posameznika, na kar opozarja tudi odločitev Upravnega sodišča RS, s katero je bila priznana pravica do varstva

[95] M. Kovačič 2010, 61.
[96] M. Kovačič 2010, 63.
[97] Up-106/05, Ur. l. RS, št. 100/2008.

zasebnosti pri uporabi službenega mobilnega telefona.[98] Upravno sodišče je v sodbi namreč zapisalo, da »pojem tajnosti pisem in drugih občil zajema tako zasebne kot tudi službene komunikacije«. V nadaljevanju še doda, da »pojem zasebno življenje torej vsebuje tako zasebne kot tudi službene telefonske linije, zaradi česar ni pomembna lastnina ali pripadnost določenega telekomunikacijskega sredstva. To varstvo je dano vsem osebam in ni mogoče slediti navedbi tožene stranke, da to ne velja za tožnike, ki so uporabljali mobilne telefone v lasti tožene stranke. Lastninski koncept zasebnosti, to je pristop z vidika dejstva, čigavo je komunikacijsko sredstvo, ki je bilo nadzirano, ni relevanten. Tudi Ustava RS ne ločuje zasebnosti v zasebni in službeni sferi.«[99]

Kovačič slikovito zaključi: »Nadzor komunikacij zaposlenega zaradi ugotavljanja, ali zaposleni morda ne »zapravlja« časa podjetja za zasebne namene, ni ne sorazmeren ne potreben. Za odpoved pogodbe o zaposlitvi namreč zadostuje že to, da delavec ni opravil dodeljenih nalog. Ali jih ni opravil zaradi pretirane uporabe interneta, elektronske pošte in telefona v neslužbene namene ali pa iz drugih razlogov, je ob vsem skupaj povsem irelevantno.«[100]

3.6. Zasebnost na javnem mestu

Z razvojem mobilne telefonije je prišlo do prehoda telefonskih pogovorov iz zasebnega v javni prostor. Kot zasebni prostor po Zakonu o varstvu javnega reda in miru (ZJRM-1[101]) razumemo »prostor, ki je v zasebni lasti ali posesti in je dostop vanj dovoljen le s soglasjem lastnika ali lastnice, posestnika ali posestnice ali druge upravičene osebe«, javni kraj pa je »vsak prostor, ki je brezpogojno ali pod določenimi pogoji dostopen vsakomur«.[102] Tu je treba poudariti, da tudi na javnem kraju obstajajo prostori, kjer lahko upravičeno pričakujemo zasebnost. Taka prostora sta npr. telefonska govorilnica in volišče.

Pri tem prehodu so, kot ugotavlja Krapeževa, »mobilni telefonski pogovori zbudili pozornost in pomisleke pri:[103]

- mimoidočih, ki so bili prisiljeni poslušati pogovor, s čimer so uporabniki telefona posegli v njihovo zasebnost;

[98] G. Klemenčič v Kovačič 2010, 63.
[99] U702/99.
[100] M. Kovačič 2010, 64.
[101] Ur. l. RS, št. 70/2006.
[102] ZJRM-1 2006, 2. člen.
[103] K. Krapež 2007, 273.

• tistih, ki so se pogovarjali, saj so bili naenkrat postavljeni pred dejstvo, da so precej bolj izpostavljeni raznim motnjam, samocenzuri in nadzoru okolice«.

»V kolikor so bili fiksni telefonski pogovori za mimoidoče moteči primarno v sferi nekega manjšega prostora (stanovanja, govorilnice), predstavljajo mobilni pogovori predvsem poseg v zvočni prostor naključnih poslušalcev. Takšni posegi so v veliki meri bolj moteči, predvsem zato, ker se zvočnim dražljajem mimoidoči ne morejo izogniti. Ti se, če hočejo ali ne, prelevijo v neprostovoljne prisluškovalce.«[104]

Poseg v zasebnost uporabnika mobilnega telefona, ki se pogovarja na javnem prostoru, ne predstavlja take grožnje, saj se avtonomno odloči, ali bo klic sprejel ali koga poklical, čeprav ga v tistem trenutku obkroža množica ljudi.[105]

Takega mnenja je tudi ustavno sodišče, ki v eni izmed svojih odločb pravi, da k pravici do zasebnosti sodi tudi to, »da se človek sam odloči o tem, kdo bo slišal vsebino komunikacije – le sogovornik, določena zaključena skupina ljudi ali javnost. Odločitev o sebi in o svoji besedi zajema torej tudi določitev kroga oseb, ki naj slišijo vsebino pogovora.« Sodišče še dodaja, da »če se človek obnaša tako, da lahko njegovo besedo brez posebnih naporov sliši nekdo tretji, mora posledice nositi sam. Bistveno je torej, ali lahko človek glede na okoliščine primera utemeljeno pričakuje, da ga tretja oseba ne bo slišala.«[106]

»Tehnologije so priložnost, ki jo posameznik preprosto lahko sprejme ali ne, jo morda prilagodi, predvsem pa izkoristi, da bi dosegel cilje. Ker tehnologija ni nevtralna, pogojuje vedenje tistih, ki jo uporabljajo.«[107] S pomočjo mobilnega telefona smo začeli govoriti povsod in o vsem, tudi o svojih najbolj intimnih zadevah, ki jih brez kančka sramu razkazujemo kar na javnih prostorih. Po mnenju Fortunatijeve je bil tako mobilni telefon eno izmed prvih opozoril o množičnem zavračanju zasebnosti.[108]

[104] K. Krapež 2007, 274.
[105] K. Krapež 2007, 274.
[106] Up-472/02, Ur. l. RS, št. 114/2004.
[107] Latour in Woolgar v L. Fortunati 2007, 9.
[108] L. Fortunati 2007, 22.

3.7. Prestrezanje komunikacij, slikanje in snemanje

Prisluškovanje mobilnim telefonom je izjemno preprosto. Posameznik, ki želi prisluškovati pogovoru, se lahko skrije v okviru zvočnega prostora govorečega, torej tja, kjer bo pogovor še slišal in mu tako prisluškoval. Seveda obstajajo tudi bolj elegantne in sofisticirane metode. Ena izmed njih so npr. sistemi,[109] ki prestrezajo in analizirajo več vrst komunikacije ter iščejo določene »nezaželene« ključne besede. Prestrezanje komunikacij je sicer lahko zakonito ali nezakonito.

3.7.1. Nezakonito prestrezanje komunikacij, slikanje in snemanje

Pri nas nezakonito oziroma, kot pravi zakon, neupravičeno prisluškovanje, zvočno snemanje, slikanje oziroma slikovno snemanje in kršitev tajnosti občil ureja kazenski zakonik. Neupravičeno prisluškovanje in zvočno snemanje opredeljuje v 137. členu.[110]

Ker imajo že skoraj vsi mobilni telefoni vgrajene fotografske aparate oziroma kamere, sem spada tudi slikovno snemanje, kar zakon opredeljuje v 138. členu.[111]

S stališča pričujočega dela je pomembno, kako zakon ureja neupravičeno branje besedilnih sporočil (SMS-ov) in ob razvoju pametnih telefonov tudi elektronskih sporočil, kar ureja 139. člen.[112]

3.7.2. Zakonito prestrezanje komunikacij

Že ustava v 37. členu določa, da se varstvo tajnosti pisem in drugih občil lahko ne upošteva samo izjemoma za določen čas, na podlagi odločbe sodišča, če je to nujno za varnost države ali uvedbo oziroma potek kazenskega postopka.[113] V takšnih izjemnih primerih je prestrezanje komunikacij dovoljeno. To ureja Zakon o kazenskem postopku v 150. členu, kjer določa, da se lahko pod pogoji, ki so določeni v 1. odstavku 150. člena, odredi »nadzor ele-

[109] Tak sistem je na primer prisluškovalni sistem Echelon, prek katerega naj bi ZDA, Združeno kraljestvo, Kanada in Avstralija prestrezale telefonske pogovore in iskale ključne besede, ki namigujejo na terorizem, po poročanju članka pa naj bi se uporabljal tudi za nezakonito prisluškovanje (Mellor 2004, http://news.techworld.com/storage/2430/want-to-know-the-hardware-behind-echelon/, 31. 1. 2013, prevedel Dolinar).
[110] KZ-1 2012, 137. člen.
[111] KZ-1 2012, 138. člen.
[112] KZ-1 2012, 139. člen.
[113] Ustava RS 1991, 37. člen.

ktronskih komunikacij s prisluškovanjem in snemanjem ter kontrola in zavarovanje dokazov o vseh oblikah komuniciranja, ki se prenašajo v elektronskem komunikacijskem omrežju; kontrola pisem in drugih pošiljk; kontrola računalniškega sistema banke ali druge pravne osebe, ki opravlja finančno ali drugo gospodarsko dejavnost; prisluškovanje in snemanje pogovorov s privolitvijo vsaj ene osebe, udeležene v pogovoru«.[114]

2. odstavek istega člena določa kazniva dejanja, zaradi katerih se lahko taki ukrepi odredijo, in jih tudi našteva. Gre za huda kazniva dejanja, kot so npr. kazniva dejanja zoper varnost Republike Slovenije, njeno ustavno ureditev, zoper človečnost in mednarodno pravo, če je v zakonu predpisana kazen zapora petih ali več let, kazniva dejanja ugrabitve, neupravičene proizvodnje in prometa s prepovedanimi drogami, nedovoljenimi snovmi v športu, neupravičenega dajanja daril, pranja denarja, tihotapstva, oškodovanja javnih sredstev itd. ter druga kazniva dejanja, za katera je v zakonu predpisana kazen zapora osmih ali več let.[115]

Prestrezanje komunikacij je po ZEKom-1 možno tudi za drugačne namene. 147. člen ZEKom-1 varuje pričakovano zasebnost na področju uporabe elektronskih komunikacij. Kljub temu smejo operaterji pridobiti informacije o komunikacijah, vendar le v obsegu, ki je nujno potreben za izvajanje določenih javnih komunikacijskih storitev. Če gre torej za nujne razloge, lahko operaterji po 4. odstavku 147. člena pridobijo tudi informacije o vsebini komunikacij, lahko tudi posnamejo ali shranijo komunikacije in z njimi povezane podatke o prometu, vendar morajo o tem ob sklenitvi naročniške pogodbe oziroma ob začetku izvajanja javne komunikacijske storitve seznaniti uporabnika, pridobljene informacije pa zbrisati takoj, ko je to tehnično izvedljivo in ko ti podatki niso več potrebni za izvedbo določene javne komunikacijske storitve.[116]

Prav tako je po 7. odstavku 147. člena »dovoljeno snemanje komunikacij in z njimi povezanih podatkov o prometu v okviru zakonite poslovne prakse zato, da se zagotovi dokaz o tržni transakciji ali katerikoli drugi poslovni komunikaciji, pod pogojem, da so stranke v komunikaciji predhodno obveščene o snemanju, njegovem namenu in trajanju hrambe posnetka (npr. avtomatski odzivniki). Posneto sporočilo je treba nemudoma izbrisati, najpo-

[114] ZKP 2012, 150. člen.
[115] ZKP 2012, 150. člen.
[116] ZEKom-1 2012, 147. člen.

zneje do poteka dobe, v kateri se posel lahko zakonito izpodbija.« Po 9. odstavku istega člena je snemanje vsebine komunikacij »dovoljeno tudi v okviru organizacij in državnih organov, ki so pristojni za izvajanje obveščevalnih in varnostnih nalog, nalog policije, obrambe in zaščite, reševanja in pomoči pod pogojem, da so kličoči uporabniki predhodno obveščeni o snemanju, njegovem namenu in trajanju hranjenja posnetka (npr. avtomatski odzivniki). Drugim državnim organom je snemanje vsebine komunikacij dovoljeno, če tako določa zakon.«[117]

4. Zaključek

Kot smo videli, je pravica do zasebnosti pri nas pravno dobro urejena, celo bolje kot na splošno v Evropi; v Evropi pa je s stališča posameznika urejena bolje kot čez lužo. Izjemno hiter razvoj na področju mobilne telefonije in tehnologije je zahteval napredek in razvoj tudi v pravu. Pravo je sicer po našem mnenju vedno korak za tehnologijo. Razlog je najbrž v bliskovitih spremembah na tem področju, saj se lahko z novostjo pojavi težava, ki je prej ni mogel nihče predvideti.

Pravo je razvoj in prisotnost tehnologije izkoristilo in ob množični uporabi mobilnih telefonov omogočilo »varovalke«, prek katerih lahko v izjemnih primerih, ob sumu ali storitvi hudih kaznivih dejanj, pooblaščena oseba pridobi tudi podatke o prometu uporabnika določenega mobilnega telefona oziroma mu prisluškuje. Z izkoriščanjem tehnologije za pomoč pri pregonu hudih kaznivih dejanj ali za pomoč žrtvam nesreč oziroma bolezni (lokacijski podatki v primeru klica v sili) ni popolnoma nič narobe, prav nasprotno. Težava se pojavi, ko žrtve postajamo tudi nedolžni oziroma tisti, ki nismo žrtve nesreč in bolezni. Težava je v hrambi prometnih podatkov, kot je opisana v kritiki obvezne hrambe podatkov o prometu, v množičnem nadzoru oziroma takem nadzoru, katerega tarča smo vsi, in to brez soglasja ali popolne upravičenosti, česar se večkrat niti ne zavedamo.

Glede na pravni trend bo, če se bo tako nadaljevalo, zasebnost postajala vse manj zasebna. Če torej želimo danes živeti normalno, moramo očitno pristati na določen nadzor. Če bi se namreč želeli pravno izolirati v smislu stroge zasebnosti, bi morala biti večina

[117] ZEKom-1 2012, 147. člen.

mobilnih aparatov (ali vsaj večji del njihovih funkcij) s pravom prepovedana. Zanimivo bo torej spremljati, kaj bo prinesla prihodnost. Glede na to, da dokaj redno spremljamo novosti in razvoj na tehnološkem področju, se je s tehnične strani zelo veselimo, medtem ko smo lahko s stališča stroge zasebnosti upravičeno zaskrbljeni.

VIRI IN LITERATURA

SAMOSTOJNE PUBLIKACIJE

I. Kaučič in F. Grad, Ustavna ureditev Slovenije, četrta, spremenjena in dopolnjena izdaja, GV založba, Ljubljana, 2007.
M. Kovačič, Zasebnost na internetu, Mirovni inštitut, Inštitut za sodobne družbene in politične študije, Ljubljana, 2003.
R. Lampe, Sistem pravice do zasebnosti, Bonex, Ljubljana, 2004.
L. Šturm in drugi, Komentar Ustave Republike Slovenije, Fakulteta za podiplomske državne in evropske študije, Ljubljana, 2002.

PRISPEVKI OZIROMA POGLAVJA V KNJIGI, ZBORNIKU

L. Fortunati, Mobilnik kot četrta komunikacijska revolucija, v: Vasja Vehovar (ur.), Mobilne refleksije, Založba FDV, Ljubljana, 2007, str. 9–28.
M. Kovačič, Zasebnost in hramba prometnih podatkov v mobilni telefoniji, v: Vasja Vehovar. (ur.), Mobilne refleksije, Založba FDV, Ljubljana, 2007, str. 243–267.
M. Kovačič, Komunikacijska zasebnost na delovnem mestu, v: Aleš Završnik (ur.), Kriminaliteta in tehnologija: Kako računalniki spreminjajo nadzor in zasebnost ter kriminaliteto in kazenski pregon? Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani, Ljubljana, 2010, str. 55–67.
K. Krapež, Mobilni telefon med zasebnim in javnim: »Intimnosti« v javni sferi, v: Vasja Vehovar (ur.), Mobilne refleksije, Založba FDV, Ljubljana, 2007, str. 269–284.

PRAVNI VIRI

Direktiva 2002/58/ES Evropskega parlamenta in sveta, Direktiva o obdelavi osebnih podatkov in varstva zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), Url: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:SL:PDF. 12. 7. 2002.
Direktiva 2006/24/ES Evropskega parlamenta in sveta, Direktiva o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij in spremembi direktive 2002/58/ES, Url: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:SL:PDF. 15. 3. 2006.
Direktiva 95/46/ES Evropskega parlamenta in sveta, Direktiva o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Url: https://www.ip-rs.si/fileadmin/user_upload/Pdf/razno/Direktive_E_parlamenta_in_Sveta.pdf. 24. 10. 1995.
Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (EKČP), Url: http://www.varuh-rs.si/pravni-okvir-in-pristojnosti/mednarodni-pravni-akti-s-podrocja-clovekovih-pravic/svet-evrope/evropska-konvencija-o-varstvu-clovekovih-pravic-in-temeljnih-svoboscin/. 13. 6. 1994.
Kazenski zakonik, Uradni list RS, št. 55/2008, 66/2008, 39/2009 in 91/2011.
Splošna deklaracija človekovih pravic, 1948, Url: http://www.varuh-rs.si/index.php?id=102. 10. 12. 1948.
Ustava RS, Uradni list RS, št. 33/91-I, 42/97, 66/2000, 24/03, 69/04 in 68/06.
Zakon o elektronskih komunikacijah, Uradni list RS, št. 43/2004, 129/2006, 110/2009 in 33/2011.
Zakon o kazenskem postopku, Uradni list RS, št. 63/1994, 70/1994, 72/1998, 6/1999, 66/2000, 111/2001, 56/2003, 43/2004, 101/2005, 14/2007, 68/2008, 77/2009 in 91/2011.
Zakon o varstvu javnega reda in miru, Uradni list RS, št. 70/2006.

SODNA PRAKSA

Odločba Ustavnega sodišča RS, št. Up-106/05, Uradni list RS, št. 100/2008.
Odločba Ustavnega sodišča RS, št. Up-472/02, Uradni list RS, št. 114/2004.
Sodba Upravnega sodišča št. U702/99 z dne 21. 3. 2000.

DRUGI VIRI

A. Andrenšek, Mobilna svoboda ali novo odpovedovanje zasebnosti? Url: http://www.dnevnik.si/objektiv/vec-vsebin/1042513900. 3. 3. 2012.
L. Cassavoy, What Makes a Smartphone Smart?
Url: http://cellphones.about.com/od/smartphonebasics/a/what_is_smart.htm. 5. 11. 2012.
Delovna skupina za varstvo podatkov iz člena 29, Mnenje DS 119, Url: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Article_29_WP/wp119_sl.pdf. 25. 3. 2006.
Gartner Inc. About Gartner, Url: http://www.gartner.com/technology/about.jsp. 5. 1. 2013.
ENISA, Smartphones: Information security risks, opportunities and recommendations for users, Url: http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users. 10. 12. 2010.
J. Hudoklin in drugi, Varnost slovenskih GSM omrežij,
Url: https://slo-tech.com/clanki/12003/. 12. 6. 2012.
M. Huš, Študija: hramba prometnih podatkov ne pomaga pri preiskavi kaznivih dejanj, Url: https://slo-tech.com/novice/t504584. 29. 1. 2012.
ISACA, Securing mobile devices, Url: «http://www.isaca.org/Knowledge-Center/Research/Research-Deliverables/Pages/Securing-Mobile-Devices.aspx. 3. 1. 2013.
ISACA, Slovenski odsek, Url: http://www.isaca.si/o_odseku.php. 3. 1. 2013.
M. Kovačič, Komunikacijska zasebnost na delovnem mestu, Url: http://hr-cjpc.si/pravokator/index.php/2010/09/22/komunikacijska-zasebnost-na-delovnem-mestu/. 22. 9. 2010.
M. Kovačič, Ko pokličejo hekerji – spreminjanje klicne identifikacije telefonskih klicev, Url: http://hr-cjpc.si/pravokator/index.php/2012/03/18/ko-poklicejo-hekerji-spreminjanje-klicne-identifikacije-telefonskih-klicev/. 18. 3. 2012.
M. Kovačič, Varnost slovenskih GSM omrežij, Url: http://hr-cjpc.si/pravokator/index.php/2012/06/16/varnost-slovenskih-gsm-omrezij/. 16. 6. 2012.
B. Kvas, Nemčija: Sodišče razveljavilo zakon o obvezni hrambi prometnih podatkov, Url: http://www.e-demokracija.si/2010/03/08/nemcija-sodisce-razveljavilo-zakon-o-obvezni-hrambi-prometnih-podatkov/. 8. 3. 2010.
B. Mekina, Vse pod nadzorom, Url: http://www.mladina.si/92678/vse-pod-nadzorom/. 22. 2. 2008.
C. Mellor, Want to know the hardware behind Echelon? Url: http://news.techworld.com/storage/2430/want-to-know-the-hardware-behind-echelon/. 15. 8. 2013.
Ministrstvo za zunanje zadeve, Evropsko sodišče za človekove pravice, Url: http://www.mzz.gov.si/si/coe/o_svetu_evrope/organi_in_institucije_sveta_evrope/evropsko_sodisce_za_clovekove_pravice/. 28. 11. 2012.
Ministrstvo za zunanje zadeve, Najpomembnejši mednarodnopravni dokumenti s področja človekovih pravic, Url: http://www.mzz.gov.si/si/zunanja_politika_in_mednarodno_pravo/zunanja_politika/clovekove_pravice/najpomemnejsi_mednarodnopravni_dokumenti_s_podrocja_clovekovih_pravic/. 26. 11. 2012.
Ris.org (RIS: raba interneta v Sloveniji), Mobilna telefonija – raziskave, Url: http://www.ris.org/db/27/12439/Raziskave/V_ZDA_17_mobilnih_uporabnikov_vecino_brskanja_po_spletu_opravi_preko_telefona/?&cat=703&p1=276&p2=285&p3=1318&p4=1359&id=1359. 17. 12. 2012.

EKČP – Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin
ENISA – European Network and Information Security Agency
ESČP – Evropsko sodišče za človekove pravice
EU – Evropska unija
GSM – Global System for Mobile Communication
IT – informacijska tehnologija
KZ – Kazenski zakonik
MMS – Multimedia Messaging Service
SDČP – Splošna deklaracija človekovih pravic
SMS – Short Message Service
ZEKom – Zakon o elektronskih komunikacijah
ZJRM – Zakon o varstvu javnega reda in miru
ZKP – Zakon o kazenskem postopku