Zasebnost osebnih podatkov

Aleš Repovž, študent, Fakulteta za varnostne vede, Univerza v Mariboru
Igor Bernik, Fakulteta za varnostne vede, Univerza v Mariboru

Namen prispevka:
Prispevek prikazuje človekovo pravico do ohranjanja zasebnosti osebnih podatkov v sodobnem svetu, kjer je ta pravica ogrožena zaradi rabe kibernetskega prostora in komuniciranja v njim, kjer je način komunikacije uporabnikom pogosto nerazumljiv z vidika načina prenosa podatkov.

Metodologija:
Uporabljena je deskriptivna metoda analize virov in sistematična sinteza pridobljenih in obstoječih znanj v pregledu zasebnosti in pravice do varovanja osebnih podatkov pri delu z informacijsko komunikacijsko tehnologijo v kibernetskem prostoru.

Ugotovitve:
Delo v kibernetskem prostoru in način prenosa in dostopa do podatkov omogoča širši dostop do osebnih podatkov posameznika in s tem kršenje temeljne človekove pravice do ohranjanja zasebnosti. Zaradi rabe tehnologije se je nadzor nad posameznikom in vdor v njegovo zasebnost v zadnjem obdobju močno povečal, zato moramo uporabniki skrbneje ravnati s svojo zasebnostjo in jo poskušati ohranjati.

Omejitve:
Članek se sklicuje le na omejen nabor virov in poznavanja področja, ni pa izvede analiza varovanja in ohranjanja zasebnosti z raziskavo in podajanjem primerjav, zato je predstavljeno delo splošen pregled.

Praktična uporabnost:
Tema zasebnosti in njene zlorabe je aktualna in pereča, tudi iz vidika, da kibernetksi prostor ne pozna mehanizma pozabljanja. Zato je splošen pregled na tem področju primeren za seznajnanje uporabnikov z izpostavljeno problematiko.

Izvirnost:
Obravnavanje zasebnosti osebnih podatkov in pregled glavnih delov je podan z namenom usposabljanja strokovne javnosti.

Ključne besede: zasebnost, osebni podatki, kibernetski prostor, posameznik

1 UVOD

Pravica do zasebnosti je ena izmed temeljnih človekovih pravic. Človekovo dostojanstvo je lahko prizadeto na katerikoli stopnji državnih postopkov, zato mora biti zagotovljena intimnost posameznika. Zasebnost je še posebej ogrožena s prepogosto uporabo sodobnih sredstev prisluškovanja, snemanja, navigacijskega sledenja in registriranja. Z izjemnim napredkom informacijske tehnologije in s spremenjenimi načini poslovanja se za vsakogar, državo, gospodarstvo ali posameznika odpirajo nove oblike tveganj in groženj zasebnosti.

Zadnja leta so prinesla odvisnost od sodobnega načina komuniciranja, pretok informacij v elektronski obliki, elektronsko bančništvo, zdravstvo, letalski prevozi, izobraževanje. Vsi postajamo vedno bolj odvisni od informacij, ki potujejo po žicah, usmerjevalnikih, požarnih pregradah, brezžičnih povezavah in omrežjih. Na tej točki pa se pojavlja vprašanje zlorabe podatkov in informacijske zasebnosti.

2 INFORMACIJSKA ZASEBNOST

Informacijska zasebnost je sopomenka za varstvo osebnih podatkov in ena od sestavin zasebnosti. Zasebnost tako ni enodimenzionalen pojem, pri čemer že Čebulj (1992, str. 7) navaja tri sestavine zasebnosti:

- zasebnost v prostoru (možnost posameznika da je sam),
- zasebnost osebnosti (svoboda misli, opredelitve, izražanja) ter
- informacijska zasebnost (možnost posameznika, da obdrži informacije o sebi, ker ne želi, da bi bili z njimi seznanjeni drugi).

Večina ljudi si pod zasebnostjo v prostoru predstavlja predvsem čas, ko nas nihče ne moti. To so trenutki, ki jih kot posamezniki ne želimo deliti z nikomer. Določen del te zasebnosti se navezuje na najbolj osnovne biološke potrebe, ki jih imamo vsi ljudje, a so tako zelo osebne, da jih želimo izvajati izključno sami. Na prostorsko zasebnost se tako navezuje fizična zasebnost, saj se zasebnost v takšnih primerih veže na določen prostor. Čeprav smo ljudje družbena bitja, imamo seveda pravico do izolacije od ostalih ljudi, tako doma, kot na delovnem mestu ali na javnem prostoru, brez video ali satelitskega nadzora (preko magnetnih in pametnih kartic). Imamo pravico do časa, ko smo lahko izključno sami s sabo, nemoteni s strani drugih ljudi (http://www.adamineva.com/zasebnost-znotraj-sten-nasega-doma/).

Pravica do svobodnega izražanja v družbeni praksi vse pogosteje prihaja v konflikt s pravico do zasebnosti. Z vidika svobode medijev je vdor v pravico do zasebnosti najpogosteje storjen s strani privatnih, zasebnih subjektov, kot so tisk, radio in televizija, manj pa neposredno s strani države. Država mora storiti vse potrebno, da zavaruje posameznikovo pravico do zasebnosti, četudi gre za razmerje med posameznikom in subjekti zasebnega prava (Teršek, 2005, str. 97–98). Kritična, oz. v informacijski družbi potencialno najbolj ogrožena, pa je tretja sestavina zasebnosti, ki vključuje tudi varstvo osebnih podatkov.

Varstvo osebnih podatkov obsega zbiranje, obdelovanje in prenos osebnih podatkov. »Pravica do zasebnosti se opredeljuje kot pravica posameznika, da zahteva, da se podatki o njegovih zasebnih razmerjih ne sporočajo komurkoli. Gre torej za kontrolo pretoka in posredovanje podatkov, ki se nanašajo nanj oziroma opisujejo njegove lastnosti« (Niblett v Brezovšek in Črnec, 2010, str. 96).

Brezovšek in Črnčec (2010, str. 195) navajata, da »star pregovor pravi, da kdor ima informacijo, ima moč«. Za današnji čas to zagotovo velja, saj sodobna računalniška tehnologija omogoča posameznikom, skupinam in organizacijam, da obdelujejo in shranjujejo ogromno število osebnih in drugih podatkov. Oseba, ki ima dostop do različnih skupin osebnih podatkov v bazah podatkov ali preko različnih tehničnih sredstev, ima ogromno možnosti, da spremlja posameznikovo vedenje in posega v njegovo intimo brez njegove vednosti in nadzora (Brezovšek in Črnčec, 2010, str. 195-196).

Preprečevanje nezakonitih in neupravičenih posegov v zasebnost posameznika pri obdelavi in uporabi osebnih podatkov se določa z varstvom osebnih podatkov. To področje pri nas ureja Zakon o varstvu osebnih podatkov [ZVOP, 2004], ki nudi posamezniku precejšnje varstvo. ZVOP načelno dopušča uporabo osebnih podatkov – osebno ime, naslov prebivališča, telefonsko številko, naslov elektronske pošte in številko telefaksa. Za zbiranje drugih osebnih podatkov pa potrebuje upravljavec osebno privolitev posameznika (Novak et al., 2006, str. 878-879). Zakon natančno opredeljuje, pod kakšnimi pogoji je dovoljeno zbirati osebne podatke o posamezniku, prav tako pa predpisuje denarne in druge kazni, ki doletijo osebe, ki zbirajo in shranjujejo osebne podatke brez pooblastila ali, ki tovrstnih zbirk osebnih podatkov ne prijavijo ustreznim organom (Berčič et al., 2003, str. 125).

Interes za zbiranje, shranjevanje in obdelavo informacij imajo različni subjekti, poseben interes na področju nadzora pa država oziroma njena administracija. Država zaradi izvajanja svojih funkcij potrebuje nekatere osebne podatke o svojih državljanih. Na tem mestu pa si nasprotujeta interes države za zbiranje, obdelovanje in shranjevanje osebnih podatkov ter interes posameznika po ohranjanju zasebnosti. Država se je vedno trudila zbirati (osebne) podatke o posameznikih, vendar v preteklosti ni bilo na voljo ustrezne tehnologije za procesiranje, klasificiranje in povezovanje podatkov, ne nazadnje pa tudi za avtomatsko (rutinsko) zbiranje le-teh. To se je spremenilo z razvojem informacijsko komunikacijske tehnologije (v nadaljevanju IKT), ki zaznamuje moderno družbo. Zasebnost posameznika je bila sicer ogrožena že pred uvedbo IKT in računalniških zbirk podatkov, vendar pa je nova tehnologija ogroženost zasebnosti samo potencirala in privedla do tega, da so se ljudje nevarnosti

pričeli zavedati bolj kot v času ročno vodenih evidenc (Čebulj, 1992, str. 16). Sodobna IKT namreč omogoča rutinsko (namensko) pa tudi "naključno" zbiranje, hitro procesiranje, klasificiranje ter povezovanje podatkov, kar je postalo še posebej enostavno s pojavom in širokim razmakom rabe internetnih in mobilnih tehnologij.
Veliko nevarnost v zvezi z zbiranjem pomeni nenatančnost, napačnost, nepopolnost ali neažurnost zbranih podatkov. Vendar je ob tem potrebno imeti v mislih tudi samo zbiranje podatkov, ki lahko pomeni potencialno grožnjo zasebnosti. Vojske, obveščevalne službe ter policije držav namreč namenjajo ogromne količine denarja za nakup in razvoj sistemov za opazovanje akcij sovražnikov ter odkrivanje potencialnih nevarnosti in sovražnikov - vse v smislu "zaščite nacionalnih interesov". To seveda pomeni, da se nadzor vrši tudi nad državljani z vidika preventivnosti, to pa že lahko ogroža svobodo in pravice posameznika (povzeto po: Mehanizmi varovanja zasebnosti v informacijski družbi, 2011).
Preventivno zbiranje podatkov ne predstavlja edinega problema, problem je tudi naključno zbiranje podatkov. Sateliti, kamere v veleblagovnici, plačevanje s bančnimi karticami, internetni portali, mobilne aplikacije in podobno "opazujejo" vse, kar "pade" pod njihovo območje. David Burnham je že leta 1983 opozoril na tako **imenovano elektronsko sled, ki** jo posamezniki puščamo za sabo. Vsakič, ko posameznik dvigne slušalko, uporabi bankomat ali plačilno kartico, gre na banko, obišče zdravnika, se poroči, rodi ali umre, avtomatski sistemi ali institucije ta dogodek zaznajo in zabeležijo. Elektronska sled je torej informacija, ki se shranjuje rutinsko in kaže na akcije določenega posameznika (Mehanizmi varovanja zasebnosti v informacijski družbi, 2011). Le-ta postaja vsebolj problematična z rabo sodobnih, že omenjenih, intenretnih in mobilnih tehnologij. IKT poleg obdelave in kombiniranja omogoča zelo eleganten prenos različnih podatkov. Naključno ali z določenim namenom zbrani podatki so zato lahko dostopni osebam ali inštitucijam, ki za njihovo uporabo niso pooblaščene oz. podatke lahko uporabijo za drugačen namen kot so bili zbrani.

2.1 Zasebnost na internetu

Internet, kot globalno omrežje pomeni s svojimi storitvami kopico možnosti za nadzor in vdor v posameznikovo zasebnost. Storitve, ki jih najpogosteje uporabljamo in omogočajo nadzor uporabnika so:

- elektronska pošta,
- deskanje po internetu,
- novičarske skupine,
- klepetalnice,
- elektronsko poslovanje in
- elektronsko oglaševanje.

Vsaka izmed omenjenih storitev je izpostavljena določenemu tveganju z vidika nepooblaščenega zbiranja podatkov. Pomanjkanje računalniškega znanja, nezadostna osveščenost, pomanjkljiva programska oprema postavlja posameznika v podrejen položaj nasproti velikim podjetjem, državi ali osebam z znanjem ter tako omogoča vdore v računalnik bodisi hekerjev ali drugih oseb.
Uporabniki pa lahko uporabijo tehnologijo sebi v prid, tako da si zagotovijo ustrezno programsko in strojno opremo za zaščito svoje zasebnosti (požarne stene, programska oprema za filtriranje elektronske pošte, kodiranje elektronske pošte, posameznih datotek, digitalni podpis, digitalni certifikat …) (Brezovšek in Črnčec, 2010, str. 203).
Vsak uporabnik ima možnost, da na internetu postavi svojo predstavitveno stran. Ljudje na predstavitveni strani navadno objavljajo svoje osebne podatke, vendar se pri tem pogosto ne zavedajo, da današnja IKT omogoča avtomatsko zbiranje na internetu objavljenih podatkov. Čeprav je zbiranje samo na prvi pogled nenevarno, pa se bo uporabnik interneta nevarnosti zavedel takrat, ko bo njegove podatke zbrala spretna marketinška agencija in mu v njegov elektronski predal pričela pošiljati reklamna sporočila, oz. tako imenovani "junk mail" (pošto z elektronskimi "smetmi").
To pa niso edini možni način zbiranja podatkov o uporabnikih interneta. Mnoge internetne strani od uporabnikov v zameno za nekaj - informacije ali določene ugodnosti - zahtevajo osebne podatke. Na straneh, kjer se ti podatki zbirajo, večinoma ne piše oz. ni razvidno, v katere namene bodo tako zbrani podatki uporabljeni (Mehanizmi varovanja zasebnosti v informacijski družbi, 2011).

Poleg zbiranja podatkov, novejše tehnologije omogočajo tudi zbiranje podatkov s pomočjo ti. "piškotov" (cookie). Piškot uporabniku pošlje strežnik, kjer je postavljena spletna stran, ki si jo uporabnik ogleduje. Upravitelj spletne strani, ki piškot pošilja, pa preko njega o uporabniku pridobi določene informacij, ne da bi se uporabnik tega zavedal. Uporabnik sicer lahko preprečijo prejemanje piškotov v svojem spletnem brskalniku, žal pa se s tem izjemno omejijo pri dostopu do določenih storitev in avtomatizma za udobno delo.
Nevarnost zasebnosti je povezana tudi s tajnostjo posameznikove elektronske pošte oz. elektronskih sporočil nasploh. Danes je elektronska sporočila mogoče povsem enostavno prestreči, ter v njih iskati določene besede. Tehnologija omogoča, da je to narejeno enostavno, rutinsko, avtomatsko in neopazno. To lahko storijo posamezniki ali institucije, povsem enostavno pa je to za upravitelja internet strežnika, ki ima do elektronske pošte svojih uporabnikov načeloma povsem prost dostop, čeprav v večini držav velja načelo pisemske tajnosti (Mehanizmi varovanja zasebnosti v informacijski družbi, 2011). Vse to pomeni grožnjo zasebnosti, ki bi morala biti bolje varovana.
Posebno mesto pri razpravi o zasebnosti pa imajo v zadnjem času spletna socialna omrežja. Določenim profilom uporabnikov so postala praktično edin način komunikacije s svetom, preko njih izmenjujejejo sporočila, sprotno komunicarajo, kar pa je najhuje – javno objavljajo svoje zasebne podatke; tako statične kot dinamične. Statične podatke (osebni, določen status v družbi, bivališče, hobiji, zanimanja ...) sicer posamezniki še skrijejo pred širšo javnostjo, dinamične (kaj počne, kdaj in kam gre, ...) pa večinoma nekritično posredujejo javnosti. Tudi če krog prejemnikov obvestil zaprejo v krog svojih "prijateljev" pa le te sprejemajo popolnoma nekritično, torej lahko prejemnik omenjenih objavljenih podatkov postane praktično vsak. Nekritičnost sprejemanja prijateljev je posebej izrazita med mladimi, saj le ti "tekmujejo" za čimvečje število, od tu pa tudi prihaja zelo velika možnost neželjenega nadzora in izgube zasebnosti. Drug problematični vidik pa je nezadostna zaščita "profila" posameznika, saj večino ljudi meni, da njihovi podatki niso nič posebnega in da so za večino drugih nezanimivi in da ne more priti do vdora v njihovo zasebnost. Seveda pa se pri tem zelo motijo, saj podatki, ki nam predstavljajo določeno vrednost, le-to lahko pomenijo tudi drugim. To pa je problem, ki ni več povezan zgolj z zagotavljanjem zasebnosti.

3 RAZPRAVA

IKT omogoča osebam, institucijam in državi zaradi načina njihovega delovanja veliko stopnjo nadzora nad zasebnostjo, kar lahko ogrozi svobodo in pravice posameznika. Na tem mestu je potrebno poudariti, da se lahko vsak posameznik zavaruje pred vdori v zasebnost, kar mu omogoča sodobna tehnologija. Seveda pa pri tem potrebuje nekaj znanja in orodja, med katerimi je mnogo prosto dostopnih, za zaščito pred vdorom v zasebnost.
Menimo, da se je nadzor nad posameznikom v zadnjem desetletju močno poostril, kar lahko pripisujemo dogajanju po svetu, tudi zaradi groženj terorizma. Glede na moč nekaterih držav (kot so npr. ZDA) so se marsikatere države po svetu njim uklonile in brez vednosti njihovih državljanov razkrile njihove osebne podatke in možnost sledenja njihovega delovanja preko spleta in sledilnih naprav. Na podlagi pritiska ZDA pa tudi Evropska skupnost z uvedbo biometričnih potnih listov, hranjenja telefonskih pogovorov in drugih "zahtevanih" ukrepov. Glede na omenjeno se sprašujem ali so izdani podatki o posamezniku stvar prisile, dobičkonosnosti ali kraja, ob tem pa "mali človek" nič ne pridobi, izgubi pa svojo zasebnost. Zapišemo lahko, da v primeru odreka zasebnosti za povečanje posameznikove varnosti na koncu le-ta ostane tako brez varnosti (zaradi nadzora države) in podarjene zasebnosti. Posledično posameznik verjetno res ne more biti zaupljiv do institucij, ki operirajo z njegovimi podatki. Nič ni narobe, če bi želeli "monopolisti" obdržati svojo dominantno vlogo, pomembno je, da ne bi prihajalo do zlorabe podatkov; žal pa do te stalno prihaja.

VIRI

Berčič, B., Bojanec, A., Krkoč, P., Mrhar, P., Patru, P. et al. (2003). Ukrepi v primeru informacijskih nesreč. Inštitut za informacijsko varnost. Šempeter pri Gorici.

Brezovšek, M., Črnčec, D. (2010). Demokratična uprava in tajnost podatkov. Fakulteta za družbene vede. Ljubljana.

Čebulj, J. (1992). Varstvo informacijske zasebnosti v Evropi in v Sloveniji. Inštitut za javno upravo na Pravni fakulteti. Ljubljana.

Egan, M., Mather, T. (2005). Varnost informacij: grožnje, izzivi in rešitve. Vodnik za podjetja. Pasadena. Ljubljana.

Mehanizmi varovanja zasebnosti v informacijski družbi. (2011). Pridobljeno 21. 11. 2011 iz http://www.ljudmila.org/matej/zasebnost/zasebnost.html

Novak, B., Korošec, D., Ambrož, M., Bubnov-Škoberne, A., Dolgan M. et al. (2006). Osebni pravni svetovalec. Nasveti največjih slovenskih strokovnjakov za vsakogar. Cankarjeva založba. Ljubljana.

Teršek, A. (2005). Svoboda izražanja in pravica do zasebnosti. Analiza in komentar sodbe ESČP v primeru Von Hannover proti Nemčiji. Revus – Revija za evropsko ustavnost, 4, 97–114.

Zakon o varstvu osebnih podatkov. (Uradni list RS, 86/2004, 113/2005, 51/2007, 67/2007, 94/2007). Pridobljeno 21. 11. 2011 iz http://www.uradni-list.si/1/objava.jsp?urlid=200794&stevilka=4690

Zasebnost znotraj sten našega doma. (2010). Pridobljeno 8. 12. 2011 iz http://www. adamineva.com/zasebnost-znotraj-sten-nasega-doma/