Javni interes i informacijska sigurnost

Scena informacijske sigurnosti nikad ne miruje. Radi se o mladoj disciplini koja se trudi uhvatiti korak sa sve bržim razvojem tehnologije i izazovima koje taj razvoj donosi. Implikacije su daleko šire od same tehnologije, one su političke, ekonomske, socijalne, općeljudske. Na taj se način dotiču i nas tehničara, koji na svoj skromni način sudjelujemo u širem društvenom zbivanju. Ali možda bismo mogli u većoj mjeri doprinjeti zajednici?

Iz medija saznajemo da Rusija planira izgraditi svoj vlastiti Internet, koji bi zapravo bio Ruski intranet, baš kao što mnoge tvrtke čuvaju svoje poslovne podatke u privatnoj mreži. Kakve su tu mogućnosti nadzora i kontrole moguće, ne treba posebno naglašavati. No vlada SAD gradi Govnet, svoj vlastiti intranet, zaštićen od napada izvana. Sve u cilju poboljšanja nacionalne sigurnosti. Pa zašto onda isto ne bi mogli napraviti Rusi? Razlika je u stupnju demokratičnosti dva društva, jer vlada SAD ne brani korištenje Interneta svojim građanima, a kritičari misle da bi se to u Rusiji moglo dogoditi. Sjećate se, ženski protestni bend PussyRiot izveo je performans u pravoslavnoj crkvi protestirajući radi činjenice da su mediji pet mjeseci prije izbora već proglasili Putina pobjednikom. Nastupom u crkvi aludirale su na povezanost Putina i vodstva crkve. Osuđene su radi "huliganizma motiviranog mržnjom prema vjeri". Nakon odslužene kazne, predvidjele su i pobjedu Trumpa, objavivši protestni video prije samih američkih predsjedničkih izbora. U SAD nisu radi toga tužene ni optužene, tamo ih nisu shvatili kao ozbiljnu prijetnju poretku.

Druga zanimljiva vijest je pokušaj SAD da spriječi širenje kineske informatičko-komunikacijske tehnologije po svijetu, prvenstveno kod svojih saveznika. Huawei proizvodi se ionako ne mogu kupiti na tržištu SAD (koje propagiraju ideologiju slobodnog tržišta), ali se prodaju u EU, pa i kod nas. Na prvi pogled, mogli bismo reći da nas Amerikanci mogu špijunirati svojim telefonima i mrežnom opremom, ali nije dobro ako to rade i Kinezi. Kad bi zatražili dokaze da Kinezi to rade, ne bi ih dobili. Možda zato što bi onda dobili i dokaze o tome da i druga strana čini iste stvari?

No tehnološki obrazovan i društveno osviješten pojedinac mogao bi reći da se radi o (ne)sigurnosti ugrađenoj u samu tehnologiju, u mrežne protokole, koje može koristiti za svoje svrhe svatko tko to zna i može. Pa onda i Rusi i Kinezi, čija društva nisu tako demokratska kao naša. Nećemo se ovdje upuštati u raspravu o tome koliko su razvijene demokracije stvarno demokratske i tko tamo zapravo upravlja društvom.

Uvijek se vraćamo na činjenicu da su problemi dijelom tehnološki, dijelom socijalni, a moćna tehnologija omogućava dosad neviđene zloupotrebe. Tako na primjer saznajemo da su u naslonima avionskih sjedala ugrađene kamere. One su dio zabavnog paketa zamišljenog da skrati dosadu prekooceanskih letova. U naslonu su sa stražnje strane ugrađeni ekrani i slušalice koje dokonim putnicima nude izbor filmova. Kamera i mikrofon su skriveni dio paketa za koji avio kompanije tvrde da ih nikad ne koriste. Ali tu su, ako zatreba..Trebamo se zabrinuti nad mišlju da zapravo ne znamo u koje su sve uređaje koje kupujemo ugrađeni mikrofoni i kamere "koji se ne koriste", a tvrtke su, eto, nekim čudnim previdom zaboravile spomenuti ih u tehničkim specifikacijama.

Jedini način da se obuzda prevelika moć koju tehnologija daje odabranim grupama jest zakonska regulativa. Pretpostavljamo da ludističko razbijanje strojeva kao rješenje problema ne dolazi u obzir. Naravno, nije dovoljno donijeti regulativu, treba je provoditi, a onda i nadzirati one koji upravljaju tehnologijom, da se ne bi, u polumraku svojih zatvorenih prostorija osilili i koristili tu moć za neke svoje ciljeve.

Tko donosi regulativu? To je ključno pitanje, koje si postavlja i legendarni Bruce Schneier. Po njemu, problem je u tome da regulativu donose ljudi koji ne poznaju tehnologiju. Propise i zakone pišu i predlažu ljudi kojima javni interes nije u prvom planu. Važniji im je neki drugi interes, briga za nacionalnu sigurnost, ili za komercijalne interese, koje lobiranjem nastoje progurati. Schneier tvrdi da nam nedostaju tehnološki obrazovani ljudi koji razumiju i kako funkcionira društvo, sposobni artikulirati i nametnuti brigu za opće dobro.

Schneier konstatira da oni koji donose pravila (policy) ne razumiju tehnologiju, niti oni koji razumiju tehnologiju razumiju političku razinu rasprave. Oni govore jedni mimo drugih, a prijedlozi politika, kad se usvoje, predstavljaju katastrofu s tehnološkog stanovišta. Takva situacija nije održiva, a jedini način koji Schneier vidi kao rješenje jest da se angažiraju tehnolozi koji se zalažu za javni interes (**public-interest technologists**).

Ovdje se moramo na trenutak zaustaviti da bi objasnili kako u engleskom postoje dva izraza, **policy** i **politics**, koji se kod nas prevode jednim izrazom, politika. Bolje bi bilo da umjesto sigurnosna politika kažemo sigurnosni pravilnik, jer su to norme ponašanja i pravila koja važe za pojedine profesije, kodeksi, a ne političke igre moći.

Dakle, možemo li reći da Schneier ne očekuje od političara ili pravnika da razumiju javni interes i opće dobro, jer su oni opsjednuti nekim drugim prioritetima, nacionalnom sigurnošću, međunarodnim prijetnjama i slično, pa su olako spremni žrtvovati osobne slobode i privatnost svojih građana kako bi ih "zaštitili"? Schneier ističe da američki zakoni bolje štite privatnost američkih građana, ali nimalo ne štite privatnost građana ostaka svijeta. "Na vašem mjestu bio bih zabrinut!", rekao na svom predavanju na konferenciji FSEC u Varaždinu. Eto, sad imamo još više razloga za brigu, jer se u tehnološko političku igru uključuju još i Kina, Rusija i tko zna koja država.

Enkripcija je u središtu interesa, oko nje se lome koplja već decenijama. Mogu li se pomiriti na prvi pogled međusobno isključive potrebe nacionalne sigurnosti i zaštita privatnosti? Obavještajcima smeta enkripcija, oni bi željeli pratiti komunikaciju terorista i kriminalaca. S druge strane, obični građani koji ne predstavljaju prijetnju nikome ne žele da ih se nepotrebno nadzire. Sama tehnologija je tu neutralna, ali se naprosto nudi za zloupotrebe raznih vrsta, od dobronamjernih do zlonamjernih. Problem je tko će se okoristiti moćima koje nudi tehnologija? Kriminalci, teroristi, nedemokratski vlastodršci, nesavjesni pojedinci na položajima koji im omogućuju neovlašteno presretanje tuđih poruka? Hoće li sve riješiti regulativa, ako znamo da će je mnogi nekažnjeno zanemarivati?

Kod nas u domeni .hr pripremaju se još jedni izbori. Kao dio predizbornog folklora plasiraju se vijesti o tome što su sve igrači na političkoj sceni zgriješili, od prometnih nesreća do sukoba interesa, materijalne koristi, itd. Te se vijesti kao slučajno plasiraju baš u predizborno vrijeme, tako da se tu ne radi o zaštiti zakonitosti, jer bi se u tom slučaju optužbe pokrenule u vrijeme kad su prekršaji počinjeni. To su igre prijestolja u kojima sudjeluje obavještajno podzemlje, sigurnjaci koji nisu pravi profesionalci već su u službi pojedinih stranaka i moćnika. Na sceni su manipulacije mnogih vrsta. Ponešto od objavljenog je istina, ponešto poluistina, uz zlonamjerno tumačenje, ponešto vjerojatno i neistina. Žrtva može tužiti novinare, ali ako i dobije zadovoljštinu to će biti za koju godinu, kad izbori već budu daleka prošlost.

Vodeća politička snaga pred lokalne izbore je objavila rezultate ankete po kojoj će na izborima dobiti 44% glasova. Na kraju ih dobiju desetak posto manje, ali se prešućuje da je to postotak onih koji su izašli na izbore, a ne postotak ukupnog stanovništva s pravom glasa. Što ako pola građana koji imaju pravo glasa uopće ne izađe na izbore? Tada stranka koja dobije stvarnih 15% svih mogućih glasova ostvari gotovo apsolutnu vlast, predstavljajući se kao glas naroda. A oni koji izađu na izbore ali glasaju za minorne stranke samo daju legitimitet izbornim pobjednicima. Sve više mojih znanaca odbija sudjelovati u toj igri, iako su svjesni činjenice da time samo ojačavaju postojeće stanje, barem dok se ne stvori kritična masa onih koji ne izlaze na izbore. Politika je složenija od tehnike, tu nije tako lako uklanjati bugove, pogotovo one ugrađene u algoritam.

Zašto spominjemo domaće izbore u članku o informacijskoj sigurnosti? Zato što, htjeli ne htjeli **tehnologija je važan dio društva, danas postaje odlučujući faktor u raspodjeli moći, a ta njena funkcija nije dovoljno osviještena** i o njoj se ne raspravlja. Osnovna pismenost danas

podrazumijeva razumijevanje načina na koji se koristi tehnologija, pa i stvaranje imuniteta na njene zloupotrebe.

Tehnolozi javnog interesa su "**tehnološki praktičari koji se fokusiraju na društvenu pravednost, zajedničko dobro i javni interes**". Tim Berners-Lee, otac World Wide Weba naziva ih "**filozofskim inženjerima**". Njiihovo je postojanje nasušna potreba ako ne želimo da se tehnologija okrene protiv čovječanstva. Citiram Bruce Schneiera: "Trebamo tehnologe javnog interesa u raspravama o politici, u osoblju kongresa, u vladinim agencijama, u nevladinim organizacijama, u akademiji, u tvrkama, u novinarstvu. Trebamo ih uključiti ne samo u kripto ratove, već svugdje gdje se kibersigurnost i politika dodiruju, u raspravama o ranjivostima, sigurnosti izbora, pravilima koja reguliraju kriptovalute, sigurnosti IoT, big data, poštenim algoritmima, strojnom učenju, kritičnoj infrastrukturi i nacionalnoj sigurnosti. Kada proširite definiciju informacijske sigurnosti, mnoga područja spadaju u presjek kibersigurnosti i politike. Naša specifična ekspertiza i način gledanja na svijet kritični su za razumijevanja mnogih tehnoloških područja, kao što je mrežna neutralnost (net neutrality) i regulacija kritične infrastrukture. Ne bih želio formulirati javnu politiku o umjetnoj inteligenciji i robotici bez sudjelovanja tehničara specijaliziranih za sigurnost."

U svijetu postoje takve organizacije tehničara usmjerenih javnoj dobrobiti, Schneier ih spominje nekoliko: od starijih organizacija poput EFF [1] i EPIC [2] do novijih poput Verified Voting [3] i Access Now [4]. Mnogi akademski programi kombiniraju tehnologiju i javne politike.. Medijski startupi kao što je The Markup [5] bave se tehnološki orijentiranim žurnalizmom, prate kako korištenje tehnologija utiče na čovječanstvo. Postoje čak programi i inicijative usmjerene na javni interes unutar komercijalnih korporacija.

No Schneira brine činjenica da ljudi takvog profila naprosto nema dovoljno! Da bi javni interes bio zaštićen, trebalo bi ih biti aktivnih mnogo više nego što je to slučaj danas! Tada bi tehnologija koju koristimo bila mnogo sigurnija već po dizajnu, a mogućnosti njezine zloupotrebe bile bi mnogo manje. Schneier uporno ponavlja da tehnologija mora biti sigurna za sve, da svaki pokušaj da se napravi tehnologija koja je sigurna "za nas" a nesigurna "za njih" dovodi do nesigurnosti za sve.

Zanimljivo je pitanje da li u .hr domeni postoje društveno osviješteni tehničari koji su spremni angažirati se na promoviranju općeg dobra? O tome nemam saznanja, ako čitatelji znaju više neka podijele informacije s nama. Demokracija je ovdje još u povojima, a većina ljudi smatra da je dovoljno dati nekoj stranci glas na izborima, pa će se oni pobrinuti za sve. Nažalost, stvari tako ne funcioniraju. U zastupničkom sustavu morate paziti čije interese zapravo zastupaju ljudi kojima ste dali povjerenje. Hoće li takvo razmišljanje potaknuti nekog kolegu sistemca da se angažira u "hakiranju društva"? Više očekujem od pobornika slobodnog softvera, jer je to po sebi već način društvenog angažmana. Tko zna, možda se za početak učlane u neki NGO?

Danas je objavljena još jedna zanimljiva vijest: Rusija radi na testiranju, u Moskovskoj oblasti, elektroničkog glasanja temeljenog na blockchain tehnologiji! Hoće li u izgradnji i korištenju te tehnološke inovacije biti uključeni tehničari koji će kao sokolovi paziti na zaštitu javnog interesa?

sri, 2019-03-13 21:37 - Aco Dmitrović**Kategorije:** Kolumna [6]
Vote: 0

No votes yet

story_tag: informacijska sigurnost [7]
javni interes [8]
Bruce Schneier [9]

Source URL: https://sysportal.carnet.hr/node/1843

Links
[1] https://www.eff.org/%20
[2] %20https://www.epic.com/
[3] https://www.verifiedvoting.org/%20
[4] https://www.accessnow.org/.
[5] https://themarkup.org/%20
[6] https://sysportal.carnet.hr/taxonomy/term/71
[7] https://sysportal.carnet.hr/taxonomy/term/101
[8] https://sysportal.carnet.hr/taxonomy/term/313
[9] https://sysportal.carnet.hr/taxonomy/term/314