VODIČ ZA OTVORENU UPRAVU

Privatnost i zaštita podataka

*Vodeći autor:OpenRightsGroup, i PrivacyInternational

Uvod

Privatnost je međunarodno priznato ljudsko pravo, utemeljeno u Univerzalnoj deklaraciji o ljudskim pravima, Međunarodnom paktu o građanskim i političkim pravima i Ustavu više od 100 zemalja širom sveta. Privatnost nije samo važno pravo samo po sebi, nego je ključni element individualne autonomije i dostojanstva i snažan faktor koji omogućava političke, duhovne, religiozne i čak i seksualne slobode. Neophodna je za definisanje odnosa između građana i njihove Vlade. Konkretni izrazi prava na privatnost zavise od konteksta i mogu reflektovati kulturne i društvene razlike.

Pravo na privatnost sažima pravo na zaštitu ličnih podataka: pojedinci imaju pravo da odluče da li da dostave ili podele svoje lične podatke i pod kojim uslovima. Tehnologija brzo menja prirodu i vrednost informacije, sa velikim količinama ličnih podataka koji se ubrzano generišu, prenose, dele i sakupljaju. Neophodno je da uprava bude transparentna i odgovorna u rukovanju ličnim podacima građana.

Pravno na privatnost i pravo na pristup informacijama – kao i sloboda izražavanja – su dva osnovna ljudska prava i moraju biti balansirana od slučaja do slučaja. Postoje slučajevi kada su ova prava u koliziji, kao na primer u slučaju obavezivanja na objavljivanje privatnih interesa političara. Ali, u većini slučajeva, „prava na informacije“ nisu suprotstavljena i zapravo međusobno jačaju jedno drugo. Rade u tandemu kako bi zadržala one koji drže moć odgovornim, uspostavljajući princip *pravo da zna*, uglavnom u smislu državne uprave, ali takođe i kada je u pitanju vrsta informacija koje državna uprava i druge relevantne institucije potencijalno drži ili koristi u donošenju odluka o građaninu/građanki (Banisar, 2011).

Napori u cilju transparenstnosti koji poštuju privatnost pokušaće da isprave asimetrije između onih koji drže moć i ostatka populacije, istovremeno umanjujući namete koji su neophodni da bi se moćni držali odgovornima. Privatnost ne treba koristiti kao izgovor za izbegavanje

odgovarajućeg nadzora.

Programi otvorene uprave i transparentnosti unose više informacija u javni prostor i mogu generisate negativne reakcije ukoliko se obični građani osećaju kao da su oni sami – a ne oni koji drže moć – ti koji su izloženi. Objavljivanje zdravstvenih kartona, poreskih prijava ili čak sudskih zapisnika su se pokazali problematičnim za privatnost pojedinca u različitim kontekstima. Tehnologije koje se koriste za odgovornost – kao što su, na primer, aplikacije i internet stranice koje prikupljaju prijave o korupciji – mogu imati ozbiljne implikacije po privatnost. Takve tehnologije uključuju prikupljanje i čuvanje velikog obima potencijalno osetljivih podataka i, kao takve, uvećavaju rizik identifikacije od strane trećih lica i nepredviđenog pristupa podacima od strane državne uprave (Open Rights Group, 2014).

Pravo na privatnost i zaštitu podataka odnose se na veliki broj državnih institucija, ali su takođe važna u regulisanju privatnog sektora, uključujući organizacije civilnog društva uključenim u programe razvoja.

Policija i službe bezbednosti su posebni slučajevi, jer njihova odgovornost uključuje i upad u privatnu sferu bez pristanka radi dostizanja javnih ciljeva kao što su krivično pravo i zaštita javne i nacionalne bezbednosti. Pitanja privatnosti odnose se na nadležnost za pretres i zaplenu, aktivnosti u nadzoru komunikacija i uspostavljanje DNK baze podataka. Poglavlje u okviru ovog vodiča koje se odnosi na Policiju i Sistem bezbednosti sadrže specifične preporuke.

Preporuke u ovom poglavlju nisu propisane, već su primeri koje treba prilagoditi lokalnim okolnostima u cilju jačanja postojeće zaštite.

Reference

Banisar,D.(2011)TheRighttoInformationandPrivacy:BalancingRightsandManagingConflicts,WashingtonDC:WorldBank.
http://wbi.worldbank.org/wbi/Data/wbi/wbicms/files/drupal-acquia/wbi/Right%20to%20Information%20and%20Privacy.pdf

Stručne organizacije

Privacy International http://https://www.privacyinternational.org/

Open Rights Group http://https://www.openrightsgroup.org/

ElectronicFrontierFoundationhttp://https://www.eff.org/

OECD http://www.oecd./sti/security-privacy

Global Privacy Enforcement Networkhttp://https://www.privacyenforcement.net

Pregled ilustrativnih obaveza

Početne

- Usvojiti propise koji se odnose na privatnost i zaštitu podataka
- Uspostaviti programe javnog obrazovanja koji se odnose na zaštitu ličnih podataka
- Uvesti vodiče za rukovanje ličnim podacima u programima otvorene uprave
- Objaviti zakone koji regulišu nadležnosti policije i obaveštajnih agencija u oblasti nadzora

Srednje

- Proceniti uticaj programa otvorene uprave na privatnost javnosti
- Objaviti izveštaje o transparentnosti koji se odnose na podatke o nadzoru, presretanju i pristupu komunikacijama
- Opozvati sve zahteve koji zahtevaju identifikaciju korisnika telefona i interneta

Napredne

- Uključiti „dizajniranu privatnost“ u programe otvorene uprave i transparentnosti
- Reformisati zakonodavstvo koje se tiče nadzora od strane državnih agencija u cilju obezbeđivanja da je ono u skladu sa ljudskim pravima

Inovativne

- Uspostaviti zaštitne mere kako bi se obezbedilo da nove tehnologije koje se koriste u nadzoru i presretanju poštuju pravo na privatnost
- Dati građanima kontrolu nad njihovim ličnim podacima i pravo na obeštećenje kada su ovi podaci zloupotrebljeni
- Objaviti detalje kompjuterskih algoritama koje koristi državna uprava

Detaljne preporuke

Početni koraci: Usvojiti propise koji se odnose na privatnost i zaštitu podataka

Obrazloženje

Zakon o zaštiti podataka je važan deo u očuvanju prava na privatnost, koje bi inače bilo lako preplavljeno silom državnih agencija i korporacija koje drže inforacije o pojedincima.

Zakonodavstvo u oblasti privatnosti i zaštite podataka je neophodno u kontekstu programa otvorene uprave u cilju pružanja garancija građanima. Sa porastom javnig angažmana, od građana se zahteva da imaju poverenje u svoje Vlade i povezane agencije sa svojim mišljenjima, vrednostima i uverenjima. Neobavezujući sporazumi nisu dovoljni, jer građani ne mogu zavisiti od dobre volje aktuelne vlasti kada je u pitanju njihova privatnost.

Kocept zaštite podataka podrazumeva da pojedicni u principu imaju pravo da odluče da li žele da daju svoje lične podatke i utvrde pod kojim su uslovima spremni da to učine. Zakoni o zaštiti podataka generalno uključuju mere za zaštitu bezbednosti ličnih podataka i omogućavaju drugima da ih koriste samo u okviru propisanih okolnosti. Više od 100 zemalja usvojile su, ili su u procesu usvajanja propisa o zaštiti podataka. Važno je da ovi zakoni pokrivaju kako javni tako i privatni sektor, obzirom da oba imaju sopstevne skupove rizika za privatnost za pojedince. Zakoni o zaštiti podataka jačaju transparentnost tako što omogućavaju građanima građanima da znaju koje informacije država uprava o njima ima.

Uz zaštitu individualne privatnosti, adekvatni zakoni o zaštiti podataka su i ekonomski imperativ za države da privuku investicije u industrijama koje se bave informacijama, kao što su međunarodni kol-centri, centri podataka; i uslugama obrade podataka.

Preporuke

1. Usvojiti zakone o privatnosti i zaštiti podataka koji regulišu lične podatke kako u privatnom tako i u javnom sektoru.
2. Uspostaviti organ za zaštitu podataka koji nadgleda usaglašenost sa propisima u oblasti zaštite podataka i posreduje u slučaju žalbi. Ukoliko organ postoji, osigurati da ima kapacitet za sprovođenje zakona o privatnosti.
3. Obezbediti edukativni materijal za informisanje građana i preduzeća o standardima zaštite podataka, njihovoj primeni i mogućnostima obeštećenja ukoliko dođe do njihovog kršenja.
4. Uvesti smislene kazne za kršenje privatnosti. Kazne bi trebalo da budu srazmerne prometu preduzeća kako bi se izbeglo da budu inkorporirane u cene.
5. Prijaviti se za akreditaciju u okviru režima zaštite podataka EU i uneti neophodne izmene u zakon.

Standardi & Smernice

- Council of Europe: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
- EuropeanUnion:EuropeanDataProtectionDirective1995http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri=CELEX:31995L0046&from=en
- OECD: Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata .htm

Primeri iz zemalja

Okvir zaštite podataka u Urugvaju akreditovan od strane EU za pružanje adekvatne zaštite

Evropska komisija je prepoznala da zakonodavni okvir Urugvaja pruža ‘adekvatnu zaštitu’ ličnih podataka u okviru Direktive EU o zaštiti podataka 95/46/EC. Ovo omogućava potpunu razmenu podataka sa EU bez potrebe za dodatnim garancijama. Kako bi postigao ovu distinkciju, Urugvaj je morao da dokaže nadležnim organima odgovarajuća usvajanja i usaglašnost sa propisima o zaštiti ličnih podataka.

Druge zemlje kojima je priznato pružanje ‘adekvatne’ zaštite podataka su Argentina, Andora, Kanada, Švajcarska, Farska Ostrva, Gernzi, Izrael, Ostrvo Men, Džerzi i Safe Harbor SAD.

Dominikanska Republika predana usvajanju zakona o zaštiti ličnih podataka u okviru svog OGP Akcionog plana

Akcioni plan za sprovođenje Akcionog plana za inicijativu Partnerstva za otvorenu upravu sadrži obavezu za stvaranje pravnoh okvira za zaštitu ličnih podataka, kako u javnoj, tako i u privatnoj sferi.

Početni korak: Uspostaviti programe javnog obrazovanja koji se odnose na zaštitu licnih podataka

Obrazloženje

Važan korak ka obezbeđivanju zaštite ličnih podataka pojedinaca je edukacija garađana o vrednosti tih podataka kao i razlozima zbog kojih bi oni trebalo da očekuju da takvi podaci budu zaštićeni. Pojedinci moraju da budu informisani o prirodi digitalnih tehnologija i internetu, tome na koji način kompanije prikupljaju i koriste podatke, kao i načinu na koji bi državna uprava mogla da pristupi tim podacima. Nove tehnologije zahtevaju nove veštine i svest o tome kako ostati bezbedan i zaštititi lične podatke (vidi Electronic Frontier Foundation, 2002). Ovo je posebno važno za legitimnost programa državne uprave koji povećavaju upotrebu ličnih podataka u procesu kreiranja politike i pružanja usluga. Osnaživanje pojedinaca u smislu ličnih podataka je u skladu sa Smernicama Organizacije za ekonomsku saradnju i razvoj o zaštiti privatnosti i prekograničnim tokovima ličnih podataka (Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980), koje naglašavaju učešće pojedinaca u zaštiti sopstvenih podataka o ličnosti.

Preporuke

1. Sprovesti javne kampanje o ličnim podacima, uključujući i aktuelne teme poput toga kako se oni mogu povezati sa drugim podacima i analizirati na načine koji mogu ugroziti pivatnost. Ovo bi trebalo prevesti na lokalne jezike i distribuirati putem odgovarajućih medija (npr. opštinski radio).
2. Obezbediti pojedincima jednostavne korake koje mogu da preduzmu u cilju zaštite svojih ličnih podataka, kako na internetu tako i drugde, kako bi se obezbedila proaktivna uloga građana u zaštiti njihovih ličnih podataka.
3. Uvesti privatnost i transparentnost zajedno u nastavni plan i program za škole.

Standardi&Smernice

- Council of Europe: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
- EuropeanUnion:EuropeanDataProtectionDirective1995http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri=CELEX:31995L0046&from=en
- OECD: Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

- United Nations: Guidelines for the regulation of computerized personal data files http://www.refworld.org/cgi- bin/texis/vtx/rwmain?docid=3ddcafaac

Primeri iz zemalja

Vlada Velike Britanije podržala internet stranicu sa savetime Ostani siguran onlajn (GetSafeOnline)

Get Safe Online nastao je 2005. godine kao zajedničko partnerstvo Vlade i industrije u cilju pružanja nepristrasnih, korisnički orijentisanih saveta o sigurnosti na internet za korisnike i manja preduzeća. Finansijski je podržan od strane Kabineta premijera i drugih vladinih tela. Agencija za organizovani criminal (SOCA) pruža ljudstvo za podršku godišnjoj "Get Safe Online" Nedelji koja obuhvata konferencije, medijske događaje i radionice.

Služba Poverenika za informacije Velike Britanije objavila pamflet o zaštiti ličnih podataka

Služba Poverenika za informacije Velike Britanije – nezavisni organ uspostavljen sa ciljem promocije pristupa informacijama i zaštite ličnih podataka u VB – objavila je pamflet o zaštiti ličnih podataka. On sadrži savete o zaštiti, pristupu i ispravljanju ličnih podataka, kao i informacije o tome kako smanjiti neželjene poruke, mejlove, itd. i kako uočiti krađu i prevaru.

Početni korak: Uvesti vodiče za rukovanje ličnim podacima u programima otvorene uprave

Obrazloženje

Državni programi povećanja transparentnosti i odgovornosti moraju razmotriti pitanje privatnosti u ranoj fazi razvoja, a ne tek na tački pružanja usluge. Pitanja privatnosti mogu prouzrokovati negativne reakcije, kao što je to bio slučaj sa objavljivanjem zdravstvenih podataka u Velikoj Britaniji. Planovi obezbeđivanja boljeg nadzora rezultata putem objavljivanja više podataka doveli su zabrinutosti da bi se mogla narušiti privatnost pacijenata.

U većini slučajeva, lični podaci se ne bi trebalo objavljivati uopšte, a svakako ne u vidu otvorenih podataka. Kada se lični podaci objavljuju u interesu javnosti, potencijalne negativne posledice treba svesti na minimum. Na primer, lične podatke ne treba učiniti dostupnim u marketinške svrhe putem objavljivanja podataka o subvencijama i porezima, ili objavljivanje registara i sudskih dokumenata. Minimizacija podataka (identifikacija i čuvanje samo minimalnog obima ličnih podataka potrebnih za određenu svrhu) i druge praktične mere , kao što su kontrola pristupa ličnim podacima putem registracije, može pomoći u kontroli rizika od zloupotrebe.

Druga potencijalna kolizija je objavljivanje podataka o rezultatima iz javnih službi – škola, bolnica, beneficija, itd. – u svrhu odgovornosti. Ova vrsta podataka se obično „anonimizuje“, ali postoji rasuća zabrinutost o riziku od re-identifikacije pojedinaca kominacijom različitih izvora podataka. Transparentnost i odgovornost bu trebalo da budu iznad objavljivanja ovakvih podataka sa zbirnom statistikom, umesto pojedinačnih nivoa podataka, kao uvek bolja opcija prvatnosti.

Podacima prikupljenim kroz programe učešća javnosti mora se rukovati sa posebnom pažnjom. U ekstremnim slučajevima mogući su ozbiljni rizici odmazde, kao što je to u slučaju prijavljivanja korupcije. U nekim slučajevima, rizici upravljanja informacijama neće biti strogo vezani za lične podatke. Na primer, objavljivanje lokacije prirodnih resursa ili zaštićenih vrsta može imati negativan uticaj na celu zajednicu.

Preporuke

1. Objaviti smernice za objavljivanje ličnih podataka u javnim registrima, uključujući minimizaciju podataka i kontrolu pristupa u skladu sa potrebama.
2. Objaviti smernice i ponuditi podršku za uključivanje privatnosti i odgovornog rukovanja podacima u kreiranju programa otvorene uprave.
3. Objaviti smernice za objavljivanje ličnih podataka o zaposlenima u javnom sektoru, npr. kriterijum staža.
4. Objaviti smernice za razmenu ličnih podataka sa privatnim preduzetnicima. Podatke bi trebalo minimizovati do nivoa koji je potreban za svrhu ugovora. Ugovarne strane koje pružaju uslugu treba da budu podvrgnute istim kontrolama kao i državni organi.

5. Koristiti sertifikate Instituta Otvoreni podaci (Open Data Institute) u objavljivanju otvorenih podataka. U bazama podataka koje sadrže lične podatke, isti bi trebalo da uključuju i pravni osnov za njihovo objavljivanje, opcije za de-identifikaciju, itd.

Standardi i Smernice

- EuropeanCommission–Article29WorkingParty:Opinion05/2014onAnonymisationTechniques http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf
- Open Data Institute: Open Data Certificates http://https://certificates.theodi.org/about

---

Početni korak: Objaviti zakone koji regulišu nadležnosti policije i obaveštajnih agencija u oblasti nadzora

Obrazloženje

Mnoge zemlje se još uvek oslanjaju na zakone o tajnosti i poverljiva tumačenja tajnih sudova za vršenje nadzora, dok u drugim zemljama ovakve aktivnosti nisu u potpunosti regulisane. Administracije pravnog sistema i zaštite nacionalne bezbednosti u demokratskim zemljama zahteva transparentan i otvoren pravni sistem koji detaljno uređuje nadležnosti i odgovornosti javnih službi bezbednosti, uključujući i obaveštajne agencije. Gde bezbednosne službe i obaveštajne agencije imaju nadležnost za vršenje nadzora u cilju postizanja bezbednosti i policijske svrhe, ove nadležnosti moraju biti jasno definisane na način koji omogućava pojedincima da predvide njihovu primenu i nadziru njihovu upotrebu.

Osnovni princip međunarodnih ljudskih prava je da mešanje u pravo na privatnost mora biti neophodno, proporcijalno i u skladu sa zakonom. Evropski sud za ljudska prava naglasio je da, da bi nadzor bio „u skladu sa zakonom“, zakoni moraju dati građanima dovoljno detalja o sledećim aspektima:

- Prirodi prekršaja koji mogu dovesti do nadzora;
- Kategorija osoba koje mogu biti podložne nadzoru;
- Ograničenje trajanja nadzora;
- Procedure koje se moraju slediti za ispitivanje, korišćenje i čuvanje prikupljenih podataka;
- Mere predostrožnosti koje treba preduzeti u razmeni podataka sa drugim strankama; i
- Okolnosti u kojima podaci moraju biti izbrisani ili trake uništane.

Preporuke

1. Objaviti sve zakone i propise koji uređuju ovlašćenja u nadzoru bezbednosnih službi i obaveštajnih agencija i usvojiti takve zakone ukoliko oni ne postoje. Ovo bi trebalo da obuhvati interna pravila i procedure, iako bi interna pravila trebalo minimizirati gde god je to moguće. Propisi koji uređuju nadzor bi trebalo prevesti u zakone kako bi se osiguralo da su predmet dovoljnog nadzora.
2. Obezbediti da su zakoni i propisi koji uređuju ovlašćenja u nadzoru dovoljno jasni u obimu i detaljima da zadovolje potrebe u smislu predvidljivosti i pristupa neophodnog u skladu sa vladavinom prava. Obezbediti objavjivanje istih uz dovoljno propratne dokumentacije i napomena kako bi građani razumeli šta to znači u praksi.
3. Edukovati građane o mehanizmima nadzora koji istražuju i prate usaglašenost bezbednosnih i obaveštajnih agencija sa zakonima i propisima koji se odnose na ovlašćenja u nadzoru. Pružiti informacije o sredstvima za obeštećenje za građane koji smatraju da su agencije prekršile zakone koji se odnose na nadzor.

Standardi i Smernice

- International Principles on the Application of Human Rights to Communications Surveillance http://https://en.necessaryandproportionate.org/text
- UN High Commissioner for Human Rights: The Right to Privacy in the Digital Age http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
- United Nations: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expressionhttp://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement

Srednji korak: Proceniti uticaj programa otvorene uprave na privatnost javnosti

Obrazloženje

Procena uticaja na privatnost (Privacy Impact Assessment – PIA) je formalna analiza o tome na kojie se način lični podaci prikupljaju, koriste, razmenjuju i održavaju. PIA omogućava odgovornost pokazujući da je privatnost inkorporirana u kreiranje određeno programa. Ovo omogućava rano uočavanje i ublažavanje rizika. PIA omogućava organizacijama jasniju komunikaciju sa javnošću o njihovom odgovornom upravljanju ličnim podacima i kako oni rešavaju pitanja koja se tiču privatnosti.

Preporuke

1. Zahtevati PIA za sve programe e-uprave i otvorene uprave. Zahtevati da PIA budu objavljene, uz tehničke napomene o tome kako podaci mogu da budu obrađeni, kao na primer u procesu de-identifikacije. Treća lica koja su prožaoci usluga treba da budu obuhvaćeni PIA i da se takođe obavežu na odgovornost.
2. Pružiti smernice i tome kako sprovesti PIA (vidi, na primer, Kodeks prakse UK)

Primeri iz zemalja

Procene uticaja na privatnost su pravni zahtev za programe e-Uprave u Sjedinjenim Američkim Državama

U SAD, PIA su potrebne u skladu sa članom 208 Zakona o e-Upravi iz 2002. godine, koji uređuje rukovođenje i promociju saveznih elektronskih državnih servisa i procesa. Zakon definiše potrebne najviše komponente PIA, oključujući i to na koji će način informacije biti obezbeđene.

Srednji korak: Objaviti izveštaje o transparentnosti koji se odnose na podatke o nadzoru, presretanju i pristupu komunikacijama

Obrazloženje

Tranparentnost u smislu upotrebe ovlašćenja nadzora je ključni način da se obezbedi da su službe bezbednosti i obaveštajne agencije pod kontrolom i da privatnost pojedinca nije narušena van strogih zakonskih granica.

Transparentnost dozvoljava građanioma da nadziru državnu upravu, obezbede da ona ne prelazi svoja ovlašćenja i da znaju kada je ravnoteža između zaštite bezbednosti i narušavanja ljudskih prava otišla previše u korist policije i službi javne bezbednosti.

Poslednjih godina, sve veći broj internet i telekomunikacionihprovajdera uveli su objavljivanje izveštaja o transparentnosti, koji detaljno navode broj zahteva koji su primili od državne uprave za pristup podacima o komunikaciji pojedinaca, kao i broj zahteva koje su primili za uklanjanje informacija iz svojih usluga. Primeri uključuju:

- Facebook Global Government Requests Report- https://www.facebook.com/about/government_requests
- Google Transparency Report-http://www.google.com/transparencyreport/
- Microsoft Law Enforcement Requests Report -https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
- Twitter Transparency Report https://transparency.twitter.com/
- Vodafone Law Enforcement DisclosureReport - http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

Vlade bi trebalo da uvedu sličnu praksu. Objavljivanjem izveštaja o transparentnosti o broju zahteva koje su podneli internet i telekomunikacionim provajderima, kao i broj naloga odobrenih bezbednosnim i obaveštajim službama za različite vrste nadzora na internetu ili druge, državna uprava može da obezbedi da je nadzor koji vrši pod lupom javnosti na način koji garantuje odgovornost.

Preporuke

1. Usvojiti zakone koji obavezuju bezbednosne i obaveštajne službe da objavljuju godišnje podatke o broju zahteva koji su podneti i odobreni od strane privatnog sektora za pristup podacima o korporativnoj komunikaciji i o broju zahteva koji su podneti i odobreni od strane sudova ili drugih nadzornih mehanizama za odobrenje za sprovođenje nadzora na internetu ili drugde.
2. Obezbediti objavljivanje izveštaja o transparentnosti na lak i pristupačan način koji je takođe i konzistentan, kompjuterski čitljiv i otvoreno licenciran za ponovnu upotrebu.

Standardi&Smernice

- Global Network Initiative: Principles on Freedom of Expression and Privacy
  http://https://globalnetworkinitiative.org/sites/default/files/GNI - Principles 1 .pdf

Primeri iz zemalja

Poverenik za presretanje komunikacija Velike Britanije objavljuje ograničene godišnje statistike

Poverenikova uloga uključuje razmatranje naloga za presretanje za nadzor u stvarnom vremenu (istorijski poznato kao "prisluškivanje") i garancije koje se tiču upotrebe informacija. On godišnje izveštava premijera o tome da li se institucije u okviru njegove nadležnosti pridržavaju zakona Poverenikov godišnji izveštaj obuhvata naloge izdate za MI5, policiju, Specijalno odeljenje i druge državne organe, ali ne i Ministarstvo spoljnih poslova ili organe za prikupljanje obaveštajnih podataka širom sveta poput Vladinog Štaba za komunikacije (GCHQ). Izveštaj pruža samo opšte zbirne podatke, a iako je obim podataka uvećan poslednjih godina, organizacije koje se bave ljudskim pravima tvrde da je i dalje neadekvatan za značajniji nadzor, preispitivanje i odgovornost u oblasti presretanja i nadzora.

http://www.iocco-uk.info/

http://www.statewatch.org/analyses/no-244-gchq-intercept-commissioner.pdf

SAD objavljuje godišnje Izveštaje o prisluškivanju

Sudovi SAD izdaju godišnji Izveštaj o prosliškivanju (Wiretap report) o upotrebi nadzornih ovlašćenja od strane službi bezbednosti. Godišnji izveštaj pruža sveobuhvatne podatke o svim saveznim I državnim aplikacijama za prisluškivanje, uključujući vrstu zločina koji se istražuje, kao I povezane troškove I da li e to rezultiralo hapšenjima ili presudama. Ne uključuju imena, adrese ili brojeve telefona subjekata pod nadzorom. Međutim, godišnji izveštaj Suda za spoljni obaveštajni nadzor (Foreign Intelligence Surveillance Court) pruža mnogo manje informacija.

Srednji korak: Opozvati sve zahteve koji zahtevaju identifikaciju korisnika telefona i interneta

Obrazloženje

Jedna od glavnih karakteristika interneta je mogućnost anonimnog pristupa i širenja informacija, kao i bezbednog komuniciranja bez potrebe za identifikacijom. U početku, ovo je bilo moguće zbog nepostojanja „sloja identiteta“ ugrađenog u internet. Međutim, u ime bezbednosti i sprovođenja zakona, Vlade širom sveta sve više ograničavaju mogućnosti anonimne komunikacije. Na primer, u nekim zemljama pojedinci moraju da se identifikuju u internet kafeima i pristanu na beleženje svojih transakcija na javnim kompjuterima. U drugim slučajevima, identifikacija i registracija su takođe potrebne za kupovinu SIM kartica i mobilnih telefona, za posete određenim velikim internet stranicama, ili za ostavljanje komentara na medijskim internet stranicama ili blogovima (Donovan and Martin, 2014).Ovde je potrebna jasna razlika između privatnih kompanija koje potrežuju podatke u komercijalne svrhe i obavezne identifikacije tražene od strane državne uprave.

Ograničenja u anonimnosti omogućavaju državni nadzor komunikacija tako što je lakše identifikovati pojedince koji pristupaju ili šire zabranjene sadržaje, čineći tako ove pojedince podložnijim drugim oblicima nadzora. Prema tome, ograničenja u anonimnosti odvraćaju od slobodnog izražavanja informacija i ideja i mogu u praksi da dovedu do onemogućavanja ljudima da pristupe vitalnim društvenim sferama, podrivajući njihovo pravo na izražavanje i pristup informacijama i jačajući društvene razlike. Ovo obhvata mnoge projekte otvorene uprave koji se oslanjanju na mobilne tehnologije koje daju građanima glas ili platformu za delovanje. Osim toga, ograničenja u anonimnosti omogućavaju da veliki obim prikupljih i razvrstavanih podataka od strane privatnog sektora postane lično identifikacioni. Ovo može dovesti do značajnog opterećenja i odgovornosti korporativnih aktera u zaštiti privatnosti i bezbednosti takvih podataka. Alternativno, može ih podstaći i da podatke monetizuju, rizikujući tako dalje narušavanje privatnosti.

Preporuke

1. Opozvati sve zakone koji zahtevaju korišćenje pravih imena ili potvrdu identiteta na internet forumima, društvenim medijima i drugim internet prostorima.
2. Ukloniti zahteve da se pojedinci identifikuju pri korišćenju internet kafea ili javnih kompjutera.
3. Programi uključenja otvorene uprave mogu povremeno zahtevati identifikaciju učesnika, ali samo nakon što je jasan slučaj utvrđen.

Standardi i Smernice

- GSMA:TheMandatoryRegistrationofPrepaidSIMCardUsers–AWhitePaperhttp://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf
- United Nations: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expressionhttp://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement

Napredni korak: Ukljuciti „dizajniranu privatnost“ u programe otvorene uprave i transparentnosti

Obrazloženje

Dizajnirana privatnost promoviše poštovanje privatnosti i zaštite podataka od momenta kada je projekat zamišljen. Ovaj pristup ne služi kao zamena za bilo kakve propise, ali će pomoći organizacije u pridržavanju svojim obavezama u skladu sa lokalnim zakonima.

Preporuke

Uključiti sedam principa *Dizajnirane privatnosti* u programe otvorene uprave:

1. Proaktivno ne Reaktvino; Preventivno ne Popravno: Predvideti i sprečiti događaje koji narušavaju privatnost pre nego što se dese.

2. Privatnost kao standardna postavka: Obezbeđivanje maksimalnog stepena privatnosti osiguravanjem da su lični podaci automatski zaštićeni u okviru bilo kog IKT sistema ili poslovne prakse. Podešavanja o privatnosti se ugrađuju u sistem kao standardna postavka, tako da nije potrebna nikakva akcija od strane pojedinca kako bi zaštitio/la svoju privatnost.

3. Privatnost ugrađena u dizajn: Privatnost ne treba da se dodaje kasnije, već da bude ugrađena u osnovnu funkcionalnost.

4. Puna funkcionalnost: Prilagoditi se svim legitimnim interesima i ciljevima u pozitivnom opštem ishodu – za opšte dobro („win-win“ manner), a ne kroz stari pristup nultog zbira (zero-sum approach) gde se prave nepotrebni kompromisi. Dizajnirana privatnost izbegava pretpostavku lažnih podela, kao što su privatnost protiv ezbednosti, pokazujući da je moguće imati oba.

5. Zaštita celog životnog ciklusa: Proširiti privatnost na ceo životni ciklus podataka, od početka do kraja. Ovo obezbeđuje sigurno i blagovremeno uništavanje svih podataka na kraju procesa.

6. Vidljivost i transparentnost: Osigurati sve zainteresovane strane da poslovna praksa ili tehnologija funkcioniše u skladu sa navedenim obećanjima i ciljevimai da je predmet nezavisne provere. Sastavni delovi i operacije treba da ostanu idljive i transparentne, kako korisnicima, tako i provajderima.

7. Poštovanje privatnosti korisnika – Iznad svega: Dizajnirana privatnost zahteva od arhitekata i operatera da zadrže interes individualca/ke iznad svegapružajući mere kao što su jaka standardna podešavanja privatnosti, odgovarajuća obaveštenja i osnaživanje korisnički orijentisanih opcija.

Standardi i Smernice

- GSMA: Privacy Design Guidelines for Mobile Application Development http://www.gsma.com/publicpolicy/privacy- design-guidelines-for-mobile-application-development
- PrivacybyDesign:7FoundationalPrinciples http://www.privacybydesign.ca/index.php/about-pbd/7-foundational- principles/

> **Napredni korak:** Reformisati zakonodavstvo koje se tiče nadzora od strane državnih agencija u cilju obezbeđivanja da je ono u skladu sa ljudskim pravima

Obrazloženje

Kako tehnologije koje omogućavaju nadzor komunikacija napreduju, a ovlašćenja obaveštajnih agencija se šire, Vlade moraju osigurati da zakoni i propisi koji se tiču nadzora komunikacija budu u skladu sa međunarodnim ljudskim pravima i da adekvatno štite prava na privatnost i slobodnu izražavanja. Potrebno je da postoji ažurirano razumevanje kako se međunarodni standardi ljudskih prava primenjuju u savremenom digitalnom okruženju, posebno u svetlu porasta i izmena u tehnologijama i tehnikama nadzora komunikacija.

Vrlo koristan alat za procenu usklađenosti su Međunarodni principi o primeni ljudskih prava u nadzoru komunikacija (International Principles on the Application of Human Rights to Communications Surveillance). Oni su razvijeni kako bi pružili Vladama okvir za procenu da lisu trenutni ili predloženi zakoni i praksa nadzora u skladu sa ljudskim pravima. Principi su ishod globalnih konsultacija sa organizacijama civilnog društva, industrijom i međunarodnim stručnjacima za zakon o nadzoru komunikacija, politike i tehnologiju. Ovi principi predstavljaju svetski standard za balansiranje potrebe za tajnošću u vezi nadzora za zahtevima za odgovornošću sadržanim u otvorenoj upravi. Ovo je jedan od najvećih problema za kreatore politike, koji zahteva stvaranje istinski odgovornih država kao hitni prioritet. Greška u uspostavljanju ovog balansa može da podrije samu osnovu demokratiju, slabljenjem osnovnih prava.

Preporuke

1. Temeljno preispitati sve zakone i propise koji se tiču ovlašćenja za nadzor bezbednosnih službi i obaveštajnih agencija kako bi se identifikovali slučajevi gde su propisi u koliziji, ili su nepotpuni, u odnosu na standarde formulisane u Međunarodnim principima.
2. Izmeniti zakonodavstvo u cilju obezbeđivanja usklađenosti sa Međunarodnim principima.

Standardi i Smernice

- International Principles on the Application of Human Rights to Communications Surveillance http://https://en.necessaryandproportionate.org/text

Inovativni korak: Uspostaviti zaštitne mere kako bi se obezbedilo da nove tehnologije koje se koriste u nadzoru i presretanju poštuju pravo na privatnost

Obrazloženje

Službe bezbednosti i obaveštajne agencije sakupljaju, čuvaju, ili imaju pristup značajnoj količini informacija – neke od njih su privatne prirode o žrtvama, svedocima, zločinima i osumnjičenima – i mnoge su poverljive. Ove informacije moraju biti prikupljene legalno i korišćene samo do nivoa koji je neophodan i propocionalan za sprovođenje zakona, i moraju biti zaštićene od zloupotreba od strane kriminalaca, novinara ili privatnih detektiva, ili upotrebu od strane politički motivisanih državnih snaga.

Tehnološki razvoj menja prirodu ovih informacija. Ljudi sada prenose velike količine digitalnih podataka o sebi i ostavljaju tragove metapodacima o ome gde se nalaze, svojim kontaktima, kao i svojim transakcijama. Drugi podaci se mogu prikupiti jeftinije, digitalizovati i analizirati. RFID tagovi omogućavaju praćenje pojedinih proizvoda, DNK se može sekvencirati, dok softveri za prepoznavanje lica i registarskih tablica omogućavaju analizu podataka (data mining) prikupljenih kamerama za nadzor (CCTV). Posebno ili zajedno ovi podaci se mogu koristiti za otkrivanje identiteta osobe, ponašanja, fizičkog ili zdravstvenog stanja, rase, boje, seksualne orijentacije, nacionalnog porekla ili stavova; ili omogućavaju mapiranje lokacije, pokreta ili interakcija osobe tokom vremena.

Ove tehnologije mogu imati važnu ulogu u sprečavanju i otkrivanju kriminala i omogućavanju pravde. Uz to, korišćene su i za podršku odgovornijoj policiji, na primer, postoje rani obećavajući dokazi u pilot programima za policijske službenike koji koriste telesne kamere, da je ova praksa ohrabrila zakonitu i dostojanstvenu interakciju i umanjila upotrebu sile.

Ipak, sve ove tehnologije takođe izazivaju zabrinutost za privatnost. Sveobuhvatno ili sistemsko praćenje ima kapacitet za otkrivanje privatnih informacija u obimu koji značajno prevazilazi pojedinačne delove, ostavljajući tako primenu pravnih principa na nove tehnologije neadekvatnom i nejasnom. Kako razvoj novih tehnologija dalje napreduje, neophodno je da su zakoni i propisi u skladu sa međunarodnim ljudskim pravima i da na adekvatan način štite pravo na privatnost i slobodu izražavanja. Evropski sud za ljudska prava priznao je da samo prikupljanje i čuvanje ličnih podataka, uključujući DNK i fotografije, od strane službi bezbednosti, može da preraste u kršenje prava na privatnost. Ovo se odnosi čak i na slučajeve kada su podaci javno dostupni i sistemski prikupljeni i sačuvani u policijskim dosijeima (Segerstedt-Wiberg protivŠvedske (2007) 44 EHHR 2; i Marper protivVelike Britanije (2009) 48 EHRR 50).

Preporuke

Sledeće preporuke zasnivaju se na „Međunarodnim principima“ i na princip 10E„Tsvane principa“ (Tshwane Principles). Zemlje bi trebalo da:

1. Objavljuju dovoljno informacija kako bi pojedinci mogli u potpunosti razumeti obim, prirodu i primenu zakona koji dozvoljavaju nadzor komunikacija.
2. Odobre pružaocima usluga komunikacija da objavljuju procedure koje primenjuju u radu sa nadzorom, pridržavaju se tih procedura i objavljuju evidencije o državnom nadzoru komunikacija.
3. Objave, u najmanju ruku, zbirne informacije o broju odobrenih i odbijenih zahteva za nadzor koumnikacija, kao i podelu ovih zahteva prema pružaocu usluga i prema vrsti i svrsi istrage.
4. Uspostave nezavisni nadzorni mehanizam kako bi se obezbedila transparentnost i odgovornost u nadzoru. Nadzorni mehanizmi treba da imaju ovlašćenje da pristupe svim potencijalno relevantnim podacima o nadzoru, procene da li je on sproveden legalno i da li je država transparentno i tačno objavljivala informacije o upotrebi i obimu tehnika i ovlašćenja u nadzoru komunikacija. Nezavisni nadzorni mehanizam treba da objavljuje periodične izveštaje o svojim nalazima.

Za službe bezbednosti, operativne posledice ovoga su uključuju potrebu za:

1. Razmatranjem mera informacione bezbednosti u svetlu novih tehnologije i tehnika kako bi se obezbedila njihova robusnost.
2. Uključivanjem novih ili proširenih tehnika u okvir nadzora pravosuđa ili drugih demokratskih nadzornih mehanizama radi utvrđivanja da li spada u domen usklađenosti sa ustavnim garancijama i međunarodnim standardima ludskih prava.

> **Inovativni korak:** Dati građanima kontrolu nad njihovim ličnim podacima i pravo na obeštećenje kada su ovi podaci zloupotrebljeni

Obrazloženje

Preduzeća i državna uprava sve više prikupljaju i analiziraju velike količine ličnih podataka o svojim klijentima i korisnicima usluga. Davanje šireg pristupa ljudima elektronskim registrima o njihovom kreditnom rejtingu, prethodnim kupovinama i potrošnji, omogućava im da donose bolje odluke o kupovini. Na primer, podaci koje telefonska kompanija ima o Vašoj upotrebi mobilnog telefona, može pomoći u odabiru nove tarife.

Od ključne je važnosti da su korisnici svesni podataka koje daju preduzećima, kao i potencijalnih upotreba tih podataka. Oni moraju imati kontrolu nad sopstvenim ličnim podacima i uspostavljene mehanizme kako bi se sprečilo da preduzeće obriše ili zameni netačne ili osetljive podatke iz svojih registara; omogućavajući im da zabrane prikupljanje ličnih podataka ukoliko ne žele da ih dele.

U mnogim zemljama nedostatak poverenja kako u Vladu tako i u privatne institucije za rukovanje ličnim podacima je u porastu. Ovo je razvilo interesovanje u tehnologije koje dozvoljavaju korisnicima kontrolu na svojim podacima. U VB postoje Servisi za rukovanje ličnim podacima, kao što su Mydex, društveno preduzeće koje pruža korisnicima platformu za prikupljanje, organizaciju preuzimanje kontrole nad njihovim ličnim podacima. Ova kompanija je sertifikovana kao provajder digitalnog identiteta za e-Upravu od strane državne uprave VB.

Lični prostor na internetu (cloud) drži lične podatke bezbednim i omogućava razmenu podataka pod izabranim uslovima; takođe omogućava i izbor aplikacije za rad na podacima. Respect Network je grupa cloud provajdera koja omogućava korisnicima da bilo gde u svetu dele osetljive lične podatke preko pouzdane privatne mreže/konekcije.

U mnogim programima otvorene uprave građanima bi se mogla dati kontrola nad njihovim podacima korišćenjem ovih vrsta tehnologija. Ovo ne bi samo izazvalo poverenje, već bi i dalo građanima podeljenu odgovornost i vlasništvo nad programima. Zaštite ličnih podataka je važna u svim državnim programima, od socijalne politike, zdravstva, obrazovanja, do tehnologija otvorene uprave za odgovornost. Davanje kontrole građanima nad njihovim podacima ne uklanja potrebu za zdravom politikom i praksom u oblasti privatnosti. Davanje kontrole korisnicima ez prethodne edukacije o privatnosti naročito može otvoriti put za njih da budu eksploatisani od strane beskrupuloznih pojedinaca ili organizacija.

Preporuke

1. Identifikovati ključne sektore za objavljivanje ličnih podataka. Raditi sa regulatorima sektora, poverenicima za informacije i potrošačkim grupama radi identifikovanja sektora kao što su bankarstvo, mobilna telefonija i energetika, kao prioritetnih za elektronsko slanje ličnih podataka korisnicima elektronski za privatni sektor;
2. Raditi sa kompanijama na razvijanju sistema koji omogućava korisnicima da bezbedno pristupe svojim podacima;
3. Ohrabriti preduzeća da razviju aplikacije koje će pomoći korisnicima u efikasnijem korišćenju njihovih podataka;
4. Usvojiti i sprovesti zakone koji korisnicima pružaju adekvatne mehanizme za rukovanje vrstom, obimom i upotrebom ličnih podataka od strane preduzeća;
5. Razmotriti propise koji obavezuju kompanije da daju podatke korisnicima;
6. U inicijativama otvorene uprave sprovesti tehnička rešenja za kontrolu ličnih podataka, kao što su skladišta podataka, upravljanje vezom sa isporučiocem, privatni cloud-ovi.

Inovativni korak: Objaviti detalje kompjuterskih algoritama koje koristi državna uprava

Obrazloženje

Kako interakcija između građana i državnih institucija i usluga postaje sve više digitalna, postoji potencijal za nove vrste „algoritamskih propisa“. Na primer, prepoznavanje registarskih tablica na vozilima se već koristi za naplatu putarine. Prikupljanje podataka sa GPS sistem u vozilima može omogućiti automatsko izdavanje kazni za vozače koji prekorače ograničenje brzine, ili im pomoći da nađu parking mesta, dok će razvoj samo-vozećih vozila i integracija javnog prevoda, kontrole saobraćaja i usluge pametne podele saobraćaja zahtevati sakupljanje i razmenu dodatnih podataka.[1]

Ovakva nova digitalna regulative nosi rizike po privatnost. Kada su podaci jednom prikupljeni u određenu svrhu, lako je smisliti nove upotrebe za njih, a kombinovanje podataka iz različitih izvora može otkriti i više nego što je potrebno. Na primer, praćenje brzine tokom vožnje takođe znači i praćenje naše lokacije. Ako se kompjuterski algoritmi koriste za ocenu, profil, odluku ili imaju bilo kakav uticaj na građane, oni moraju biti podvrgnuti istom javnom nadzoru i odgovornosti kao bilo koja druga komponenta otvorene uprave.

To znači da algoritmi moraju biti javni.[2]

Tek smo na početku revolucije podataka i mere za zaštitu privatnosti se moraju razvijati paralelno.

Preporuke

1. Informisati javnost o upotrebi algoritamskih propisa i sprovesti konsultacije o pitanjima privatnosti i dizajna.
2. Razviti algoritamske propise sa jasno definisanim ciljevima i gde god je to moguće kreirati mere kvaliteta u realnom remenu za praćenje i poboljšanje performansi ka ovim ciljevima i izbeći „zastoje u misiji“ u korišćenju podataka.
3. Usvojiti principe „dizajnirane privatnosti“ pri razvoju algoritamskih propisa, odbacujući ili anonimizujući podatke koji nisu potrebni za ispunjenje ciljeva.
4. Eksplicitno uključiti algoritme u okviru delokruga zakona o pristupu informacijama, idealno uspostaviti i propis o proaktivnom objavljivanju svih javnih algoritamskih propisa i njihov cilj.
5. Razviti metode za korisnu transparentnost tako da se relevantni aspekti algoritma mogu predstaviti na razumljiv način i lednostavnim jezikom, možda i sa više nivoa detalja.
6. Osigurati da su podaci korišćeni za donošenje odluka podložni reviziji i, kada god je to moguće, otvoreni za javni nadzor.
7. Preiodično sprovesti i objaviti dublju analizu o tome da li su sami algoritmi tačni i da li rade kao što je očekivano.