

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Povzetek mnenja Evropskega nadzornika za varstvo podatkov o spletni manipulaciji in osebnih podatkih

(Celotno besedilo tega mnenja je na voljo v angleščini, francoščini in nemščini na spletišču Evropskega nadzornika za varstvo podatkov (v nadaljnjem besedilu: ENVP) www.edps.europa.eu)

(2018/C 233/06)

Digitalizacija družbe in gospodarstva ima mešan vpliv na državljansko udejstvovanje pri sprejemanju odločitev in na ovire pri vključevanju javnosti v demokratične procese.

Analitika masovnih podatkov in sistemi umetne inteligence omogočajo zbiranje, združevanje, analiziranje in stalno shrambo ogromnih količin podatkov. V zadnjih dveh desetletjih se je za večino spletnih storitev vzpostavil prevladujoč poslovni model, ki temelji na sledenju ljudem na spletu in zbiranju podatkov o njihovem značaju, zdravju, razmerjih ter mislih in mnenjih, da bi se ustvarjali prihodki iz digitalnega oglaševanja. Ti digitalni trgi so se skoncentrirali okrog nekaj podjetij, ki delujejo kot učinkoviti vratarji svetovnega spleta in katerih tržna vrednost, prilagojena za inflacijo, je višja od vrednosti katerih koli drugih podjetij v zgodovini.

Ta digitalni ekosistem je povezal ljudi po vsem svetu, saj svetovni splet uporablja 50 % prebivalstva, pri tem pa je mogoče opaziti zelo neenakomerno geografsko, zdravstveno in spolno zastopanost. Po začetnem optimizmu glede potenciala, ki ga imajo spletna orodja in družbeni mediji pri državljanskem udejstvovanju, se je pojavila zaskrbljenost, da se z ljudmi manipulira, in to tako s stalnim zajemanjem pogosto zaupnih informacij o njih kot z nadzorom informacij, ki jih glede na to, v katero kategorijo so umeščeni, vidijo na spletu. Viralno ogorčenje je ključno gonilo vrednosti za veliko storitev na podlagi algoritmov, pri čemer so nekateri proizvodi in aplikacije zasnovani tako, da kar najbolj pritegnejo pozornost in povečujejo zasvojenost. Povezanost je, vsaj po sedanjem modelu, vodila v nesoglasja.

Razprava, ki je sledila, se je vrtela okrog zavajajočih, napačnih ali klevetniških informacij (vsebin), prikazanih ljudem, da bi vplivale na politični diskurz in volitve – ta pojav je bil imenovan lažne novice ali spletne dezinformacije. Rešitve so bile usmerjene v ukrepe za preglednost, ki so izpostavili vir informacij, hkrati pa zapostavili odgovornost akterjev v ekosistemu, ki s škodljivim ravnanjem kujejo dobiček. Medtem koncentracija na trgu in vzpon prevladujočih platform ustvarjata novo grožnjo medijskemu pluralizmu. Po mnenju ENVP ta kriza zaupanja v digitalni ekosistem ponazarja soodvisnost zasebnosti in svobode izražanja. Zaupen prostor, ki je na voljo ljudem, se je kot posledica neizogibnega nadzora podjetij in vlad zmanjšal, kar negativno vpliva na sposobnost in pripravljenost ljudi, da bi se izražali in neovirano navezovali stike tudi v civilni sferi, ki je zelo pomembna za trdno demokracijo. Zato to mnenje obravnava način, kako se uporabljajo osebni podatki, s katerimi se izvaja mikrociljanje posameznikov in skupin s specifično vsebino, zadevne temeljne pravice in vrednote ter ustrezne zakone za blažitev s tem povezanih groženj.

ENVP se že več let zavzema za tesnejše sodelovanje med organi za varstvo podatkov in drugimi regulativnimi organi, da bi se zaščitile pravice in interesi posameznikov v digitalni družbi, zaradi česar je leta 2017 vzpostavil digitalno klirinško hišo. Glede na zaskrbljenost, da politične kampanje morda izrabljajo digitalni prostor, da bi se izognile veljavni zakonodaji ⁽¹⁾, verjamemo, da je zdaj čas, da se to sodelovanje razširi tudi na volilne in avdiovizualne regulativne organe.

1. ZAKAJ OBJAVLJAMO TO MNENJE

(i) Intenzivna potekajoča javna razprava

Trenutno poteka intenzivna javna razprava o učinku današnjega obširnega in kompleksnega ekosistema digitalnih informacij ne le na tržno gospodarstvo, ampak tudi na politično ekonomijo, na to, kako politično okolje vpliva na gospodarstvo. Glavne platforme so v središču tega ekosistema, s čimer nesorazmerno pridobivajo zaradi rasti digitalnega oglaševanja, in z njegovim razvojem povečujejo svojo sorazmerno moč. Osebni podatki so potrebni za razčlenjevanje, ciljanje in prilagajanje sporočil, prikazanih posameznikom, vendar se večina oglaševalcev ne zaveda, kako se take odločitve sprejmejo, in večina posameznikov se ne zaveda, kako se uporabljajo. Sistem nagrajuje senzacionalistično in viralno

⁽¹⁾ Glej na primer <http://www.independent.co.uk/news/uk/politics/election-2017-facebook-ads-marginal-seats-tories-labour-outdated-election-spending-rules-a7733131.html> (dostop 18.3.2018).

vsebinsko ter na splošno ne razlikuje med oglaševalci, bodisi komercialnimi ali političnimi. Razkritja o tem, kako so se namerne dezinformacije (lažne novice) razširjale po tem sistemu, so privedla do bojazni, da je integriteta demokracij morda v nevarnosti. Gonilo sistemov umetne inteligence – katerih trg tudi zaznamuje koncentracija – so podatki in če ti ne bodo preverjeni, bodo okrepili oddaljevanje in nesprejemanje odgovornosti pri sprejemanju odločitev v tem okolju.

(ii) Pomembnost zakonodaje o varstvu podatkov in političnih kampanj

Temeljne pravice do zasebnosti in varstva podatkov so pri izboljšanju tega stanja nedvomno ključni dejavnik, zaradi česar je to vprašanje strateška prednostna naloga za vse neodvisne organe za varstvo podatkov. Regulativni organi za varstvo podatkov so v svoji *Resolution on the Use of Personal Data for Political Communication* (resoluciji o uporabi osebnih podatkov v politični komunikaciji) iz leta 2005 izrazili poglobitve pomisleke z vsega sveta v zvezi z varstvom podatkov, povezane z obsežnejšo obdelavo osebnih podatkov, ki jo izvajajo nekomercialni akterji. Nanašala se je zlasti na obdelavo občutljivih podatkov, povezanih z resničnimi ali domnevnimi moralnimi in političnimi prepričanji ali dejavnostmi ali z glasovalnimi dejavnostmi in napadalno oblikovanje profilov različnih ljudi, ki so trenutno razvrščeni – včasih netočno ali na podlagi površnega stika – kot simpatizerji, podporniki, privrženci ali strankarski (¹). V mednarodni resoluciji so pozvali k strožjemu izvrševanju predpisov o varstvu podatkov glede zmanjšanja količine podatkov, zakonite obdelave, privolitve, preglednosti, pravic posameznikov, na katere se nanašajo osebni podatki, omejitve namena in varnosti podatkov. Zdaj je morda čas, da se ta poziv obnovi.

Zakonodaja EU o varstvu podatkov in zaupnosti elektronskih komunikacij se nanaša na zbiranje podatkov, oblikovanje profilov in mikrociljanje in če bi se ustrezno izvrševala, bi morala zmanjšati škodo, nastalo zaradi poskusov manipulacije posameznikov in skupin. Obdelava podatkov o volivcih, ki jo izvajajo politične stranke, v EU spada na področje uporabe Splošne uredbe o varstvu podatkov. V Splošni uredbi o varstvu podatkov so osebni podatki, ki razkrivajo politična mnenja, opredeljeni kot posebna vrsta podatkov. Obdelava takih podatkov je na splošno prepovedana, razen kadar velja katera od naštetih izjem. V kontekstu političnih kampanj sta posebej relevantni naslednji dve izjemi, ki ju je vredno navesti v celoti:

- „(d) obdelavo v okviru svojih zakonitih dejavnosti z ustreznimi zaščitnimi ukrepi izvaja ustanova, združenje ali katero koli drugo neprofitno telo s političnim, filozofskim, verskim ali sindikalnim ciljem in pod pogojem, da se obdelava nanaša samo na člane ali nekdanje člane telesa ali na osebe, ki so v rednem stiku z njim v zvezi z njegovimi nameni, ter da se osebni podatki ne posredujejo zunaj tega telesa brez privolitve posameznikov, na katere se nanašajo osebni podatki;
- (e) obdelava je povezana z osebnimi podatki, ki jih posameznik, na katerega se nanašajo osebni podatki, sam objavi [...];
- (g) obdelava je potrebna iz razlogov bistvenega javnega interesa na podlagi prava Unije ali prava države članice, ki je sorazmerno z zastavljenim ciljem, spoštuje bistvo pravice do varstva podatkov ter zagotavlja ustrezne in posebne ukrepe za zaščito temeljnih pravic in interesov posameznika, na katerega se nanašajo osebni podatki.“

Izjava 56 pojasnjuje člen 9(2)(g): „[k]adar med volilnimi dejavnostmi delovanje demokratičnega sistema v državi članici zahteva, da politične stranke zberejo osebne podatke o političnih mnenjih ljudi, se lahko obdelava takih podatkov dovoli iz razlogov javnega interesa, če so vzpostavljeni ustrezni zaščitni ukrepi.“

Več organov za varstvo podatkov je razvilo pravila ali smernice o obdelavi podatkov v politične namene:

- marca 2014 je italijanski organ za varstvo podatkov sprejel pravila o obdelavi osebnih podatkov, ki jo izvajajo politične stranke. Pravila so poudarila splošno prepoved uporabe osebnih podatkov, objavljenih na svetovnem spletu, na primer na družbenih omrežjih ali forumih, za namene političnega komuniciranja, če so bili ti podatki zbrani za druge namene (²),
- novembra 2016 je francoska državna komisija za varstvo podatkov (CNIL) predpisala dodatne smernice k svojim priporočilom o političnem komuniciranju iz leta 2012, pri čemer je določila pravila za obdelavo osebnih podatkov na družbenih omrežjih. Komisija je poudarila predvsem, da je zbiranje podatkov o volivcih zaradi oblikovanja profilov in ciljanja na družbenih omrežjih lahko zakonito samo, če temelji na privolitvi, ki je podlaga za obdelavo podatkov (³),

(¹) Resolucija je na voljo na spletnem naslovu: <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Political-Communication.pdf> (dostop 18.3.2018).

(²) <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267>, „Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale“, v uradnem listu številka 71 dne 26. marca 2014 objavil italijanski organ za varstvo podatkov (splet. št. dok. 3013267).

(³) <https://www.cnil.fr/fr/communication-politique-queles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux-sociaux?>, 8. novembra 2016 objavila Commission Nationale de l'informatique et des libertés (francoska državna komisija za informatiko in pravice).

- aprila 2017 je urad informacijskega pooblaščenca Združenega kraljestva (ICO) izdal posodobljene smernice *Guidance on political campaigning* (smernice o političnih kampanjah), ki so vključevale tudi smernice o uporabi analitike podatkov v političnih kampanjah. Urad informacijskega pooblaščenca je razložil, da ko politična organizacija za izvedbo analitike pooblasti tretjo družbo, potem je ta družba verjetno obdelovalec podatkov, organizacija pa upravljavec. Da bi bila obdelava zakonita, je treba upoštevati specifične določbe zakona o varstvu podatkov, ki urejajo razmerje med upravljavcem in obdelovalcem ⁽¹⁾.

Smernice nacionalnih organov za varstvo podatkov bi lahko zagotovile dodatno zanesljivo tolmačenje določb o varstvu podatkov in zakonodaji o zasebnosti, ki upoštevajo razlike pri organizaciji nacionalnih političnih sistemov ⁽²⁾.

(iii) Namen tega mnenja ENVP

Vizija ENVP je pomagati EU, da v globalnem dialogu o varstvu podatkov in zasebnosti v digitalni dobi daje zgled, tako da prepozna interdisciplinarne politične rešitve za izzive na področju masovnih podatkov in razvija etično razsežnost obdelave osebnih podatkov ⁽³⁾. ENVP je pozval, naj se posameznika, na katerega se nanašajo osebni podatki, obravnava „kot posameznika, ne pa le kot potrošnika ali uporabnika“, in poudarili etična vprašanja v zvezi z napovednim oblikovanjem profilov in individualnim prilagajanjem na podlagi algoritmov ⁽⁴⁾. Pozval je tudi k odgovornemu in trajnostnemu razvoju digitalne družbe, ki temelji na nadzoru posameznika nad osebnimi podatki o njem, inženiringu, ki upošteva vidik zasebnosti, ter sprejemanju odgovornosti in skladnem izvrševanju ⁽⁵⁾. Svetovalna skupina za etiko pri ENVP je v poročilu iz januarja 2018 ugotovila, da „mikrociljanje volilnega agitiranja spreminja pravila javnega govora, s čimer zmanjšuje prostor za razpravo in izmenjavo idej“, zato je „nujno potrebna demokratična razprava o uporabi in izkoriščanju podatkov za politične kampanje in odločanje“ ⁽⁶⁾.

To vprašanje uporabe informacij in osebnih podatkov z namenom manipulacije ljudi in politike seveda močno presega pravico do varstva podatkov. Posamezniku prilagojeno in mikrociljano spletno okolje ustvarja filtrirne mehurčke, zaradi česar so ljudje izpostavljeni približno enakim informacijam in naletijo na manj mnenj, kar povzroča večjo politično in ideološko polarizacijo ⁽⁷⁾. To krepi prodornost in prepričljivost lažnih zgodb in zarot ⁽⁸⁾. Raziskave kažejo, da bi manipulacija virov novic ali rezultatov iskanja lahko vplivala na volilno vedenje ljudi ⁽⁹⁾.

ENVP se zavzema za to, da je obdelava osebnih podatkov, kot je navedeno v Splošni uredbi o varstvu podatkov, koristna za ljudi, ne pa obratno ⁽¹⁰⁾. Tehnološki napredek se ne sme ovirati, temveč ga je treba usmerjati v skladu z našimi vrednotami. Spoštovanje temeljnih pravic, vključno s pravico do varstva podatkov, je odločilno za zagotovitev poštenih

⁽¹⁾ https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf, urad informacijskega pooblaščenca, „Guidance on political campaigning“ (20170426).

⁽²⁾ V skladu s členom 57(1)(d) GDPR vsak nadzorni organ na svojem ozemlju „spodbuja ozaveščenost upravljavcev in obdelovalcev glede njihovih obveznosti na podlagi te uredbe“.

⁽³⁾ Glej Zgledno delovanje: Strategija ENVP za obdobje 2015–2019, str. 17 Masovni podatki se po našem mnenju nanašajo na prakso združevanja velikih količin podatkov iz različnih virov in njihovo analizo, pri čemer se pogosto uporabljajo algoritmi samostojnega učenja za informirane odločitve. Ena od največjih vrednosti masovnih podatkov za podjetja in vlade pa izhaja iz spremljanja vedenja ljudi, kolektivno in individualno, in temelji na njegovi predvidljivi zmogljivosti, mnenje Evropskega nadzornika za varstvo podatkov št. 4/2015 z naslovom Novi digitalni etiki naproti: podatki, dostojanstvo in tehnologija, 11.9.2015, str. 6.

⁽⁴⁾ Profili, ki se uporabljajo za napovedovanje vedenja ljudi, so pod pritiskom tveganja stigmatizacije, krepitve obstoječih stereotipov, družbenega in kulturnega razlikovanja in izključevanja, tovrstna kolektivna inteligenca pa ogroža posamezno izbiro in enake možnosti. Taki filtrirni mehurčki ali osebne zaprte celice lahko na koncu ovirajo ustvarjalnost, inovativnost ter pravici do izražanja ter zbiranja in združevanja, ki so omogočile, da so digitalne tehnologije zaživele, mnenje Evropskega nadzornika za varstvo podatkov št. 4/2015, str. 13 (viri niso vključeni).

⁽⁵⁾ Mnenje Evropskega nadzornika za varstvo podatkov št. 7/2015 z naslovom Soočanje z izzivi masovnih podatkov, str. 9.

⁽⁶⁾ Poročilo svetovalne skupine za etiko pri Evropskem nadzorniku za varstvo podatkov, januar 2018, str. 28.

⁽⁷⁾ Glej na primer *The Economist*, How the World Was Trolled (4. november 2017), vol. 425, št. 9065, str. 21–24.

⁽⁸⁾ Allcott, H., in Gentzkow, M., Social Media and Fake News in the 2016 Election (pomlad 2017). Stanford University, *Journal of Economic Perspectives*, vol. 31, št. 2, str. 211–236. <https://web.stanford.edu/~gentzkow/research/fakenews.pdf>, str. 219.

⁽⁹⁾ V enem poskusu so uporabnike družbenih platform seznanili, kaj so povedali njihovi prijatelji glede tega, kako so volili, kar je povzročilo, da je statistično pomembno večji segment prebivalstva (0,14 % prebivalstva z volilno pravico ali približno 340 000 volivcev) odšel na vmesne volitve za kongres leta 2010; Allcott, H., in Gentzkow M., Social Media and Fake News in the 2016 Election (pomlad 2017), Stanford University, *Journal of Economic Perspectives*, vol. 31, št. 2, str. 211–236, str. 219. V drugi študiji so raziskovalci trdili, da razlike pri rezultatih Googlevega iskanja lahko spremenijo glasovalne izbire neodločenih volivcev za 20 %; Zuiderveen Borgesius, F., Trilling, D., Möller, J., Bodó, B., de Vreese, C., in Helberger, N. (2016). Should we worry about filter bubbles?. (Nas morajo filtrirni mehurčki skrbeti?) *internet Policy Review*, 5(1). DOI: 10.14763/2016.1.401, str. 9.

⁽¹⁰⁾ Uvodna izjava 4 iz Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljnjem besedilu: Splošna uredba o varstvu podatkov).

volitev, zlasti ko se približujemo volitvam za Evropski parlament, ki bodo leta 2019 ⁽¹⁾. To mnenje je zadnje v vrsti obsežnejših aktivnosti ENVP v zvezi z vprašanjem, kako je treba izvajati varstvo podatkov, da se obravnavajo najbolj pereči pomisleki v javni politiki. Temelji na dosedanjem delu ENVP v zvezi z masovnimi podatki in digitalno etiko ter potrebo po uskladitvi zakonske ureditve o konkurenčnih in poštenih trgih ⁽²⁾. V mnenju bo najprej povzet proces, pri katerem osebni podatki spodbujajo in določajo prevladujoč cikel digitalnega sledenja, mikrociljanja in manipulacije. Nato bodo obravnavane vloge različnih akterjev v ekosistemu digitalnih informacij. Obravnavani bodo zadevne temeljne pravice, ustrezna načela varstva podatkov in druge ustrezne pravne obveznosti. Končalo se bo s priporočilom, da se bo težava spletne manipulacije najverjetneje le še poslabšala, da posamezni regulativni pristopi sami po sebi ne bodo zadostni in da morajo regulativni organi zato nujno sodelovati, da bi se spopadli ne le z lokaliziranimi zlorabami, ampak tudi s strukturnimi izkrivljanji, ki jih povzročata prevelika koncentracija na trgu.

7. SKLEPNA UGOTOVITEV

Spletna manipulacija ogroža družbo, saj se zaradi filtrirnih mehurčkov in zaprtih skupnosti ljudje težje razumejo med sabo in delijo svoje izkušnje. Oslabitev tega družbenega lepila bi lahko omajalo demokracijo ter druge temeljne pravice in svoboščine. Spletna manipulacija je tudi simptom nejasnosti in neprevzemanja odgovornosti v digitalnem ekosistemu. Težava je resnična in pereča ter bo verjetno postala še hujša s tem, ko bo več ljudi in stvari povezanih s svetovnim spletom in bo vloga sistemov umetne inteligence narasla. Srž težave je deloma neodgovorna, nezakonita in neetična uporaba osebnih podatkov. Preglednost je potrebna, vendar ni dovolj. Upravljanje vsebine je morda potrebno, vendar se ne sme dovoliti, da bi ogrozilo temeljne pravice. Del rešitve je torej dosledno izvrševanje veljavnih predpisov, zlasti Splošne uredbe o varstvu podatkov, skupaj z drugimi normativnimi predpisi o volitvah in medijskem pluralizmu.

Ker želi ENVP prispevati k pospeševanju razprave, bo spomladi leta 2019 sklical delavnico, na kateri bodo nacionalni regulativni organi s področja varstva podatkov ter volilne in avdiovizualne zakonodaje lahko podrobneje proučili te interakcije, razpravljali o izzivih, s katerimi se spoprijemajo, in obravnavali možnosti za skupne ukrepe, tudi ob upoštevanju prihodnjih volitev za Evropski parlament.

V tem mnenju so podane utemeljitve o tem, da tehnologija in vedenje na trgu povzročata škodo zaradi strukturnih neravnovesij in izkrivljanj. ENVP je pozval k prilagoditvi spodbud za uvajanje inovacij. Tehnološki velikani in pionirji so do zdaj uživali koristi delovanja v razmeroma nenadzorovanem okolju. Prizadete so tradicionalne panoge in osnovni koncepti krajevne pristojnosti in suverenosti ter tudi družbene norme, vključno z demokracijo. Te vrednote so odvisne od pluralnosti glasov in ravnovesja med strankami. En sam akter ali sektor se s tem ne more spopasti. Varstvo podatkov je del rešitve in to morda večji, kot bi pričakovali. Ni dovolj, da se zanašamo na dobro voljo komercialnih akterjev, ki se na koncu izkažejo za neodgovorne. Zdaj moramo ukrepati, da se na bolj pošten način razširijo koristi digitalizacije.

V Bruslju, 19. marca 2018

Giovanni BUTTARELLI

Evropski nadzornik za varstvo podatkov

⁽¹⁾ Kot je navedlo Evropsko sodišče za človekove pravice v primeru Orlovskaya Iskra proti Rusiji, „svobodne volitve in svoboda izražanja, zlasti svoboda politične razprave, skupaj tvorijo temeljni kamen vsakega demokratičnega sistema. Obe pravici sta vzajemno povezani in delujeta tako, da druga drugo utrjujeta: svoboda izražanja je na primer eden od pogojev, potrebnih za svobodno izražanje mnenja ljudstva pri izbiri zakonodajnega telesa. Zaradi tega je v obdobju pred volitvami še posebej pomembno, da se dovoli svobodno širjenje vseh vrst mnenj in informacij. V kontekstu volilnih soočenj je neovirano uveljavljanje svobode govora kandidatov še posebej pomembno“ (viri niso vključeni v besedilo), odstavek 110. <http://hudoc.echr.coe.int/eng?i=001-171525>.

⁽²⁾ 2014: predhodno mnenje o zasebnosti in konkurenčnosti v dobi velikih podatkov, 2015: Mnenje št. 4/2015 z naslovom Novi digitalni etiki naproti: podatki, dostojanstvo in tehnologija, 2015: Mnenje št. 7/2015 z naslovom Soočenje z izzivi masovnih podatkov. Poziv za preglednost, nadzor uporabnikov, vgrajeno varstvo podatkov in odgovornost, 2016: Mnenje ENVP št. 8/2016 o učinkovitem izvrševanju temeljnih pravic v dobi masovnih podatkov.