



Bruselj, 12.9.2018
COM(2018) 637 final

**SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU
EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ**

Zagotavljanje svobodnih in poštenih evropskih volitev

*Prispevek Evropske komisije k srečanju voditeljev v
Salzburgu 19. in 20. septembra 2018*

Zagotavljanje svobodnih in poštenih evropskih volitev

Ključni trenutek za prihodnost Evropske unije

Bistvo Evropske unije je njena obramba demokracije in demokratičnih vrednot. Te so nujne za družbo, v kateri prevladujeta pluralizem in strpnost, evropski državljani pa lahko volijo z gotovostjo, da niso zavedeni. Demokracija je skupaj s pravno državo in temeljnimi pravicami del „tega, kdo smo“, in opredeljuje našo Unijo.

Volitve v Evropski parlament maja 2019 bodo potekale v zelo drugačnem okviru kot vse prejšnje volitve. Politični izzivi Unije in njenih držav članic so veliki. Jasno je, da je treba oblikovati trdnejšo Unijo, ki bo lahko na svetovnem prizorišču, na katerem se za oblast potegujejo svetovne sile, ki nimajo nujno enakih interesov ali vrednot kot mi, delovala verodostojno in močno. Močna Unija, ki temelji na učinkovitem pravosodnem sodelovanju, izmenjavi informacij za boj proti terorizmu in organiziranemu kriminalu ter dobro delujočem notranjem trgu, zahteva zaupanje med državami članicami in v naše demokratične sisteme. V tem edinstvenem okviru bodo evropske volitve maja 2019 oblikovale prihodnost Evropske unije v naslednjih letih.

Zagotavljanje odpornosti demokratičnih sistemov Unije je del varnostne unije, saj so napadi na volilno infrastrukturo in informacijske sisteme kampanj hibridne grožnje, ki jih mora obravnavati Unija. Politično motivirane množične spletne dezinformacijske kampanje, vključno s tistimi, ki jih izvajajo tretje države, in katerih cilj je predvsem diskreditirati volitve ter jim odvzeti legitimnost, so bile priznane kot vse večja grožnja našim demokracijam¹. Evropska unija mora sprejeti vse ukrepe v okviru svojih pooblastil, da obrani svoje demokratične procese pred manipulacijami tretjih držav ali zasebnimi interesi. Izkazalo se je, da so volilna obdobja še posebej izpostavljena ciljno usmerjenim dezinformacijam. Ti napadi ogrožajo integriteto in poštenost volilnega procesa ter zaupanje državljanov v izvoljene predstavnike in tako ustvarjajo pomisleke glede same demokracije.

Evropski državljani bi morali imeti možnost voliti s popolnim razumevanjem političnih izbir, ki so jim na voljo. To pomeni boljšo ozaveščenost glede groženj in več preglednosti v našem političnem procesu. Odprta javna sfera, varovana pred pretiranim vplivom, zagotavlja enake konkurenčne pogoje za politične kampanje in volilne procese, ki jim javnost lahko zaupa². Bistveno je, da naše demokracije zagotovijo prostor za živahno politično kampanjo, ki volivcem jasno ter neizkrivljeno prikaže zamisli in programe strank, ki se potegujejo za njihov glas. Zato se je treba aktivno boriti proti goljufijam in drugim namernim poskusom manipuliranja z volitvami, med drugim tudi s sankcijami.

¹ Glej Skupno sporočilo Evropskemu parlamentu, Evropskemu svetu in Svetu z naslovom Povečanje odpornosti in krepitev zmogljivosti za obravnavanje hibridnih groženj, JOIN(2018) 16 final, in sklepe Evropskega sveta z dne 28. junija 2018 (<http://www.consilium.europa.eu/sl/press/press-releases/2018/06/29/20180628-euco-conclusions-final/pdf>).

² Beneška komisija Sveta Evrope daje smernice glede volitev ([http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2002\)023rev-e](http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev-e)), tudi glede medijskega okolja ([http://www.venice.coe.int/webforms/documents/?pdf=CDL-PI\(2016\)006-e](http://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2016)006-e)).

Spletne dejavnosti, vključno s tistimi med volilnimi procesi, se hitro razvijajo, zato so ključni večja varnost in enaki konkurenčni pogoji na političnem prizorišču. Konvencionalni (nespletni) volilni zaščitni ukrepi, kot so pravila, ki veljajo za politično komunikacijo v volilnih obdobjih, preglednost in omejitve izdatkov za volitve, spoštovanje volilnega molka in enako obravnavanje kandidatov, bi se morali prav tako uporabljati na spletu³. Preglednost uporabe političnih oglasov na televiziji ali panojih, njeno omejevanje in transparentnost teh oglasov bi podobno morali veljati tudi v spletnem svetu. Trenutno ni tako, zato je to treba pred naslednjimi evropskimi volitvami popraviti.

Novi izzivi in trenutni razvoj dogodkov

Čeprav je spletna komunikacija zmanjšala ovire in stroške za politične akterje pri stikih z državljanji ter ponuja velike priložnosti, je enako povečala možnosti zlonamernih akterjev, da napadejo demokratično razpravo in volilne procese. Spletno okolje akterjem omogoča, da lažje prikažejo informacije in pri tem prikrijejo njihov izvor ali namen, tudi tako, da ne razkrijejo, da je sporočilo (na primer objava v družbenih medijih) plačan oglas, in ne poročanje dejstev, da mnenje podajo, kot da gre za novinarstvo, in da poročajo izbirno, da bi prilili olja na ogenj ali polarizirali razpravo. Pri tem se nihče ne bi smel vdajati iluzijam glede teh groženj, saj Evropska unija in njeni politični sistemi niso nedovzetni za take grožnje.

Poleg tega lahko integriteto volitev resno prizadenejo „konvencionalni“ kibernetški incidenti, vključno s kibernetškimi napadi, katerih tarča so volilni procesi, kampanje, infrastruktura političnih strank, kandidati ali sistemi javnih organov, in zloraba osebnih podatkov. Nedavna razkritja, vključno s tistimi v zadevi „Facebook/Cambridge Analytica“, so tipičen primer tega. Osební podatki naj bi bili zlorabljeni in nezakonito dani tretjim osebam za uporabo, ki se zelo razlikuje od prvotno predvidene. To je poudarilo morebitna tveganja, da bi se nekatere spletne dejavnosti uporabljale za prikrito naslavljanje državljanov s političnimi oglasi in drugimi objavami, ter tveganja nezakonite obdelave in zlorabe osebnih podatkov državljanov za manipulacijo mnenj, širjenje dezinformacij ali zgolj spodkopavanje resnice, kadar to ustreza političnim namenom ali povečuje razkol⁴.

³ Glej nedavno publikacijo Sveta Evrope *Internet and electoral campaigns – Study on the use of internet in electoral campaigns* (Internet in volilne kampanje: študija uporabe interneta v volilnih kampanjah), ki jo je pripravil odbor strokovnjakov Sveta Evrope za pluralnost medijev in preglednost lastništva medijev (MSI-MED) (<https://www.coe.int/en/web/human-rights-rule-of-law/-/internet-and-electoral-campaigns-a-new-study-has-been-published>). Študija preučuje posledice premika volilnega oglaševanja na internet, zlasti glede izdatkov za volitve in tehnik oglaševanja, ki temeljijo na izjemno natančnem ciljnem usmerjanju na volivce z individualiziranimi sporočili. Glej tudi Priporočilo Sveta Evrope CM/Rec(2016)5 o svobodi interneta, ki se nanaša na odgovornost držav, platform in posrednikov glede političnih kampanj, ki jih politične stranke, kandidati in drugi posamezniki izvajajo po spletu.

⁴ Glej vmesno poročilo, ki ga je objavil organ Združenega kraljestva za varstvo podatkov (ICO) po začetku uradne preiskave o uporabi podatkovne analitike za politične namene, potem ko so se pojavili očitki o nezakoniti obdelavi podatkov in izjemno natančnem ciljnem usmerjanju s političnimi oglasi med referendumom o EU (<https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf>). Poročilo poudarja, da „hiter družbeni in tehnološki razvoj na področju uporabe velepodatkov pomeni, da sta poznavanje in preglednost tehnik obdelave podatkov „v ozadju“ (vključno z algoritmi, analizo, primerjanjem podatkov in oblikovanjem profilov), ki jih organizacije in podjetja uporabljajo za izjemno natančno ciljno usmerjanje na posameznike, omejena. Jasno pa je, da lahko ta orodja znatno vplivajo na zasebnost ljudi. Pomembno je, da je preglednost glede uporabe takih tehnik večja in pristna, s čimer se zagotavlja, da imajo ljudje nadzor nad svojimi podatki in da se zakoni spoštujejo. Če je namen uporabe teh tehnik povezan z demokratičnim

Podpiranje svobodnih in poštenih volitev v Evropi

Evropske institucije ne skrbijo za potek volitev. Za ukrepe v tem okviru so v prvi vrsti odgovorne države članice. Te so odgovorne za organizacijo volitev in spremljanje izvajanja volilnega procesa⁵. Kljub temu pa obstaja očitna razsežnost, ki zadeva Unijo. V evropskih volilnih kampanjah so glavni akterji nacionalne in regionalne politične stranke, ki predlagajo kandidate za volitve v Evropski parlament. Evropske politične stranke in z njimi povezane fundacije imajo pomembno vlogo pri organiziranju dopolnilnih kampanj na evropski ravni, vključno s kampanjami za vodilne kandidate za mesto predsednika Evropske komisije.

Komisija se je po volitvah v Evropski parlament leta 2014 v povabilnem poročilu iz leta 2015⁶ zavezala, da bo opredelila načine za dodatno okrepitev evropske razsežnosti in demokratične legitimnosti postopka odločanja na ravni EU ter nadalje preučila in obravnavala razloge za stalno nizko volilno udeležbo v nekaterih državah članicah. Komisija je februarja 2018 pozvala k zgodnjemu in stalnemu sodelovanju z državljani v razpravah o evropskih vprašanjih, zgodnejšemu začetku kampanj političnih strank za volitve v Evropski parlament, vključno s kampanjami njihovih kandidatov za predsednika Evropske komisije, večji preglednosti povezav med nacionalnimi in evropskimi političnimi strankami ter k temu, da bi države članice spodbujale volilno pravico, zlasti pri slabše zastopanih skupinah.

Evropska unija je že sprejela nekatere pomembne ukrepe za vzpostavitev demokratične odpornosti v Evropi, vključno z novim evropskim okvirom za varstvo podatkov, ki se uporablja od maja letos. Splošna uredba o varstvu podatkov, ki se je začela neposredno uporabljati v vsej Evropski uniji, zagotavlja orodja, potrebna za obravnavanje primerov nezakonite uporabe osebnih podatkov v okviru volitev. Potekajo tudi prizadevanja za spodbujanje varnejšega spletnega okolja s povečanjem splošne odpornosti proti kibernetским grožnjam, vključno s spletnimi dezinformacijami in manipulacijo vedenja.

Pomembno je, da je kar se da jasno, kako izvajati evropska pravila o varstvu podatkov v tem novem okviru, hkrati pa moramo okrepiti svoja prizadevanja za izboljšanje ozaveščenosti, preglednosti in varnosti. Državljeni bi morali biti sposobni prepoznati, kdo jih po spletu nagovarja z oglasnimi in političnimi sporočili in kdo plačuje za politične oglase ali politična sporočila. Smernice o izvajanju novih pravil o varstvu podatkov v okviru evropskih volitev bi morale prispevati k večji jasnosti in boljšemu razumevanju, saj večje sodelovanje in izmenjava informacij med pristojnimi organi ter z drugimi prispevata k večji varnosti.

Sveženj za okrepitev demokratične odpornosti, predstavljen skupaj s tem sporočilom, zajema uravnotežene, celovite in ciljno usmerjene ukrepe za podporo integritete in učinkovite izvedbe volitev v Evropski parlament leta 2019. To je skupna odgovornost vseh akterjev, udeleženih v

procesom, so razlogi za visoke standarde preglednosti toliko bolj upravičeni. "Poudarjen je tudi pomen boljšega vključevanja vidikov varstva podatkov v širši regulativni okvir, ki ureja volitve.

⁵ V okviru zakonodaje EU in svojih mednarodnih obveznosti.

⁶ Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij z naslovom Poročilo o volitvah v Evropski parlament leta 2014 (COM(2015) 206 final).

volilnem procesu. Zahteva stalen nadzor in prožno prilagajanje dinamičnemu okolju ter novemu tehnološkemu razvoju. Z zagotovljenimi smernicami, priporočili in potrebnimi orodji lahko evropske in nacionalne politične stranke, nacionalne vlade, organi, zasebni subjekti in zainteresirane strani jasneje sodelujejo pri ustvarjanju varnejšega demokratičnega okolja in v enakih konkurenčnih pogojih.

Države članice se poleg tega spodbuja, naj načela uporabljajo tudi pri drugih volitvah in referendumih, ki jih organizirajo na nacionalni ravni.

Cilji ukrepov, predlaganih v tem svežnju, so:

1. zagotoviti posebne smernice glede obdelave osebnih podatkov na volitvah;
2. priporočiti dobre prakse obravnavanja tveganj, povezanih z dezinformacijami in kibernetскими napadi, ter spodbuditi spletno preglednost in odgovornost v volilnem procesu EU; okrepiti sodelovanje med pristojnimi organi in zagotoviti orodja, ki jim bodo omogočila, da posredujejo in po potrebi uvedejo sankcije, da se zavaruje integriteta volilnega procesa.
3. obravnavati primere, v katerih imajo politične stranke ali z njimi povezane fundacije koristi od praks, s katerimi se kršijo pravila o varstvu podatkov, da bi se namerno vplivalo ali poskušalo vplivati na izid evropskih volitev.

Pri predstavitvi tega svežnja je Komisija poskrbela, da ne bi prišlo do nepotrebnih upravnih bremen in neprimerne omejevanja manevrskega prostora za evropske, regionalne in nacionalne politične stranke ter fundacije.

1. Trenutni obrambni mehanizmi EU, s katerimi se zagotavlja varstvo svobodnih in poštenih volitev

Unija je že sprejela pomembne ukrepe za varstvo integritete volitev in krepitev demokratičnega procesa.

S Splošno uredbo o varstvu podatkov⁷, ki se od 25. maja 2018 neposredno uporablja v vsej Uniji, je Evropska unija zdaj v celoti opremljena za pomoč pri preprečevanju in reševanju primerov nezakonite uporabe osebnih podatkov. Kot taka je Evropska unija oblikovalka standardov na tem področju.

Poleg tega je bil pred kratkim spremenjen akt o volitvah poslancev Evropskega parlamenta, med drugim zaradi zagotovitve dodatne preglednosti v evropskem volilnem procesu⁸.

⁷ Uredba (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 (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

⁸ Sklep Sveta (EU, Euratom) 2018/994 z dne 13. julija 2018 o spremembi Akta o volitvah članov Evropskega parlamenta s splošnimi neposrednimi volitvami, ki je priložen Sklepu Sveta 76/787/ESPJ, EGS, Euratom z dne 20. septembra 1976 (<https://eur-lex.europa.eu/legal-content/sl/TXT/?uri=CELEX:32018D0994&qid=1531826494620>).

Revidirana uredba o statutu in financiranju evropskih političnih strank⁹, sprejeta 3. maja 2018, povečuje priznavanje, učinkovitost, preglednost in odgovornost evropskih političnih strank in evropskih političnih fundacij. Priporočilo Komisije (EU) 2018/234¹⁰ poudarja ključne korake za nadaljnjo krepitve učinkovite izvedbe volitev v Evropski parlament leta 2019.

Direktiva 2002/58/ES Evropskega parlamenta in Sveta (Direktiva o zasebnosti in elektronskih komunikacijah¹¹) se nanaša na nepovabljen sporočila za neposredno trženje, vključno s političnimi sporočili, ki jih podajo politične stranke in drugi akterji, udeleženi v volilnem procesu. Poleg tega zagotavlja zaupnost in zaščito informacij, shranjenih v terminalski opremi uporabnika, kot je pametni telefon ali računalnik¹². Predlagana uredba o zasebnosti in elektronskih komunikacijah¹³, o kateri trenutno potekajo pogajanja, bo s povečanjem preglednosti dodatno okrepila nadzor državljanov in razširila obseg varstva, ki bo poleg tradicionalnih telekomunikacijskih operaterjev vključevalo tudi internetne elektronske komunikacijske storitve.

Poleg tega je Komisija pred kratkim v svojem sporočilu z dne 26. aprila 2018¹⁴ predložila evropski pristop k boju proti dezinformacijam na spletu. S tem sporočilom želi spodbujati preglednejše, verodostojnejše in odgovornejše spletno okolje. Eden njegovih ključnih končnih rezultatov je razvoj ambicioznega **kodeksa ravnanja glede dezinformacij**, ki bi spletne platforme in oglaševalsko industrijo zlasti moral zavezati k zagotavljanju preglednosti in omejitvi možnosti ciljnega usmerjanja političnega oglaševanja¹⁵. Kodeks naj bi bil objavljen septembra 2018¹⁶, do oktobra pa naj bi dosegel merljive rezultate.

Podpisniki kodeksa ravnanja bi se morali zlasti dogovoriti, da „sleparska“ spletna mesta in spletna mesta, ki gostijo dezinformacije, prikrajšajo za prihodke od oglaševanja, zagotovijo preglednost glede sponzorirane vsebine, še posebej političnega in tematskega oglaševanja, ter vzpostavijo jasne sisteme in pravila označevanja za bote¹⁷, da se poskrbi, da njihovih dejavnosti ni mogoče zamenjati za človeške interakcije, in da se okrepijo prizadevanja za zaprtje lažnih računov. Podpisniki bi se prav tako morali dogovoriti, da bodo s spodbujanjem

⁹ Uredba (EU, Euratom) št. 1141/2014 Evropskega parlamenta in Sveta z dne 22. oktobra 2014 o statutu in financiranju evropskih političnih strank in evropskih političnih fundacij (UL L 317, 4.11.2014, str. 1).

¹⁰ Priporočilo Komisije (EU) 2018/234 z dne 14. februarja 2018 o krepitvi evropskega značaja in učinkovite izvedbe volitev v Evropski parlament leta 2019 (UL L 45, 17.2.2018, str. 40).

¹¹ Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

¹² Da bi lahko spletna mesta dostopala do takih informacij ali spremljala vedenje uporabnika na spletu, na primer s shranitvijo piškotkov v uporabnikovo napravo, je potrebna uporabnikova privolitev.

¹³ Predlog uredbe Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah), COM(2017) 10 final.

¹⁴ Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij z naslovom Boj proti dezinformacijam na spletu: evropski pristop (COM(2018) 236 final).

¹⁵ Za pripravo tega kodeksa ravnanja je Komisija maja 2018 sklicala forum, ki ga sestavljata „delovna skupina“ (sestavljena iz glavnih spletnih platform ter predstavnikov oglaševalske industrije in velikih oglaševalcev) in „posvetovalni odbor“ (sestavljen iz predstavnikov medijev in civilne družbe).

¹⁶ Potem ko posvetovalni odbor izda svoje mnenje.

¹⁷ Boti vključujejo avtomatizirano objavljanje na platformah družbenih medijev in bolj interaktivne aplikacije, kot so boti za klepet, ki neposredno komunicirajo z uporabniki.

razvoja kazalnikov verodostojnosti virov vsebin uporabnikom olajšali ocenjevanje vsebine, zmanjšali vidnost dezinformacij z izboljšanjem možnosti, da se najdejo verodostojne vsebine, in uporabnikom zagotovili informacije o prednostnem prikazovanju vsebin z algoritmi. Poleg tega bi podpisniki morali zaupanja vrednim organizacijam za preverjanje dejstev in akademskim ustanovam zagotoviti dostop do informacij o platformah. Ocena kodeksa ravnanja bo del prizadevanj za akcijski načrt s posebnimi predlogi za usklajen odziv EU na izziv dezinformacij, ki ga bosta pred koncem leta predstavili Komisija in visoka predstavnica.

Glede bolj „tradicionalnih“ kibernetских incidentov, kot so vdori v sisteme IT ali poškodbe spletnih mest, so bile na ravni Evropske unije opredeljene kaznivih dejanj in minimalne ravni za najvišje kazni v zvezi z napadi na informacijske sisteme usklajene z Direktivo 2013/40/EU o napadih na informacijske sisteme.

Skupina za sodelovanje, ustanovljena na podlagi Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta¹⁸, je kibernetško varnost volitev opredelila kot skupen izziv. Ta skupina za sodelovanje, ki jo sestavljajo pristojni nacionalni organi za kibernetško varnost, Komisija ter Agencija Evropske unije za varnost omrežij in informacij (ENISA), je pripravila pregled obstoječih nacionalnih pobud o kibernetški varnosti omrežij in informacijskih sistemov, ki se uporabljajo za volitve. Opredelila je tveganja, povezana z nezadostno ravno kibernetške varnosti, ki bi lahko vplivala na naslednje volitve v Evropski parlament, in pripravila zbirko praks na področju kibernetške varnosti za volilne tehnologije, vključno s tehničnimi in organizacijskimi ukrepi, ki temeljijo na izkušnjah in dobrih praksah. Zbirka praks daje praktična navodila organom za kibernetško varnost in organom za izvedbo volitev.

2. Nadaljnja krepitev demokratične odpornosti: izboljšanje mrež za volilno sodelovanje, spletne preglednosti, zaščite pred kibernetскими incidenti in boja proti dezinformacijskim kampanjam v okviru volitev v Evropski parlament

Zaradi razsežnosti izziva in glede na to, da so formalne odgovornosti na tem področju razdeljene med več organi, bodo pomembni rezultati doseženi le, če bodo vsi zadevni akterji sodelovali.

Temu sporočilu je priloženo Priporočilo Komisije o mrežah za volilno sodelovanje, spletni preglednosti, zaščiti pred kibernetскими incidenti in boju proti dezinformacijskim kampanjam v okviru volitev v Evropski parlament. Za zagotovitev svobodnih in poštenih volitev bi morali vsi akterji to priporočilo izvesti pravočasno za volitve v Evropski parlament leta 2019.

V priporočilu vse države članice spodbujamo, da vzpostavijo in podprejo nacionalno mrežo za volitve. Organi držav članic, ki so pristojni za volilne zadeve, bi morali poskrbeti za pravočasno in učinkovito sodelovanje z organi na povezanih področjih (kot so organi za

¹⁸ Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

varstvo podatkov, regulatorji na področju medijev, organi za kibernetično varnost itd.). Po potrebi bi morali sodelovati tudi z organi kazenskega pregona. To jim bo omogočilo hitro odkrivanje morebitnih groženj za volitve v Evropski parlament in hitro izvrševanje obstoječih pravil, vključno z razpoložljivimi finančnimi sankcijami, kot je povračilo javnega prispevka. Zakonodajajo EU in nacionalno zakonodajo je treba spoštovati in izvrševati. V tem pogledu Komisija države članice poziva, naj v skladu z veljavnim nacionalnim pravom in pravom Unije spodbujajo organe za varstvo podatkov, da organom, pristojnim za spremljanje volitev, posredujejo informacije, ter da spodbujajo spremljanje dejavnosti in financiranja političnih strank, če to izhaja iz njihovih odločitev ali če obstajajo drugi utemeljeni razlogi za domnevo, da je kršitev povezana s političnimi dejavnostmi nacionalnih političnih strank ali fundacij v okviru volitev v Evropski parlament.

Priporoča se tudi, da države članice določijo kontaktne točke za vključitev v evropsko mrežo za sodelovanje pri volitvah v Evropski parlament. Komisija bo te mreže za sodelovanje podprla tako, da bo do januarja 2019 sklicala prvo srečanje imenovanih kontaktnih točk. Ta forum bo ob upoštevanju nacionalnih pristojnosti in postopkovnih zahtev, ki veljajo za zadevne organe, zagotavljal jedro evropskega postopka opozarjanja v realnem času ter bo forum za izmenjavo informacij in praks med organi držav članic.

Politične stranke, fundacije in organizacije, ki sodelujejo pri kampanjah, morajo zagotavljati pregledne prakse pri svojih političnih sporočilih državljanom in skrbeti, da se evropski volilni proces ne izkrivlja zaradi nepoštenih praks. Komisija predstavlja konkretne ukrepe za večjo preglednost, da bodo državljani lahko videli, kdo stoji za političnim sporočilom, ki ga prejmejo, in kdo ga plačuje¹⁹. Države članice bi morale podpirati in spodbujati tako preglednost ter prizadevanja pristojnih organov pri spremljanju kršitev in izvrševanju pravil, vključno z uporabo sankcij, kadar je to potrebno. Kadar je to ustrezno, bi morali sodelovati tudi organi kazenskega pregona, da se zagotovita ustrezen odziv na incidente in uporaba ustreznih kazni²⁰.

Odpornost, odvrčanje in obramba so bistveni za vzpostavitev močne kibernetične varnosti za Evropsko unijo²¹. Pristojni evropski in nacionalni organi, politične stranke, fundacije in organizacije, ki sodelujejo pri kampanjah, bi se morali v celoti zavedati tveganj za volitve, ki bodo naslednje leto, ter si ustrezno prizadevati za varstvo svojih omrežij in informacijskih sistemov²².

¹⁹ Ti predlogi dopolnjujejo kodeks ravnanja, ki ga pripravlja forum več zainteresiranih strani, ki ga je Komisija sklicala na podlagi svojega sporočila z dne 26. aprila 2018 o dezinformacijah na spletu.

²⁰ To bi se nanašalo zlasti na primere zlonamernega napada na volilni proces, vključno z incidenti na podlagi napadov na informacijske sisteme. Glede na okoliščine so lahko primerne kazenske preiskave, ki lahko privedejo do kazenskih sankcij. Kakor je navedeno zgoraj, so bile opredelitve kaznivih dejanj in minimalne ravni za najvišje kazni v zvezi z napadi na informacijski sistem usklajene z Direktivo 2013/40/EU.

²¹ Visoka predstavnica Unije za zunanje zadeve in varnostno politiko ter Evropska komisija v skupnem sporočilu iz septembra 2017 priznavata, da je potreben celovit odziv, da bi v Uniji vzpostavili močno kibernetično varnost, ki bo temeljila na odpornosti, odvrčanju in obrambi (JOIN(2017) 450 final).

²² Zbirka praks, ki jo je pripravila skupina za sodelovanje, ustanovljena z Direktivo (EU) 2016/1148, daje v zvezi s tem koristna navodila. Cilj Direktive (EU) 2016/1148 je doseči visoko skupno raven odpornosti na področju kibernetične varnosti

3. Uporaba pravil o varstvu podatkov v volilnem procesu

Uredba (EU) 2016/679 Evropskega parlamenta in Sveta (Splošna uredba o varstvu podatkov)²³, ki se je v vsej Uniji začela neposredno uporabljati 25. maja 2018, Uniji zagotavlja orodja, potrebna za obravnavo primerov nezakonite uporabe osebnih podatkov v volilnem kontekstu.

Ker se bodo ta v evropskem volilnem kontekstu prvič uporabila ob prihodnjih volitvah v Evropski parlament, je pomembno, da vsi akterji, udeleženi v volilnih procesih, kot so nacionalni volilni organi, politične stranke, posredniki in analitiki podatkov, platforme družbenih medijev ter spletna oglaševalna omrežja, jasno razumejo, kako ta pravila najbolje uporabiti ter kaj dovoljujejo in česa ne.

Komisija je tako pripravila posebne smernice, da bi poudarila obveznosti glede varstva podatkov, ki so pomembne v volilnem kontekstu. Nacionalni organi za varstvo podatkov morajo kot izvrševalci Splošne uredbe o varstvu podatkov v celoti izkoristiti svoja okrepljena pooblastila za obravnavanje morebitnih kršitev, da se preprečijo zlonamerni poskusi zlorabe osebnih podatkov posameznikov, zlasti za namene izjemno natančnega ciljnega usmerjanja.

4. Krepitev pravil o financiranju evropskih političnih strank

Politične stranke in fundacije so seveda ključni akterji na volitvah. S svojimi kampanjami se potegujejo za glasove volivcev. Da bi se zagotovili enaki konkurenčni pogoji ter bi se vse politične stranke in fundacije obvarovale pred zlorabami, je bistveno preprečiti primere, v katerih bi lahko katera koli oseba imela koristi od nezakonitih praks, ki kršijo pravila o varstvu podatkov. Take prakse, ki ne kršijo le zasebnosti ljudi, temveč bi lahko vplivale tudi na izid volitev v Evropski parlament, bi bilo treba sankcionirati. Komisija poleg poziva državam članicam, naj take sankcije po potrebi uporabijo za stranke in fundacije na nacionalni ravni, predlaga uvedbo ciljno usmerjene spremembe Uredbe (EU, Euratom) št. 1141/2014, da se v primerih, v katere so vpletene politične stranke in fundacije na evropski ravni, zagotovijo sorazmerne sankcije. Cilj navedene spremembe, ki izboljšuje obstoječa pravila, je zagotoviti, da lahko volitve v Evropski parlament potekajo v okviru trdnih demokratičnih pravil in ob

po vsej Uniji. Za doseg tega cilja direktiva podpira razvoj nacionalnih zmogljivosti kibernetike varnosti in varuje zagotavljanje bistvenih storitev v ključnih sektorjih. Da bi Komisija okrepila prizadevanja za ustrezno izvajanje direktive, do leta 2020 prek Instrumenta za povezovanje Evrope (IPE) zagotavlja financiranje v višini več kot 50 milijonov EUR. Ukrepi za obvladovanje tveganj iz Direktive (EU) 2016/1148 so ustrezna merila uspešnosti za volilni proces. Splošna uredba o varstvu podatkov določa tudi obveznosti za izvajanje ustreznih tehničnih in organizacijskih ukrepov, da se zagotovi raven varnosti za osebne podatke, ki se obdelujejo. Velja za vse akterje, udeležene v volilnem procesu, vsebuje pa tudi obveznost sporočanja kršitev varstva osebnih podatkov pristojnim organom za varstvo podatkov in zadevnim posameznikom (glej smernice, ki jih je izdala Komisija).

²³ Uredba (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 (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

polnem spoštovanju vrednot, na katerih temelji Unija, zlasti demokracije, temeljnih pravic in pravne države.

Komisija poziva Evropski parlament in Svet, naj zagotovita, da bodo te osredotočene spremembe uveljavljene pred volitvami v Evropski parlament leta 2019.

5. Sklepne ugotovitve

Nedavni dogodki so pokazali, da so tveganja za manipulacijo volilnega procesa z napadi na informacijske sisteme, zlorabo osebnih podatkov in nepreglednimi praksami resnična in akutna. EU za taka tveganja ni nedovzetna. Spletne dejavnosti v volilnem kontekstu pomenijo novo grožnjo in zahtevajo posebno varstvo. Za državljane in demokracijo bomo največ storili tako, da se že zdaj pripravimo. Ne moremo čakati, da bi take dejavnosti odkrili po volitvah ali referendumih in se šele takrat odzvali nanje.

Varovanje demokracije v Uniji je skupna ter resna odgovornost Evropske unije in njenih držav članic. Poleg tega gre za nujno vprašanje. Vsi vpleteni akterji morajo okrepiti svoja prizadevanja in sodelovati, da se odvrne, prepreči in kaznuje zlonamerno vmešavanje v volilni sistem. Ukrepi, ki jih je Komisija predlagala v tem svežnju, podpirajo ta prizadevanja.

Komisija bo po volitvah v Evropski parlament leta 2019 poročala o izvajanju tega svežnja ukrepov.

Naslednji koraki do volitev v Evropski parlament leta 2019

- *Komisija poziva Evropski parlament in Svet, naj zagotovita pravočasno uvedbo predlaganih ciljno usmerjenih sprememb Uredbe (EU, Euratom) št. 1141/2014 za volitve v Evropski parlament leta 2019.*
- *Komisija bo skupaj z visoko predstavnico podprla pripravo skupnih evropskih odzivov, ki bodo obravnavali morebitno tuje vmešavanje v volitve v Evropski uniji²⁴. Na podlagi sklepov Evropskega sveta iz junija 2018 bosta v sodelovanju z državami članicami do decembra 2018 predstavili akcijski načrt s posebnimi predlogi za usklajen odziv EU na izziv dezinformacij.*
- *Komisija bo okrepila ozaveščenost in ohranila dialog z organi držav članic prek konference na visoki ravni o kibernetičnih grožnjah za volitve, ki bo potekala 15. in 16. oktobra 2018, njeni rezultati pa bodo vključeni v naslednji kolokvij o temeljnih*

²⁴ To bi lahko vključevalo tudi uporabo ukrepov, oblikovanih v okviru za skupni diplomatski odziv EU na zlonamerne kibernetične dejavnosti.

*pravica*h (26. in 27. novembra 2018), ki bo osredotočen na demokracijo v Evropski uniji.