Specijalna edukacija i rehabilitacija (Beograd), Vol. 12, br. 1. 25-41, 2013.

UDK: 316.644-057.875:341.721(497.11); 343.982:004.4
ID: 198146572
Originalni naučni rad
doi: 10.5937/specedreh12-3283

Marina M. KOVAČEVIĆ-LEPOJEVIĆ[1]
Vesna ŽUNIĆ-PAVLOVIĆ
Tatjana S. MENTUS
Univerzitet u Beogradu
Fakultet za specijalnu edukaciju i rehabilitaciju

PREISPITIVANJE MODELA TEHNOLOŠKOG PRAGMATIZMA U TUMAČENJU BEZBEDNOSTI I PRIVATNOSTI[2]

Model tehnološkog pragmatizma pretpostavlja svest o tome da tehnološki razvoj sa sobom nosi brojne dobrobiti, ali i opasnosti sa druge strane. Većina savremenih bezbednosnih tehnologija u svojoj suštini predstavlja sredstvo masovnog nadzora građana, pri čemu može doći do kompromitovanja značajne količine ličnih podataka usled odsustva ili nedovoljnog institucionalnog nadzora i kontrole. Sa druge strane, građani su zainteresovani za poboljšanje zaštite od kriminala i smanjenje straha od potencijalne viktimizacije što im se u ovom okviru nudi kao racionalno opravdanje za evidentan gubitak privatnosti, ličnih sloboda i prava. Stavovi građana prema kategorijama bezbednost i privatnost i njihovom uravnotežavanju mogu dati neophodne smernice za regulisanje primene bezbednosnih tehnologija u datom kontekstu.

Cilj rada predstavlja sagledavanje stavova studenata Univerziteta u Beogradu (N=269) prema primeni bezbednosnih tehnologija i identifikovanje ključnih dimenzija stavova. Na osnovu relevantnih istraživanja pošlo se od pretpostavke o izdvajanju dimenzija bezbednost, privatnost, poverenje u državne institucije i zabrinutost zbog zloupotrebe bezbednosnih tehnologija. Za potrebe prikupljanja podataka

1 E-mail: marina.lepojevic@gmail.com

2 Rad je proistekao iz projekta „Kriminal u Srbiji: fenomenologija, rizici i mogućnosti socijalne intervencije“, broj 47011 (2011-2014), čiju realizaciju finansira Ministarstvo prosvete, nauke i tehnološkog razvoja Republike Srbije.

korišćen je upitnik Prise Questionnaire on Security Technology and Privacy. Faktorskom analizom izdvojeno je osam faktora koji zajednički objašnjavaju 58% ukupne varijanse, sa najvećim zasićenjem na četiri faktora koji su označeni kao bezbednost, privatnost, poverenje i zloupotreba. Rezultati istraživanja podržavaju model tehnološkog pragmatizma u tumačenju odnosa bezbednosti i privatnosti. Otkrivene korelacije između faktora bezbednost i privatnost i faktora poverenje i zloupotreba ukazuju na spremnost studenata da žrtvuju svoju privatnost u funkciji unapređivanja bezbednosnog statusa i obrnuto.

Ključne reči: *bezbednosne tehnologije, kriminal, privatnost, Srbija, studenti*

UVOD

Još uvek se vode polemike oko odgovora na pitanje gde je granica bezbednosti i u kom trenutku „više" bezbednosti postane „premalo" slobode. Da li smo spremni da podnesemo različite kolektivne i individualne žrtve „unapređene" bezbednosti i jesu li one neophodne? Da li su prava na zaštitu građana od kriminala „starija" od prava na zaštitu ličnosti? U tom kontekstu razmatraju se kategorije bezbednost i privatnost sa tehnološkog, ekonomskog, socijalnog, kulturnog i drugih aspekata. Međutim, odnosi između pomenutih dimenzija predmet su stalnih rasprava i pravi izazov za akademsku i širu javnost.

Tehnološki pragmatizam nalazi utemeljenje u radovima autora koji su se bavili izučavanjem fenomena rizičnosti prema kojima se svako uvećanje sloboda i prava građana tumači kao umanjenje bezbednosti i obrnuto (Beck, 2002; Bauman, 2009; Svensen, 2008). Sa stanovišta tehnološkog pragmatizma koji se oslanja na racionalnu procenu rizika i dobiti koje se ostvaruju putem primene bezbednosnih tehnologija, bezbednost i privatnost su viđene kao pojave koje su u protivrečju, gde višak bezbednosti neminovno povlači manjak privatnosti i obrnuto (Pavone & Esposti, 2012; Dourish & Anderson, 2006; Davis & Silver, 2004; Boywer, 2004). Suština pragmatičnog pristupa je sagledavanje opasnosti od gubitka privatnosti i drugih rizika kao opravdanih i u funkciji unapređivanja bezbednosti pojedinaca i grupa. Model se smatra ekonomskim ne u finansijskom smislu, već u kontekstu proračunatog izbora za nagradu, uz izvestan rizik, odnosno do-

bit uz određenu cenu koja je u najširem smislu uvek u vezi sa otkrivanjem i prenošenjem određenih informacija kojima se trguje (Dourish & Anderson, 2006:326). Prema tome, u kontekstu primene bezbednosnih tehnologija trguje se privatnošću zarad bezbednosti i obrnuto.

Nacionalno istraživanje stavova građana SAD prema bezbednosnim tehnologijama nakon terorisičkih napada 11. septembra 2001. godine, pokazalo je veću spremnost ispitanika da ustupe svoju privatnost zarad više bezbednosti. Međutim, rezultati istraživanja ukazuju na značaj i nekoliko drugih faktora u opredeljivanju za „više" bezbednosti ili privatnosti sa druge strane. Na primer, Afroamerikanci su se češće nego belačka i latinoamerička populacija opredeljivali za više privatnosti, što je razumljivo imajući u vidu njihovu istorijsku borbu za ljudska prava, kao i liberali za razliku od konzervativaca. Nivo potencijalne pretnje i to kolektivne učestalije nego lične, pokazao se kao važan faktor za opredeljivanje u pravcu unapređenja bezbednosti (Davis & Silver, 2004). Istraživanje stavova građana prema bezbednosnim tehnologijama u Evropi nije potvrdilo značaj nivoa pretnje pri odlučivanju za povećanje bezbednosti, s tim što se izvesne razlike uočavaju u pravcu percipiranja kolektivne pretnje. Građani Španije, zemlje sa istorijom terorističkih napada tako nisu pokazali spremnost da ustupe privatnost zarad više bezbednosti (Pavone & Pereira, 2009). Istraživanja pokazuju da na percepcije bezbednosnih tehnologija i odnosa bezbednosti i privatnosti posebno utiče faktor poverenja u državne institucije odgovorne za uvođenje i primenu bezbednosnih tehnologija u datom kontekstu. Prema tome, u duhu tehnološkog skepticizma i uz prisutno nepoverenje u državne institucije, građani bezbednosne tehnologije nekritički smatraju ugrožavajućim po privatnost, bez opažanja i najmanjih pozitivnih uticaja. Sa druge strane, tehnološkim entuzijazmom zaneseni stručnjaci i građani imaju bezrezervno poverenje u bezbednosne tehnologije koje smatraju neophodnim oruđem za borbu protiv kriminala negirajući i minimalna ograničenja privatnosti.

Istraživačka studija stavova građana šest zemalja Evropske unije (Austrija, Španija, Nemačka, Danska, Mađarska i Norveška) pokazala je da je mišljenje građana o uvođenju bezbednosnih tehnologija pretežno polarizovano (Pavone & Esposiți, 2012). Građani koji su imali poverenja u državne institucije i verovali da bezbednosne tehnologije povećavaju njihovu bezbednost zanemarivali su negativne posledice primene, kao

na primer ograničenja privatnosti. Sa druge strane, građani koji su bili zabrinuti oko toga koliko bezbednosne tehnologije negativno utiču na očuvanje slobode i privatnosti, zanemarivali su pozitivne potencijale bezbednosnih tehnologija. Poverenje u državne institucije koje odgovaraju za primenu bezbednosnih tehnologija i državnu politiku generalno se pokazalo kao presudno za one koji su izražavali podršku primeni bezbednosnih tehnologija i uverenju da one doprinose boljoj bezbednosti ne ugrožavajući ljudska prava. Obrnuto, oni koji su se plašili da će državne službe zloupotrebiti slobode građana, smatrali su da bezbednosne tehnologije samo ograničavaju privatnost.

Polarizovano mišljenje građana u odnosu na faktor poverenja u državne institucije koje sprovode politiku kontrole kriminala potvrđeno je pri pomenutom istraživanju stavova građana prema bezbednosnim tehnologijama u SAD (Davis & Silver, 2004). Pored toga, i drugi istraživački nalazi idu u pravcu preispitivanja koncepta racionalizacije privatnosti, pridružuju se priznavanju prethodno opisane i uočene dihotomije, uz zapažanje da su građani spremni da svesno ugroze svoju privatnost za najminimalniju nagradu (Hann et al., 2002).

Predmet ovog rada su aspekti bezbednosti i privatnosti u primeni bezbednosnih tehnologija. U radu se preispituju postojeća stanovišta o percepcijama studenata u pogledu primene bezbednosnih tehnologija. Prvo stanovište je da na percepcije utiče racionalna procena dobiti (unapređenje bezbednosti) i gubitaka (ugrožavanje privatnosti). Drugo stanovište naglašava presudan uticaj faktora poverenja u institucije koje su odgovorne za uvođenje i primenu bezbednosnih tehnologija u oblikovanju percepcija. U radu se preispituje koncept tehnološkog pragmatizma. Posebno, razmatra se koliko prethodna uverenja studenata u kontekstu poverenja u državne institucije i zabrinutosti zbog zloupotrebe utiču na formiranje stavova koji se odnose na zalaganje za bezbednost ili privatnost.

Cilj istraživanja

Cilj istraživanja je utvrđivanje latentnih dimenzija stavova studenata prema bezbednosnim tehnologijama. U isto vreme je ispitana kriterijumska validnost originalnog instrumenta na srpskom govornom području, s obzirom da je originalna engleska verzija prevođena na pet

jezika (nemački, norveški, danski, španski i mađarski) (PRISE, 2007). Pitanje na koje se ovim radom pokušava odgovoriti je da li je struktura latentnih dimenzija koje stoje u osnovi stavova prema bezbednosnim tehnologijama dvodimenzionalna (bezbednost i privatnost) ili četvorodimenzionalna (bezbednost, privatnost, poverenje i zloupotreba).

METODE ISTRAŽIVANJA

Uzorak je činilo 269 studenata fakulteta na kojima se izučavaju krivičnopravne i kriminološke nauke Fakulteta za specijalnu edukaciju i rehabilitaciju, Kriminalističko-policijske akademije i Pravnog fakulteta (123 muškog i 146 ženskog pola). Za potrebe prikupljanja podataka korišćen je *Prise Questionnaire on Security Technology and Privacy* (PRISE, 2007), koji se sastoji iz 170 pitanja zautvrđivanje stavova prema biometrijskim tehnologijama, video nadzoru i skeniranju, prisluškivanju, tehnologijama za lociranje građana i automobila, zadržavanju podataka o ličnosti, tehnologijama za zaštitu privatnosti, dilemama u vezi sa primenom bezbednosnih tehnologija, ljudskim pravima i predlozima za zaštitu privatnosti. Na početku, izdvojena je grupa od dvadeset sedam pitanja koja izražavaju stavove studenata u pogledu doprinosa navedenih bezbednosnih tehnologija u pravcu unapređivanja bezbednosti ili narušavanja privatnosti. Sve varijable su petostepene, pri čemu se ponuđeni odgovori kreću u rasponu od „potpuno se slažem“ do „ne slažem se uopšte“. Za statističku obradu podataka korišćena je eksplorativna analiza glavnih komponenata za primenu kose rotacije faktora, kako bi se izdvojile relevatne dimenzije za tumačenje stavova studenata prema pitanjima bezbednosti i privatnosti kao i za analizu kriterijumske validnosti upitnika pri primeni na sprskom govornom području.

REZULTATI ISTRAŽIVANJA

Nakon što je preliminarnim testovima utvrđeno da je moguće primeniti ovu vrstu analize (Kaiser-Meyer-Olkin skor adekvatnosti uzorkovanja 0,8 i Bartlett test χ^2=1760; p<0,000) pristupljeno je eksplorativnoj faktorskoj analizi.

Primenom Guttman-Kaiser kriterijuma izdvojeno je osam faktora koji zajednički objašnjavaju 58% ukupne varijanse. U Tabeli 1 prikazano je koliko svaka od izdvojenih dimenzija prema Guttman – Kaiser kriterijumu doprinosi objašnjenju varijanse bezbednosnih tehnologija. Primećuje se da su prve dve dimenzije najznačajnije i da zajednički objašnjavaju 28% ukupne varijanse, dok ostale objašnjavaju preostalih 30%.

Tabela 1 – Izdvojene komponente i ukupna varijansa objašnjena faktorima

Dimenzija	Suma kvadratnih zasićenja dimenzija			Suma kvadratnih zasićenja nakon rotacije
	Ukupno	% varijanse	Kumulativni %	Ukupno
1	4,17	15,45	15,45	3,33
2	3,44	12,76	28,22	2,83
3	1,76	6,52	34,75	2,63
4	1,52	5,64	40,39	2,49
5	1,37	5,09	45,48	2,37
6	1,22	4,54	50,03	1,79
7	1,12	4,17	54,21	1,55
8	1,05	3,91	58,13	1,47

Prethodno izolovane glavne komponente su, radi lakše interpretacije aktuelne faktorske strukture, rotirane u promax poziciju, a zatim je sadržinskom analizom izdvojeno četiri faktora koji zajednički objašnjavaju 40% varijanse zavisne varijable (Tabela 2). Primećuje se da prvi, a zatim i drugi faktor imaju najveća faktorska zasićenja što nije neobično s obzirom na to da je poredak faktora definisan proporcijom ukupne varijanse protumačene određenim faktorom. Prvi faktor ima najveće zasićenje na stavki „Mogućnost lociranja mobilnih telefona osumnjičenih je dobro sredstvo da policija istraži i prevenira ugrožavanje građana i kriminal“ (0,69), a najmanje na stavkama „Video nadzor čini da se osećam mnogo sigurnijim/om“ (0,56) i „Prisluškivanje je dobro sredstvo za policijsku istragu“ (0,56). Drugi faktor ima ujednačena zasićenja na svim stavkama (0,60), osim na stavki sa najvećim zasićenjem „Mogućnost lociranja svih mobilnih telefona ugrožava privatnost“ (0,70).

Tabela 2 – Matrica komponenti

	1	2	3	4
Mogućnost lociranja mobilnih telefona osunjičenih je dobro sredstvo da policija istraži i prevenira ugrožavanje građana i kriminal.	0,69			
Skladištenje i kombinovanje ličnih podataka iz različitih baza podataka je dobro sredstvo da policija prevenira ugrožavanje građana.	0,67			
Mogućnost lociranja svih automobila je dobro sredstvo da policija istraži i prevenira ugrožavanje građana i kriminal.	0,64			
Skeniranje građana u cilju pronalaženja skrivenih predmeta je potpuno prihvatljivo.	0,61			
Čuvanje biometrijskih podataka svih građana u centralnoj bazi podataka je prihvatljiv korak u borbi protiv kriminala.	0,61			
Kada su bezbednosne tehnologije dostupne treba da ih koristimo.	0,57			
Države bi trebalo da čuvaju sve podatke koje smatraju važnim iz bezbednosnih razloga onoliko dugo koliko misle da je potrebno.	0,57			
Video nadzor čini da se osećam mnogo sigurnijim/om.	0,56			
Prisluškivanje je dobro sredstvo za policijsku istragu.	0,56			
Mogućnost lociranja svih mobilnih telefona ugrožava privatnost.		0,70		
Prisluškivanjem se ozbiljno narušava privatnost.		0,60		
Mogućnost lociranja svih automobila ugrožava privatnost.		0,60		
Skladištenje i kombinovanje ličnih podataka iz različitih baza podataka ugrožava privatnost građana.		0,60		
Video nadzor narušava moju privatnost.		0,60		
Neprijatno je biti pod nadzorom čak i kada nemate kriminalne namere.		0,60		
Postoji mogućnost da državne službe zloupotrebe nove tehnologije.			0,57	
Postoji mogućnost da kriminalci zloupotrebe nove bezbednosne tehologije.			0,53	
Ako nemate šta da krijete, ne treba da brinete zbog ugrožavanja privatnosti putem tehnologija.				0,55
Treba čuvati samo one podatke o komunikaciji putem telefona, mobilnog i interneta koji su neophodni za naplaćivanje usluga.				0,54

Daljom analizom stavke su se sadržinski preraspodelile na četiri faktora sa po četiri (prvi i drugi faktor), odnosno tri (treći i četvrti faktor) stavke koje ih zasićuju. U Tabeli 3 prikazani su odgovarajući koeficijenti zasićenja stavki rotiranih dimenzija nakon primene kose rotacije faktora.

Tabela 3 - Matrica sklopa

	1	2	3	4
Skeniranje građana u cilju pronalaženja skrivenih predmeta je potpuno prihvatljivo.	0,70			
Video nadzor čini da se osećam mnogo sigurnijim/om.	0,68			
Skladištenje i kombinovanje ličnih podataka iz različitih baza podataka je dobro sredstvo da policija prevenira ugrožavanje građana.	0,65			
Čuvanje biometrijskih podataka svih građana u centralnoj bazi podataka je prihvatljiv korak u borbi protiv kriminala.	0,56			
Mogućnost lociranja svih automobila je dobro sredstvo da policija istraži i prevenira ugrožavanje građana i kriminal.		0,70		
Tehnologije za zaštitu privatnosti ne bi trebalo da budu dostupne ukoliko ometaju policijsku istragu i prevenciju ugrožavanja građana i kriminala.		0,65		
Mogućnost lociranja mobilnih telefona osumljičenih je dobro sredstvo da policija istraži i prevenira ugrožavanje građana i kriminal.		0,65		
Prisluškivanje je dobro sredstvo za policijsku istragu.		0,61		
Korišćenje baza ličnih podataka za neku drugu svrhu osim one za koju su prvobitno namenjeni ozbiljno ugrožava privatnost			0,83	
Skladištenje i kombinovanje ličnih podataka iz različitih baza podataka ugrožava privatnost građana.			0,77	
Prisluškivanjem se ozbiljno narušava privatnost.			0,59	
Postoji mogućnost da državne službe zloupotrebe nove tehnologije.				0,84
Postoji mogućnost da kriminalci zloupotrebe nove bezbednosne tehnologije.				0,79
Neprijatno je biti pod nadzorom čak i kada nemate kriminalne namere.				0,70

U Tabeli 4 prikazani su rezultati ekstrahovanih rotiranih faktora metodom analize glavnih komponenti uz primenu promax rotacije faktora. Izdvojeni su i imenovani sledeći faktori: bezbednost, privatnost, poverenje u državne institucije i zabrinutost zbog zloupotrebe bezbednosnih tehnologija. Faktor bezbednost ima najveća zasićenja na stavkama „Skladištenje i kombinovanje ličnih podataka iz različitih baza podataka je dobro sredstvo da policija prevenira ugrožavanje građana“ (0,69), „Video nadzor čini da se osećam mnogo sigurnijim/om“ (0,68) I „Skeniranje građana u cilju pronalaženja skivenih predmeta je potpuno prihvatljivo“ (0,68). Faktor privatnost ima najveća zasićenja na stavkama „Skladištenje i kombinovanje ličnih podataka iz različitih baza podataka ugrožava privatnost građana“ (0,74) i „Prisluškivanjem se ozbiljno narušava privatnost“ (0,71). Faktor koji pretpostavlja

poverenje u državne institucije koje su odgovorne za uvođenje i primenu bezbednosnih tehnologija najveća zasićenja ima na stavkama „Mogućnost lociranja svih automobila je dobro sredstvo da policija istraži i prevenira ugrožavanje građana i kriminal“ (0,80) i „Mogućnost lociranja mobilnih telefona osumnjičenih je dobro sredstvo da policija istraži i prevenira ugrožavanje građana i kriminal“ (0,70). Kod faktora koji reprezentuje zabrinutost zbog zloupotrebe bezbednosnih tehnologija najviše zasićenje zastupljeno je na stavkama „Postoji mogućnost da državne službe zloupotrebe nove tehnologije“ (0,82) i „Postoji mogućnost da kriminalci zloupotrebe nove tehnologije“ (0,77).

Tabela 4 – Matrica strukture

BEZBEDNOST	Faktor 1				
	Skladištenje i kombinovanje ličnih podataka iz različitih baza podataka je dobro sredstvo da policija prevenira ugrožavanje građana.	0,69			
	Video nadzor čini da se osećam mnogo sigurnijim/om.	0,68			
	Skeniranje građana u cilju pronalaženja skrivenih predmeta je potpuno prihvatljivo.	0,68			
	Čuvanje biometrijskih podataka svih građana u centralnoj bazi podataka je prihvatljiv korak u borbi protiv kriminala.	0,60			
	Države bi trebalo da čuvaju sve podatke koje smatraju važnim iz bezbednosnih razloga onoliko dugo koliko misle da je potrebno.	0,54			
PRIVATNOST	Faktor 2				
	Skladištenje i kombinovanje ličnih podataka iz različitih baza podataka ugrožava privatnost građana.		0,74		
	Prisluškivanjem se ozbiljno narušava privatnost.		0,71		
	Korišćenje baza ličnih podataka za neku drugu svrhu osim one za koju su prvobitno namenjeni ozbiljno ugrožava privatnost.		0,67		
POVERENJE	Faktor 3				
	Mogućnost lociranja svih automobila je dobro sredstvo da policija istraži i prevenira ugrožavanje građana i kriminal.			0,80	
	Mogućnost lociranja mobilnih telefona osumnjičenih je dobro sredstvo da policija istraži i prevenira ugrožavanje građana i kriminal.			0,70	
	Prisluškivanje je dobro sredstvo za policijsku istragu.			0,60	
	Tehnologije za zaštitu privatnosti ne bi trebalo da budu dostupne ukoliko ometaju policijsku istragu i prevenciju ugrožavanja građana i kriminala.			0,60	

ZLOUPOTREBA	Faktor 4				
	Postoji mogućnost da državne službe zloupotrebe nove tehnologije.				0,82
	Postoji mogućnost da kriminalci zloupotrebe nove tehnologije.				0,77
	Neprijatno je biti pod nadzorom čak i kada nemate kriminalne namere.				0,68

Izračunavanjem koeficijenata korelacije između identifikovanih faktora uočena je slaba pozitivna korelacija između faktora bezbednost i privatnost (0,26) i faktora poverenje i zloupotreba (0,35). Između faktora bezbednost i zloupotreba zabeležena je zanemarljiva korelacija (0,00) (Tabela 5).

Tabela 5 – Matrica interkorelacije faktora

	Faktor 1	Faktor 2	Faktor 3	Fasper 4
1	1,00	0,26	0,05	0,00
2	0,26	1,00	0,08	0,16
3	0,05	0,08	1,00	0,35
4	0,00	0,16	0,35	1,00

DISKUSIJA

U skladu sa ciljem istraživanja koji se sastoji u utvrđivanju latentnih dimenzija stavova studenata prema bezbednosnim tehnologijama, izvršena je eksplorativna faktorska analiza kojom su uz primenu kose rotacije faktora izdvojene relevatne dimenzije za tumačenje stavova: bezbednost, privatnost, poverenje i zabrinutost. Analizom faktorskih interkorelacija utvrđene su korelacije na relacijama bezbednost-pivatnost i poverenje-zabrinutost što upućuje na priznavanje tehnološkog pragmatizma kao dominantnog modela u tumačenju stavova studenata prema bezbednosnim tehnologijama.

Istraživački nalazi studije o stavovima građana Evropske unije prema bezbednosnim tehnologijama, ukazuju na dvofaktorsku strukturu stavova, pri čemu je potvrđeno da faktor poverenja u institucije koje su odgovorne za uvođenje i primenu bezbednosnih tehnologija ima veliki uticaj na stavove koji idu u pravcu unapređenja sigurnosti i obrnuto. Prema tome, bezbednost i poverenje nalaze se na jednom, a privatnost i zabrinutost na drugom polu (Pavone & Esposito, 2012).

Rezultati ovog istraživanja sugerišu da su beogradski studenti pokazali bolje poznavanje pozitivnih i negativnih aspekata primene bezbednosnih tehnologija istovremeno sagledavajući uvećanje bezbednosti i gubitak privatnosti s tim u vezi. Razlog može biti to što su uzorkom obuhvaćeni studenti sa određenim predznanjem o primeni bezbednosnih tehnologija. Međutim, postavlja se pitanje koliko je informisanost o primeni bezbednosnih tehnologija presudna za izražavanje stavova u pravcu uravnotežavanja privatnosti i sigurnosti. Dostupna istraživanja sugerišu da postoji spremnost da se bez obzira na posledice za minimalnu nagradu ustupa velika količina privatnih podataka, bez obzira na posledice (Acquisti & Grossklags, 2005).

Drugi razlog može biti taj što se u Srbiji kasni sa uvođenjem savremenih bezbednosnih tehnologija koje su po pravilu i najinvazivnije i izazivaju najviše polemike, pa se može reći da je rasprava u domaćoj javnosti nastupila paralelno sa uvođenjem relevantnih tehnologija u svetu. Nadalje, zemlje u kojima je zapaženo nekritičko opredeljivanje građana za unapređivanje bezbednosti (na primer SAD) imale su iskustvo drastičnih terorističkih napada (Davis & Silver, 2004), što ne važi za Srbiju. Zatim, prisluškivanje, skladištenje, pretraživanje i kombinovanje baza podataka o ličnosti i neovlašćeno zadržavanje podataka studenti su mogli smatrati naročito ugrožavajućim iz razloga suočavanja sa proteklim primerima zloupotrebe privatnosti mnogih političara, biznismena i drugih javnih i privatnih lica. Kontrolom Poverenika i Ombudsmana evidentirano je preko million slučajeva nezakonitog zadiranja u privatne komunikacije građana od strane bezbednosnih službi na godišnjem nivou (Šabić, 2012).

Republika Srbija još uvek nije usaglasila svoju legislativu koja se odnosi na zaštitu privatnosti sa međunarodnim i evropskim standardima, dok se paralelno radi i na ujednačavanju kriterijuma privatnosti u relevantnim zakonima i podzakonskim aktima. Međutim, sa značajnim problemima u tom smislu suočavaju se i zemlje Evropske unije, pri čemu su najuočljivije razlike u pogledu prirode političke kontrole, nivoa tehnološkog razvoja i stepena usaglašenosti regulative na nacionalnom, nadnacionalnom, međunarodnom nivou (Lodge, 2007:24).

Praktična iskustva pokazuju da nije jednostavno obezbediti da se, kako je propisano, podaci koriste isključivo u skladu sa propisima, odnosno samo u određene svrhe, kada je to nužno i pod posebnim

uslovima (Directive 95/46/EC). Nameće se pitanje da li je spremnost studenata da ustupe svoju bezbednost zarad privatnosti i obrnuto deklarativna ili nalazi svoju praktičnu primenu. Istraživanja su pokazala da su Amerikanci spremni da ustupe svoje lične podatke za eventualnu sekundarnu obradu za cenu od 39,8 do 49,7 dolara, pa se stiče utisak da privatnost ima i svoju ekonomsku cenu (Hann et al., 2002). Istraživački nalazi sugerišu da oni sa najnižim primanjima najmanje brinu u vezi sa potencijalnom zloupotrebom privatnosti (Acquisti & Grossklags, 2005). Autori ističu neke negativne aspekte popularizacije tehnološkog pragmatizma, kao što je na primer pretpostavka da su bezbednost i privatnost previše apstraktne vrednosti da bi se njima trgovalo, da je privatnost socijalna i kulturna kategorija, više nego ekonomska i tehnološka, i da se ne može svesti prosto na manipulisanje privatnim podatkom odnosno informacijom, već predstavlja deo šire socijalne prakse (Dourish & Anderson, 2006).

Preostale dve dimenzije, poverenje u državne institucije i zloupotreba bezbednosnih tehnologija se smatraju socijalno-političkim kategorijama. Često smo suočeni sa političkim manipulacijama strahom građana od kriminala, glorifikacijama borbe protiv terorizma, zastrašujućim procenama rizika na svetskom, nacionalnom i ličnom nivou. Prenaglašavanje pretnji može biti u funkciji skretanja pažnje sa drugih relevatnih političkih tema ili podsticati na poverenje u pravcu primene bezbednostnih tehnologija održavanjem ranjivosti i straha i podelu odgovornosti sa građanima sa druge strane (Pavone & Pereira, 2009). Američka baza otisaka prstiju sadrži 73 hiljade otisaka prstiju osoba koje su okarakterisane kao teroristi (FBI, 2012), dok se sredstva za obezbeđenje od terororizma zasnivaju na broju potencijalnih terorističkih ciljeva, pri čemu se na listi nalaze i prodavnice sladoleda, đevreka i slično (Svensen, 2008). Stiče se utisak da su sloboda, pravda, jednakost i demokratija pod stalnom pretnjom, na primer terorista, što je uticalo da se odustane od demokratskog principa „aktivnog poverenja" i promoviše „aktivno nepoverenje" (Beck, 2002:44). Kako bi se drugačije i objasnila velika popularnost bezbednosnih tehnologija bez značajne empirijske potvrde (Kovačević-Lepojević i Žunić-Pavlović, 2012). Ovim su zatvorena vrata racionalnom pragmatičnom modelu viđenja bezbednosnih tehnologija i odnosa bezbednosti i privatnosti.

Izjašnjavanje o poverenju u primenu bezbednosnih tehnologija može zavisiti i od vrste i dostupnosti date tehnologije. Na primer, rezultati istraživanja stavova građana Evrope prema primeni bezbednosnih tehnologija pokazuju da su se oni najnegativnije izjašnjavali o upotrebi tehnologija sa kojima imaju najmanje dodira, kao što je uređaj za skeniranje do gole kože ili tehnologija koje najviše zadiru u privatnost kao što je centralizacija biometrijskih podataka u registre (Jacobi & Holst, 2007). Građani bi prema preporukama autora pri izjašnjavanju o uvođenju bezbednosnih tehnologija trebalo da sagledaju da li je privatnost koja se tim putem potencijalno narušava suštinska ili ne, da li je bezbednost koja se tim putem uvećava privremena ili trajna, da li je uvećavanje bezbednosti značajno ili minorno (Bowyer, 2004).

Međutim, istraživanja kojim je utvrđen presudan značaj poverenja u državu su pokazala da se građani opredeljuju i za invazivnije tehnologije koje zahtevaju veći nadzor i kontrolu građana ukoliko veruju da su kao efektivnije preporučene od strane države (Pavone & Espositi, 2012). Faktor poverenja u državu je identifikovan kao snažniji od faktora nivoa potencijalne pretnje po nacionalnu bezbednost (Davis & Silver, 2004). Pojedini autori smatraju da je poverenje u državne institucije, u smislu donošenja relevantnih zakonskih i podzakonskih akata i njihove primene jedini uslov za uravnotežavanje privatnosti i bezbednosti (Chandler, 2006:241).

Prema sadržinskom kriterijumu pozitivna očekivanja prema bezbednosnim tehnologijama i poverenje u državne institucije nalaze se na jednoj, a zalaganje za privatnost i zabrinutost da ono može biti zloupotrebljeno na drugoj strani. Međutim, ono što je zajedničko za stavke na dimenzijama bezbednosti i privatnosti je da reprezentuju lične, a za poverenje i zabrinutost kolektivne dobiti odnosno pretnje. Korelaciona analiza identifikovanih faktora je pokazala da su srpski studenti na odnos bezbednosti i privatnosti, kao i poverenja i zabrinutosti gledali pretežno racionalno, u duhu tehnološkog pragmatizma. Naime, oni studenti koji su se zalagali za povećanje bezbednosti istovremeno su bili svesni neminovnog gubitka privatnosti, i po istom principu oni koji su imali poverenja u državne institucije odgovorne za uvođenje i primenu bezbednosnih tehnologija imali su u vidu da može doći do potencijalne zloupotrebe bezbednosnih tehnologija. Prema tome, može se reći da prethodna uverenja studenata u kontekstu poverenja u državne institu-

cije i straha od zloupotrebe nisu bitno uticala na formiranje stavova koji se odnose na zalaganje za bezbednost ili privatnost.

ZAKLJUČAK

Primenom upitnika *Prise Questionnaire on Security Technology and Privacy* na uzorku srpskih studenata dobijene su četiri dimenzije stavova: bezbednost, privatnost, poverenje i zloupotreba. Iste dimenzije su identifikovane primenom ovog upitnika u zemljama Evropske unije (Pavone & Esposti, 2012), čime je potvrđena njegova validnost na našem području. Izmerene su izvesne korelacije između faktora bezbednost i privatnost i faktora poverenje i zloupotreba. Navedeni rezultati upućuju na zaključak da poverenje u državne institucije nije značajan faktor pri opredeljivanju za „više" bezbednosti, već da odnos bezbednosti i privatnosti treba tumačiti u kontekstu tehnološkog pragmatizma. Jednostavno rečeno, kategorije isključuju jedna drugu, dok je njihovo uravnotežavanje jedan od najznačajnijih zadataka savremenog društva. Međutim, nađene korelacije su slabe i shodno tome treba ih uzeti sa rezervom, ali mogu poslužiti kao dobra polazna osnova za dalja istraživanja bezbednosti i privatnosti.

Za one koji poput Klarka (2009:189) nalaze da ne postoji izbor između bezbednosti i privatnosti, da se može imati ili oboje ili nijedno, kao značajna smernica za buduća istraživanja može poslužiti praktično viđenje privatnosti koje se zasniva na konstantnom i paralelnom unapređivanju bezbednosti sa jedne i privatnosti sa druge strane (Dourish & Anderson, 2006). Tehnologije za zaštitu privatnosti pokazuju kako tehnološke inovacije mogu staviti u funkciju unapređenja privatnosti, a da se istovremeno ne utiče na umanjenje bezbednosti.

LITERATURA

1. Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *Security and Privacy IEE*, *3* (1), 26-33. Bauman, Z. (2009). *Fluidni život*. Novi Sad: Mediterran publishing.
2. Beck, U. (2002). The terrorist threat: world risk society revisited. *Theory, Culture and Society*, *19* (4), 39-55.
3. Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine, 23* (1), 9–19.
4. Chandler, S. (2006). Collateral damage? The impact of national security crises on the fourth amendment protection against unreasonable searches. *University of Pittsburg Law Review, 68* (1), 217-241.
5. Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: public opinion in the context of the terrorist attacks on America. *American Journal of Political Science*, *48* (1), 28–46.
6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031-0050. Retrieved November 16, 2012. from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
7. Dourish, P., & Anderson, K. (2006). Collective information practice: exploring privacy and security as social and cultural phenomena. *Human-computer Interaction*, 21 (1), 319-342.
8. FBI (2012). *Integrated Automated Fingerprint Identification System*. Retrieved November 16, 2012. from http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis
9. Hann, H., Hui, K., Lee, T., & Png, I. (2002). Online information privacy: measuring the cost-benefit trade-off. 23rd Annual International Conference on Information Systems. Barcelona, Spain, 2002., p. 1-10. Retrived January 20, 2013. from http://www.comp.nus.edu.sg/~ipng/research/privacy_icis.pdf
10. Jacobi, A., & Holst, M. (2007).*Synthesis Report - Interview Meeting on Security Technology and Privacy*. Vienna: PRISE.

11. Kovačević-Lepojević, M., Žunić-Pavlović, V. (2012). Stavovi studenata prema primeni biometrijske identifikacije u bezbednosne svrhe. U N. Glumbić, V. Vučinić (ur.), *VI međunarodni skup Specijalna edukacija i rehabilitacija danas* (str. 159-163). Beograd: Fakultet za specijalnu edukaciju i rehabilitaciju.
12. Klark, R. (2009). *Kriminalitet u Americi*. Beograd: Univerzitet u Beogradu, Pravni fakultet.
13. Lodge, J. (2007). Freedom, security and justice: the thin end of the wedge for biometrics? *Ann Ist Super Sanita, 43* (1), 20-26.
14. Pavone, V., & Pereira, M. (2009). The privacy vs. security dilemma in a risk society: insights from the PRISE project on the public perception of new security technologies in Spain. In J. Čas (Ed.), *Towards privacy enhancing security technologies – the next steps* (pp. 109-127). Vienna: PRISE.
15. Pavone, V., & Esposti, S. D. (2012). Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security. *Public Understanding of Science, 21* (5), 1-16.
16. PRISE (2007). Questionnaire on Security technology and privacy. Vienna: PRISE
17. Svensen, L. (2008). *Filozofija straha*. Beograd: Geopoetika.
18. Šabić, R. (2012). Neophodno je obezbediti punu zaštitu ustavnih garancija o tajnosti komunikacija (Saopštenje poverenika, 2. novembar 2012.). Republika Srbija, Poverenik za informacije od javnog značaja. Pristupljeno 24. novembra 2012. sa http://www.poverenik.rs/sr/saopstenja/1480-neophodno-je-obezbediti-punu-zastitu-ustavnih-garancija-o-tajnosti-komunikacija.html

REVIEW OF THE MODEL OF TECHNOLOGICAL PRAGMATISM CONSIDERING PRIVACY AND SECURITY

Marina M. Kovačević-Lepojević, Vesna Žunić-Pavlović,
Tatjana S. Mentus
University of Belgrade – Faculty of Special Education and Rehabilitation

Summary

The model of technological pragmatism assumes awareness that technological development involves both benefits and dangers. Most modern security technologies represent citizens' mass surveillance tools, which can lead to compromising a significant amount of personal data due to the lack of institutional monitoring and control. On the other hand, people are interested in improving crime control and reducing the fear of potential victimization which this framework provides as a rational justification for the apparent loss of privacy, personal rights and freedoms. Citizens' perception on the categories of security and privacy, and their balancing, can provide the necessary guidelines to regulate the application of security technologies in the actual context.

The aim of this paper is to analyze the attitudes of students at the University of Belgrade (N = 269) toward the application of security technology and identification of the key dimensions. On the basis of the relevant research the authors have formed assumptions about the following dimensions: security, privacy, trust in institutions and concern about the misuse of security technology. The Prise Questionnaire on Security Technology and Privacy was used for data collection. Factor analysis abstracted eight factors which together account for 58% of variance, with the highest loading of the four factors that are identified as security, privacy, trust and concern. The authors propose a model of technological pragmatism considering security and privacy. The data also showed that students are willing to change their privacy for the purpose of improving security and vice versa.

Key words: security technology, crime, privacy, Serbia, students

Primljeno: 24. 01. 2013. *Prihvaćeno: 22. 03. 2013.*