Mag. Andrej Tomšič, Informacijski pooblaščenec RS

Varstvo zasebnosti na internetu na poti od netransparentnih poslovnih praks do regulacije
Privacy protection on the internet on the road from non-transparent business practice to regulation

Povzetek

Spletni velikani, spletna oglaševalska industrija in nekatera inovativna start-up podjetja se na podlagi pritiskov varuhov zasebnosti počasi premikajo iz sistema naknadnega preklica (opt-out) v sistem vnaprejšnje privolitve v obdelavo osebnih podatkov (opt-in). Ali je opt-in sistem tisto ključno orodje, s katerim lahko posamezniku vrnemo pravico do odločanja o svojih osebnih podatkih, in ali se lahko nanj v popolnosti zanesemo?

Ključne besede: zasebnost, osebni podatki, spletna družbena omrežja, DPI, privolitev, opt-in, opt-out.

Abstract

Major web companies, the web advertising industry and some innovative start-ups, facing recurrent pressures from privacy advocates, are slowly shifting from opt-out to opt-in regimes for processing personal data. Is opt-in the key tool that can restore users' power of control of our personal data, and can we fully rely on this concept?

Key words: privacy, personal data, social networks, Deep Packet Inspection, consent, opt-in, opt-out.

»Najprej ocenijo, ali lahko uporabniki in regulatorji ugotovijo, kaj v resnici počnejo s podatki. Nato presodijo, ali se bodo ljudje začeli množično odjavljati z njihove storitve, in ocenijo, kakšne so možnosti tožbe. Če so tveganja zanemarljiva, bodo zakone pač prekršili.« Tako je modus operandi večjih internetnih podjetij, kot sta Google in Facebook, v intervjuju Lenartu J. Kučiću pojasnil avstrijski študent prava Max Schrems, ki ga je omenjeno stanje dovolj vznemirilo, da se je spustil v boj z mlini na veter. In uspel. Na podlagi zahteve za seznanitev z lastnimi osebnimi podatki – ene temeljnih pravic posameznika po evropski zakonodaji o varstvu osebnih podatkov – je dobil za dobrih 1200 strani svojih osebnih podatkov in irskemu informacijskemu pooblaščencu (Facebook ima v Dublinu svojo podružnico) podal 22 prijav kršitev irskega zakona o varstvu osebnih podatkov. Schrems je zaključil, da kot onesnaževanja ni več mogoče zagovarjati z argumentom, da so okoljski standardi nepraktični, dragi in da znižujejo konkurenčnost onesnaževalcev, tudi ni več razloga, zakaj ne bi smeli od internetnih podjetij zahtevati, naj spoštujejo zakone, poslujejo transparentno in upoštevajo pravice uporabnikov, ne pa da jih obravnavajo zgolj kot surovine, na katerih temeljijo njihovi poslovni modeli.

Schremsove ugotovitve lahko povsem enostavno potrdimo sami. Se spomnite storitve Facebook Beacon? Beacon je bil del Facebookovega oglaševalskega sistema, pri čemer so se podatki o uporabi 44 drugih spletnih mest posameznikov (npr. nakupi na eBayu) prikazovali na njihovem zidu. Posamezniki se pred tem

seveda niso kaj dosti strinjali, saj jim je bila dana zgolj možnost naknadnega odstopa od uporabe (t. i. opt-out). Po obsežnem nasprotovanju v javnosti je bila storitev umaknjena septembra 2009, Facebookov ustanovitelj Mark Zuckerberg pa je nato izjavil, da je bil Beacon napaka. Opisani primer lepo kaže ustaljeno prakso poskusov, v smislu »ali bo šlo čez«. V tej luči je tudi opazen počasen prehod iz sistema poznejšega odstopa (opt-out) v sistem vnaprejšnje privolitve (opt-in). Sistem opt-out so tako posamezniki kot varuhi zasebnosti že dalj časa zamerili Facebooku, ki se je nanj zanašal pri marsikateri svoji funkcionalnosti, npr. pri dodajanju prijateljev v skupine brez njihove vnaprejšnje privolitve ali pri označevanju (t. i. tagging). Z vidika varstva osebnih podatkov je treba poudariti, da je razlika med omenjenima sistemoma ogromna in da vsaj evropska zakonodaja omogoča obdelavo osebnih podatkov praviloma na podlagi zakona ali osebne privolitve (torej opt-in), sistem opt-out pa je kvečjemu izjema in ga je moč zaslediti le na tistih področjih, kjer bi bilo vztrajanje pri sistemu opt-in nesmiselno, nesorazmerno ali celo neizvedljivo, npr. pri neposrednem trženju po navadni pošti in telefonu ali pri izvajanju videonadzora. V letih so z nekakšno prikrito legalizacijo opt-outa s pomočjo piškotkov uspešno poslovali tudi oglaševalci na internetu, saj nas nihče predhodno ni vprašal, ali dovolimo namestitev piškotkov na svoj računalnik in jih lahko le blokiramo in pozneje brišemo.

In kakšna je razlika med opt-in in opt-out? Da gre pri opt-out in opt-in za dva izrazito različna sistema lepo opozarja primer iz čisto drugega sveta – doniranje organov. Študija, ki sta jo izvedla Johnson in Goldstein, je namreč ugotovila, da se v večini držav stopnja doniranja organov ustali bodisi okrog 20 odstotkov bodisi okrog 80 odstotkov populacije. Sprva je kazalo, da so krive kulturne razlike, kar pa ni pojasnilo ogromne razlike med Švedsko (85,9 %) in Dansko (4,25 %). Ugotovili so, da ima že samo način, kako je postavljeno vprašanje, izrazit vpliv na rezultate in tako so imeli v državah z nizkimi odstotki donacij organov sistem opt-in, kjer je morala oseba sama izraziti to željo, tiste z visokimi deleži pa so uporabljale opt-out – če nisi reagiral nasprotno, si se uvrstil med donatorje. Da, eno samo potrditveno okence lahko pomeni bistveno razliko.

Nadvse zgovoren primer, ki nakazuje na razliko med opt-out in opt-in, prihaja iz ZDA, kjer se je ponudnik internetnega dostopa Embarq odločil, da se bo povezal s podjetjem NebuAd, in sicer bo NebuAd izvajal vedenjsko trženje na podlagi dostopa do podatkov o spletnih aktivnostih uporabnikov internetnega dostopa Embarq.[1] Testiranje delovanja sta pogodbena partnerja zavila v politiko zasebnosti, ki je bila dolga 5000 besed, uporabnikov pa posebej niso obvestili o tem, da bodo z določenim dnem podvrženi testiranju NebuAd-ove tehnologije. Uporabnikom je bila dana možnost, da pozneje zavrnejo takšno spremljanje spletne aktivnosti, in sicer prek povezave, ki je bila bolj ali manj skrita v prej omenjeni politiki zasebnost. Rezultat je bil zelo zgovoren – možnost zavrnitve spremljanja spletne aktivnosti, torej opt-out, je izkoristilo le 15 od 26.000 naročnikov Embarqa, ki so bili vključeni v testiranje. Torej je le 0,06 % uporabnikov izkoristilo možnost opt-out, zato lahko trdimo, da je med načelom opt-in, ki temelji na predhodni privolitvi, in načelom opt-out, ki omogoča le

[1] arstechnica.com/old/content/2008/07/06-opt-out-nebuad-hides-link-in-5000-word-privacy-policy.ars> (21. 7. 2009)

poznejšo zavrnitev, ogromna razlika. Pri varstvu osebnih podatkov je zato lahko načelo opt-out le pogojno uporabljeno, in sicer na mestih, kjer naj posegi v zasebnost posameznika ne bi bili tolikšni, da bi zahtevali vnaprejšnjo privolitev posameznika in bi se lahko s poznejšo zavrnitvijo obdelave osebnih podatkov lahko ustrezno zagotovilo varstvo pravic posameznika.

Kako gre nekaterim panogam sistem opt-out v nos, kaže tudi srdit boj spletne oglaševalske industrije proti novemu režimu oglaševanja na podlagi spletnih piškotkov, ki ga prinaša Direktiva 2009/136. Slednja bi (že) morala biti prenesena v zakonodaje članic EU maja lani, uveljavlja pa sistem opt-in na področju piškotkov. Oglaševalska industrija, ki je dolga leta kovala dobičke s profiliranjem posameznikov in ciljnim oglaševanjem, ne da bi se spletni uporabniki sploh zavedali, kako to poteka, kdo vse zbira njihove podatke in v kakšnih sociodemografskih kategorijah so sploh uvrščeni, seveda ne izbira sredstev v boju proti takšni ureditvi.

Ne gre seveda pozabiti tudi na primer Phorm, ki je na skrivaj izvajal poskuse z uporabo t. i. »Deep Packet Inspection« tehnologije tako, da bi v sodelovanju s ponudniki dostopa do interneta in s poseganjem v samo vsebino komunikacije lahko uspešneje izvajal ciljno oglaševanje. Po javnem napadu je podjetje izginilo iz novic, s sorodnimi ponudniki, kot je Kindsight, pa se počasi vrača s pretkanim prehodom na sistem opt-in in mamljivimi ponudbami za uporabnike: »Prav. Glasno in jasno vam povemo – brali bomo vsebino vaše spletne komunikacije in temu prilagajali oglase. Gmail to že počne. V zameno vam damo cenejši – kaj cenejši, BREZPLAČNI dostop do interneta.« Uporabniki bodo podpisovali anekse kot nori. In to ni vse – Kindsigth ponuja brezplačen varnostni paket in varovanje pred krajo identitete in kot navaja njihov promocijski material, je 60 % uporabnikov pripravljenih uporabiti njihove brezplačne varnostne storitve v zameno za prejemanje ciljnih oglasov. Kakšna ironija, opozarja Ryan Kim – posamezniki so pripravljeni ponuditi svoje osebne podatke o uporabi spleta v korist dobička oglaševalcev in operaterjev v zameno za varstvo pred »zlonamernimi tretjimi osebami«, ki bi želeli vdreti v njihove osebne podatke in jim ukrasti identiteto za lastno finančno korist.

Vrnimo se k spletnim družbenim omrežjem, kjer ne moremo mimo Facebooka in Googla s storitvijo Google+. Oba sta pred kratkim najavila uvedbo metod za samodejno prepoznavo (obrazov) oseb na fotografijah. Google+ bo na fotografijah, ki jih bodo uporabniki naložili, samodejno identificiral njihove prijatelje, Facebook pa uvaja podobno funkcionalnost (»Tag Suggestions«), ki uporabniku s pomočjo prepoznave obrazov poda namige, kdo naj bi bil udeležen na fotografijah in kako mu enostavno pripeti ime in priimek. Če je Facebook to možnost vključil kot privzeto in dal uporabnikom le možnost opt-out, je Google ubral bolj prefinjeno pot in je uporabo tega orodja označil kot izbirno. Glede na dogovor z irskim pooblaščencem bo, kot vse kaže, tudi Facebook moral veliko svojih praks spremeniti v sistem opt-in. Spletni velikani so že sprevideli, da jo precej bolje odnesejo, če nas prepričajo, da si nekaj res želimo, kot pa da nas prisilijo v deljenje podatkov s sistemom opt-out.

Je torej opt-in rešitev in srebrna krogla za težave z netransparentnimi poslovnimi praksami in zavajanjem posameznikov? Se bojim, da ne (povsod).

Kot navaja Morozov, se spletni velikani ne sprašujejo, ali ima uporaba njihovih orodij, kot je samodejna prepoznava obrazov, tudi katere širše, celo negativne družbene posledice, temveč na orodja gledajo le kot na sredstvo za doseganje cilje, ki naj ne bi imelo drugih implikacij. Morozov to ponazarja z uporabo avtomobila kot orodja za premik iz točke A v točko B, pri čemer pa uporaba avtomobila za sabo pušča obsežen vpliv na ljudi, prostor, okolje, stopnjo smrtnosti in podobno, pri tem pa vprašanje, ali je uporabnik tehnologijo začel uporabljati po sistemu opt-in ali opt-out, ni tako bistveno. Podobno ima tudi samodejna prepoznava obrazov svoje implikacije, tega pa različni Phormi, NebuAdi in Facebooki ne želijo obravnavati, podobno kot prodajalce sistemov za nadzor dostopa na prstne odtise ne zanimajo nikakršni negativni vidiki uporabe le-teh. V njihovih propagandnih materialih ne boste dobili odgovorov na vprašanje, kje bomo ob zlorabi dobili nov prstni odtis ali obraz, če ga bomo nekega dne uporabljali kot vsakdanje sredstvo identifikacije pri vstopu v pisarno, računalnik, na mestni avtobus ali nogometni stadion. Preden se ljudska masa zave negativnih implikacij, je običajno že prepozno, saj je tehnologija že preveč vgrajena v naše življenje. Neoluditi na pohodu, bodo na to rekli kritiki – kako pa naj predvidimo vse mogoče uporabe tehnologije, ne da bi pri tem zavirali tehnološkega razvoja? Odgovor je težko najti, gotovo pa zanašanje na privolitev uporabnikov ne more biti vedno dovolj.

Nekatera področja našega življenja se namreč dotikajo tako pomembnih vrednot, da mehanizmov varstva enostavno ne smemo prepustiti posamezniku. Država nas nič ne vpraša, ali se strinjamo z obvezno uporabo varnostnega pasu v avtomobilu, čeprav bi marsikateri voznik raje podpisal sto soglasij in izjav, da se zaveda nevarnosti, samo da se mu ne bi bilo treba privezati pred vožnjo. Takšnih področij, kjer je država ocenila meje, kjer soglasje posameznika ne zadošča, je seveda veliko. Če bi namreč pristali na splošno poseganje v zasebnost komunikacije na podlagi privolitve posameznika v zameno za brezplačni internet, kot to želijo Phorm in njemu podobni, potem smo podpisali smrtno obsodbo zasebnosti na internetu. Čeprav v zameno za brezplačni internet je to cena, ki si je ne moremo in ne smemo privoščiti. Negativne eksternalije izgubljene zasebnosti so namreč preveč dolgoročno porazdeljene, da bi jih posameznik zmogel ustrezno oceniti. Mnenje Mednarodne delovne skupine za varstvo osebnih podatkov v telekomunikacijah (IWGDPT) tako trdno zagovarja stališče, da bi se operaterji morali vzdržati kakršnekoli uporabe DPI-tehnologij v namene oglaševanja. Če želimo ohraniti svojo komunikacijsko in informacijsko zasebnost na internetu, morajo biti države na področjih, kjer so vprašljive temeljne človekove pravice, toliko pokroviteljske, da bodo šle tudi čez zavestne odločitve posameznika in bodo od spletnih velikanov zahtevale več etičnosti in presoje vplivov na zasebnost oziroma bodo posegle po orodjih regulacije. Spremembe ePrivacy direktive v Evropi in ukrepi ameriškega nadzornika za trg (Federal Trade Commission) le-to potrjujejo.

Države so bile primorane regulirati monopole na številnih področjih. Ali nas torej protimonopolna zakonodaja čaka tudi pri monopolistih na trgu zbiranja osebnih podatkov? Če država ne bo poskrbela za nas, si bomo pomagali sami? Če se uporabniki doslej še niso vprašali, pa je verjetno sedaj – ko nam je Google z združitvijo podatkov svojih storitev na enem mestu in enotno politiko »zasebnosti« bolj plastično predstavil, kaj dejansko vse ve o nas – pravi čas za ponovni

premislek, ali resnično lahko zaupamo toliko podatkov enemu samemu podjetju. Morda pa regulacija s strani države ni pravi pristop in se rešitev skriva v civilni nepokorščini, ekstremni ozaveščenosti in aktivizmu uporabnikov interneta. Gibanja 99 %, pravične trgovine in okoljske aktiviste že poznamo v realnem svetu. Lahko podobno pričakujemo na področju zasebnosti in svobode na internetu? Annonymous in piratske stranke kažejo v to smer. Bomo videli. Se dobimo čez deset let, ko se tega najbrž ne bomo več spraševali.

Viri:

- International Working Group on Data Protection in Telecommunications: Working Paper on the Use of Deep Packet Inspection for Marketing Purposes, 48th meeting, 6-7 September 2010, dostopno na: http://www.datenschutz-berlin.de/attachments/726/WP_DPI_07_09_2010_675_41_10__2_.pdf?1292413821.
- Johnson, E. in Goldstein, D. Medicine: Do Defaults Save Lives? Science Magazine, 302 (5649), 1338-1339, 21. 11. 2003.
- Kim, R.: Deep Packet Inspection Circles Back for a Second Look. 24. 11. 2011, dostopno na: http://gigaom.com/2010/11/24/deep-packet-inspection-circles-back-for-a-second-look/.
- Kučić, Lenart J: Prvi uspeh kampanje proti Facebooku. 24. 12. 2011, dostopno na: http://www.lenartkucic.net/2011/12/24/prvi-uspeh-kampanje-proti-facebooku/.
- Lyons, D.: The Truth About Facebook Privacy—if Zuckerberg Got Real, 30. 11. 2011, dostopno na: http://www.thedailybeast.com/articles/2011/11/30/the-truth-about-facebook-privacy-if-zuckerberg-got-real.html.
- Morozov E.: Saving Face. How Google, Facebook, and other tech companies hide behind “opt-in” policies, 19.12.2011, dostopno na: http://www.slate.com/articles/technology/future_tense/2011/12/google_s_and_facebook_s_facial_recognition_opt_in_policies_are_a_smokescreen_.html
- O'Dell J.: Facebook’s biggest change yet: Actions are here. 18.1.2012, dostopno na: http://venturebeat.com/2012/01/18/facebook-actions-rollout/
- Tomšič, Andrej in Burnik, Jelena: DPI - pandorina skrinjica interneta? Pravna praksa 2011/13, 7.4.2011.