



Štrasburg 24. jún 2019

CDL-AD(2019)016

Stanovisko č. 925/2018

org. anglicky

EURÓPSKA KOMISIA PRE DEMOKRACIU PROSTREDNÍCTVOM PRÁVA

(BENÁTSKA KOMISIA)

SPOLOČNÁ SPRÁVA

BENÁTSKEJ KOMISIE

**A RIADITEĽSTVA PRE INFORMOVANÚ SPOLOČNOSŤ A BOJ PROTI
KRIMINALITE A GENERÁLNEHO RIADITEĽSTVA PRE ĽUDSKÉ PRÁVA
A PRÁVNÝ ŠTÁT (DGI)**

O DIGITÁLNYCH TECHNOLOGIÁCH A VOĽBÁCH

**prijatá Radou pre demokratické voľby na svojom 65. zasadnutí
(Benátky, 20. júna 2019)**

**prijaté Benátskou komisiou na svojom 119. plenárnom zasadnutí (Benátky, 21. – 22.
júna 2019)**

na základe poznámok

pána Richarda BARRETTA (člen, Írsko)

pani Herdísy KJERULF THORGEIRSDOTTIR (člen, Island)

pána Rafaela RUBIA NUÑEZA (zastupujúci člen, Španielsko)

pána Josého Luisa VARGASA VALDEZA (zastupujúci člen, Mexiko)

pani Krisztiny ROZGONYIOVEJ (expertka DGI, divízia správy médií a internetu)

pani Neveny RUZIC (expertka DGI, divízia ochrany údajov)

Obsah

I. Úvod.....	3
II. Pozadie.....	3
III. Nové technológie a informácie.....	7
IV. Vplyv sociálnych médií a internetu na demokraciu a volebné procesy	11
V. Relevantné európske a medzinárodné štandardy a nástroje	15
A. Právo na slobodné voľby a sloboda prejavu.....	15
1. Základné princípy.....	15
2. Financovanie volebných kampaní	18
3. Politický prejav a medializácia volebných kampaní	19
B. Právo na súkromie a ochrana osobných údajov.....	22
C. Ochrana pred počítačovou kriminalitou	25
VI. Iné medzinárodné a vnútroštátne právne predpisy, judikatúra a iniciatívy.....	26
A. Medzinárodná úroveň.....	26
B. Európska únia	27
C. Príklady na národnej úrovni	29
VII. Elektronické výzvy pre demokraciu a ľudské práva.....	32
A. Výzvy pre volebnú demokraciu	33
B. Výzvy pre deliberatívnu demokraciu	37
VII. Závery	43

I. Úvod

1. Rada pre demokratické voľby na základe iniciatívy pána Josého Luisa Vargasa Valdeza a na základe jeho „Štúdie o úlohe sociálnych médií a internetu v demokratickom vývoji“ (CDL-LA(2018)001) sa na svojom 59. zasadnutí (15. júna 2017) spoločne s oddelením informačnej spoločnosti Rady Európy rozhodli podstúpiť štúdiu o používaní digitálnych technológií vo volebnom procese.

2. Okrem pána Vargasa Valdeza ako spravodajcovia vystupovali aj pani Herdis Kjerulf Thorgeirsdóttir a páni Richard Barrett a Rafael Rubio Nuñez. Pani Krisztina Rozgonyi a pani Nevena Ružić vystupovali ako experti zastupujúci Riaditeľstvo pre informačnú spoločnosť a boj proti kriminalite, oddelenie správy médií a internetu a oddelenie ochrany údajov. Pán Alexander Seger, vedúci oddelenia počítačovej kriminality, taktiež prispel k príslušným častiam tejto správy.

3. Táto spoločná správa bola pripravená na základe pôvodnej štúdie pána Vargasa Valdeza a na základe poznámok predložených spravodajcami a už uvedenými expertmi; bola preskúmaná na zasadnutí Podkomisie pre latinskú Ameriku 30. novembra 2018, prijatá Radou pre demokratické voľby na jej 65. zasadnutí (Benátky 20. júna 2019) a následne prijatá Benátskou komisiou na jej 119. plenárnom zasadnutí (Benátky 21. – 22. júna 2019).

II. Pozadie

4. Digitálne (alebo nové) technológie a sociálne médiá – tie sa chápu ako „internetové platformy, ktoré umožňujú obojsmernú interakciu prostredníctvom obsahu vytváraného používateľmi“¹ – revolucionizovali spôsob interakcie ľudí a výkon ich slobody prejavu a práva na informácie, ako aj ďalšie súvisiace – a niekedy protichodné – základné práva.² Ľudia, ktorí sa zapájajú do sociálnych médií, môžu používať internet na organizovanie a požadovanie lepších služieb, väčšej transparentnosti a zmysluplnej účasti na politickej scéne.³ Jednotlivci všade na planéte sú dnes schopní formovať globálne vnímanie, zahrnúť témy do svojich vnútroštátnych politických programov a podporovať politický aktivizmus.⁴ Táto digitálna transformácia pretvára vzťah medzi štátom a občanmi.

¹ Táto štúdia je založená na definícii sociálnych médií ako «webových alebo mobilných platforiem, ktoré umožňujú obojsmernú interakciu prostredníctvom obsahu vytváraného používateľmi (UGC) a komunikácie. Sociálne médiá teda nie sú médiá, ktoré pochádzajú len z jedného zdroja, alebo sú vysielané zo statickej webovej stránky. Ide skôr o médiá na špecifických platformách, ktoré umožňujú používateľom vytvárať („generovať“) obsah a interagovať s informáciami a ich zdrojom (International IDEA 2014: 11). Zatiaľ čo sociálne médiá sa spoliehajú na internet ako médium, je dôležité poznamenať, že nie všetky internetové stránky alebo platformy spĺňajú definíciu sociálnych médií. Niektoré webové stránky neumožňujú interaktivitu s publikom, zatiaľ čo iné umožňujú používateľom uverejňovať komentáre iba ako reakciu na konkrétny zverejnený obsah ako diskusné príspevky (alebo „vlákna“), ktoré sú moderované a kontrolované.» (International IDEA 2014: 11).

² Parlamentné zhromaždenie Rady Európy, Rezolúcia 1987 [2014] o práve na prístup na internet.

³ Santiso, 2018.

⁴ Sú na to pozoruhodné príklady: od egyptských tínedžerov, ktorí využívali Facebook na zhromaždenie demonštrantov na námestie Tahrir, cez vplyv dezinformácií na výsledok kenských prezidentských volieb až po Číňanov, ktorí viedli online kampaň, aby sa hlasovanie v zámorí „Haz tu voto volar“ stalo kľúčovou volebnou otázkou, alebo projekt overovania faktov „Verificado2018“ v Mexiku.

5. Podľa Globálnej digitálnej správy 2018 viac ako polovica svetovej návštevnosti internetových stránok teraz pochádza z mobilných telefónov. Z celkového počtu 7,6 miliardy obyvateľov planéty sú približne 4 miliardy používateľmi internetu (čo predstavuje 53 % celkovej populácie) a 3,2 miliardy sú aktívnymi používateľmi sociálnych médií (čo predstavuje 42 % celkovej populácie).

6. Medzi rokmi 2017 a 2018 počet používateľov internetu vzrástol o 7 % a počet aktívnych používateľov sociálnych médií vzrástol o 13 %. Bežný používateľ internetu strávi online 6 hodín každý deň. Väčšinu tohto času strávi na platformách ako Facebook (viac ako 2 miliardy používateľov), YouTube (1 a pol miliardy používateľov), Instagram (800 miliónov používateľov) a Twitter (330 miliónov používateľov).

7. Približne 2 miliardy používateľov internetu dnes využíva sociálne siete⁵ na dennej báze, ktoré sa stali neoddeliteľnou súčasťou modernej politickej kampane, pričom ich efekt na verejnosť je závislý od viacerých faktorov, ako sú napríklad premenné kanálov (napr. Twitter v Instagram), špecifické charakteristiky a predispozícia publika, motivácia užívateľov a celkový kontext politickej kampane.⁶

8. Hoci sa zdá, že každý používa internet a sociálne médiá, rôzne vekové kategórie ich využívajú na rôzne účely. Podľa správy *Reuters Institute Digital News Report 2017* sa sociálne médiá zdajú byť hlavným zdrojom spravodajstva pre osoby od 18 do 34 rokov, zatiaľ čo pre osoby nad 5 rokov je dôležitejšia televízia.

9. Podľa tej istej štúdie *Reuters Institute* viac ako polovica respondentov (54 %) preferuje postupy, ktoré na selektovanie príbehov využívajú algoritmy (vyhľadávače, sociálne médiá a mnoho agregátov informačných kanálov), a nie redaktorov alebo novinárov (44 %). To znamená, že mladí ľudia môžu svoje politické rozhodnutia zakladať na informáciách filtrovaných algoritmami týchto digitálnych médií namiesto prísnych novinárskych štandardov. Zároveň je potrebné poznamenať, že podľa nedávnej štúdie⁷ môžu personalizované odporúčania prostredníctvom algoritmov poskytovať rovnako rozmanité ponuky ako ľudská redakcia.

10. Podľa správy *Reuters Institute Digital News Report 2018* sa používanie sociálnych médií na prístup k spravodajstvu v roku 2017 znížilo. Zdá sa, že ľudia menej dôverovali zdrojom na sociálnych sietiach. Dalo sa tiež spozorovať, že „internet sa rýchlo zmenil z primárneho zdroja prístupu k informáciám na účastnícke prostredie, ktoré dôkladne napodobňuje tradičnú demokratickú účasť vo fyzickom svete“.⁸ V dôsledku toho masívne využívanie internetu a sociálnych médií na celom svete mení viaceré aspekty spoločenského a politického života. Sociálne mechanizmy vytvárania znalostí a názorov sa stali viac kolaboratívnymi

⁵ Statista – Najpopulárnejšie sociálne siete na svete od októbra 2018. Dostupné na: <<https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>>.

⁶ Dimitrova & Matthes, 2018.

⁷ Pozri <<https://www.tandfonline.com/doi/abs/10.1080/1369118X.2018.1444076>> a <<https://www.thatseemsimportant.com/content/blame-the-algorithm/>>.

⁸ Laidlaw 2015, s. 7.

a samo-regulačnými (napríklad Wikipedia a Facebook) a politický aktivizmus si našiel nové spôsoby organizácie a vyjadrenia.⁹

11. Na začiatku bol internet oslavovaný ako príslub rovnosti a slobody. Považoval sa za potenciálnu novú verejnú sféru, platformu demokratickej verejnej politickej diskusie, ktorá umožňuje jednotlivcom byť aktívnymi účastníkmi verejnej diskusie a vďaka aktívnej diskusii na sociálnych médiách prispievať k efektívnejšej politickej demokracii s osvietenou verejnosťou. Verejná sféra bola hierarchicky organizovaná so stanovenými a zavedenými funkciami rôznych aktérov ako štát, médiá, cirkev a výchovné inštitúcie, pričom dnes už všetky stratili kontrolu nad horizontálnou výmenou správ a názorov medzi užívateľmi. Sociálne siete sľúbili, že dajú hlas každému. Na rozdiel od tradičných masmédií internet má otvorenú viacsmernú architektúru a náklady na prístup k nemu sú relatívne nízke. Vďaka týmto vlastnostiam je internet obzvlášť efektívnym médiom pre bežného občana, ktorý sa tam môže stať aktívnym vystupujúcim namiesto toho, aby informácie len získaval, a vytvoril tak „*verejnú sféru prepojenú sieťou*“, kde môžu jednotlivci „*sledovať a narúšať používanie moci masmédií*“ vďaka okamžitému prístupu k viacerým zdrojom informácií a ich distribúcii.

12. V minulosti to boli novinári, ktorí so svojimi redakčnými postupmi a etickou zodpovednosťou zastávali v komunikácii rolu strážnika nielen svojimi rozhodnutiami, čo dať do tlače alebo zverejniť, ale aj tým, že boli zodpovední za dodržiavanie zákonných požiadaviek, ako sú spravodlivé a vyvážené spravodajstvo s ohľadom na verejnoprávne médiá, rešpektovanie prípadného mlčania, ak bolo relevantné, a/alebo práva na odpoveď a rovnocenné opravné prostriedky pre kandidátov a politické strany. Dnes túto úlohu strážcu čoraz viac preberajú nové sprostredkovateľské subjekty. Medzi také spoločnosti patria napríklad internetoví poskytovatelia služieb, vyhľadávače a sociálne médiá. Internetoví sprostredkovatelia¹⁰ sú organizácie (predovšetkým podnikateľské spoločnosti), ktoré „*zdržujú alebo uľahčujú transakcie medzi tretími stranami na internete. Poskytujú prístup k hostovaniu, prenosu a indexovaniu obsahu, produktom a službám od tretích strán na internete alebo poskytujú internetové služby tretím stranám*“. Tak získali kontrolu nad tokom, dostupnosťou, prístupnosťou a vyhľadávaním informácií a obsahu online.¹¹

13. Veľkým sľubom internetu bolo jeho fungovanie nezávisle od existujúcich monopolov v oblasti komunikácie, ale v skutočnosti majú veľké nadnárodné korporácie¹² globálnu kontrolu nad tokom informácií, a sú preto v postavení, v ktorom môžu tvarovať politickú

⁹ Castells 2011; Cohen et al. 2012.

¹⁰ Pojem „internetoví sprostredkovatelia“ sa vzťahuje na prevádzkovateľov online mediálnych platforiem, vyhľadávačov, sociálnych sietí a obchodov s aplikáciami (van der Noll, Helberger a Kleinen-von Königslöw, 2015). Podľa odporúčania Rady Európy CM/Rec(2018)2 o úlohách a zodpovednostiach internetových sprostredkovateľov tieto subjekty uľahčujú interakcie na internete medzi fyzickými a právnickými osobami tým, že ponúkajú a vykonávajú rôzne funkcie a služby. Niektoré pripájajú používateľov k internetu, umožňujú spracovanie informácií a údajov alebo hostujú webové služby vrátane obsahu vytváraného používateľmi. Iné zhromažďujú informácie a umožňujú vyhľadávanie; poskytujú prístup, hostujú a indexujú obsah a služby navrhnuté a/alebo prevádzkované tretími stranami. Niektoré uľahčujú predaj tovaru a služieb vrátane audiovizuálnych služieb a umožňujú iné obchodné transakcie vrátane platieb.

¹¹ <https://www-cdn.law.stanford.edu/wp-content/uploads/2017/04/07_28.2_Persily-web.pdf>

¹² Pozri o. i. <<https://www.forbes.com/sites/steveandriole/2018/09/26/apple-google-microsoft-amazon-and-facebook-own-huge-market-shares-technology-oligarchy/#372d73d92318>>.

diskusiu a formovať názory. Fungujú tu rovnaké sily ako v prostredí tradičných médií, ibaže teraz sú ich hlasy zosilnené sociálnymi médiami a sú schopné dosiahnuť každý kút sveta a meniť spoločnosti a životy. Predstava, že internet by mal pre nových účastníkov poskytovať aspoň minimálne konkurenčné prostredie, sa už javí ako neaktuálna. Niekoľko súkromných aktérov, ktorí vlastnia informačné toky, je dostatočne vplyvných a neregulovaných na to, aby diktovali podmienky sociálnych, individuálnych a politických slobôd, čím sa stávajú tretím aktérom v aréne demokracie; vytváranie obsahu sa stalo natoľko „demokratickým“ a anonymným, že je neskutočne ťažké identifikovať dôveryhodné informácie a pripísať zodpovednosť za protiprávne konanie online.

14. Sociálne média ako napríklad Facebook nie sú nič iné ako tradičné médiá kontrolované trhovými silami. Akcie Facebooku ako každej veľkej mediálnej korporácie závisia od príjmov z reklamy, aby mohli finančne rásť a zachovávať si trhovú hodnotu. Reklama na Facebooku funguje tak, že sa prostredníctvom technologicky vyspelej operácie určia záujmy používateľov na základe údajov získaných z ich vyhľadávania, „páči sa mi“ a podobne. Internetové stránky zarábajú z kliknutí a prostredníctvom regulácie algoritmov vytvárajú komnaty ozvien (*echo chambers*) a filtračné bubliny (*filter bubbles*), v ktorých jednotlivci získavajú taký typ informácií, ktoré si buď vopred vybrali, alebo čo je hrozivejšie, o ktorých algoritmy zistili, že chcú počuť. To umožňuje, aby bola politická reklama stále viac cielená a prispôbená jednotlivcovi. Miesto toho, aby bol internet verejným miestom, kde zaznie veľa názorov, ľudia sa stávajú izolovanejšími a nie sú v kontakte s celým spektrom verejnosti.

15. „Demokratizácia“ vytvárania obsahu a centralizácia online distribučných kanálov má ako nezamýšľaný účinok šírenie nepravdivých informácií a taktiku súkromných a verejných dezinformácií. Každý príchod nového komunikačného prostriedku (1) zvyšuje šírenie informácií a prístup k nim (sloboda komunikácie); (2) vedie k riziku zneužitia (škodlivý obsah); (3) otvára cestu k cenzúre a (4) manipulácii zo strany vplyvných verejných a súkromných subjektov.

16. Vývoj internetu a sociálnych médií priniesol masovú komunikáciu a proces šírenia a získavania informácií posunul do rozmerov, aký bol od vytvorenia knižnice nepredstaviteľný. Šírenie nepravdivých informácií, taktika šírenia verejných a súkromných dezinformácií sa preto za posledných niekoľko rokov stala výrazne rozšírenejšou a technicky sofistikovanejšou s internetovými botmi, tvorcami propagandy, dezinformačnými médiami, ktoré využívajú sociálne médiá, a vyhľadávacími algoritmami, ktoré im zaisťujú vysokú viditeľnosť a bezproblémovú integráciu s dôveryhodným obsahom, zavádzajúc tak široké publikum konzumentov spravodajstva, ba čo viac, voličov. Hoci bola dezinformácia vždy stratégiou na zdiskreditovanie oponentov a na nasmerovanie politickej podpory na jednu alebo druhú stranu, digitálne technológie zvýšili hrozbu, ktorú predstavujú falošné informácie pre demokraciu z rôznych dôvodov: rýchlosť šírenia (nepravdivých) informácií prostredníctvom internetu;¹³ skutočnosť, že ich šírenie je uľahčené architektúrou

¹³ Teraz sú k dispozícii aj dôkazy, že ľudia častejšie zdieľajú falošné správy. Navyše, podľa doteraz najväčšej štúdie tohto fenoménu v digitálnych médiách vykonanej MIT sú falošné správy náchylnejšie na šírenie digitálnymi prostriedkami. Okrem toho sa zdá, že pravdivým príbehom trvá asi šesťkrát dlhšie ako falošným, kým sa dostanú k ľuďom (Vosoughi, Roy a Aral, 2018). Podľa globálnej správy Edelman Trust Barometer 2018 sa takmer 70 % globálnych používateľov internetu obáva používania „falošných správ“ ako zbrane.

vyhľadávačov a sociálnych médií; nedostatok nástrojov (či už právnych, spoločenských alebo technických) na ich identifikovanie a zastavenie šírenia; a zložitosť vyšetrovania a stíhania takého správania cez internet.

17. V posledných rokoch sa zahraničné zásahy do volieb prostredníctvom používania sociálnych sietí stali obavou pre demokraciu. Technologické zdroje ako napríklad nízko nákladové špionážne kampane, platení užívatelia a internetové boty, selektívne zverejňovanie informácií alebo vytváranie nepravdivých informácií zmenili pravidlá hry počas volebnej kampane. Vedľajším účinkom je narušenie dôvery v demokratické vlády.

18. V celosvetovom meradle môže táto už spomínaná prax – ktorá je podporovaná technológiami – predstavovať hrozbu demokracii a spochybňovať myšlienku internetu ako technického prostriedku pre demokratickejšiu správu verejných vecí.

19. Existencia digitálnych technológií a ich uplatnenie na takmer všetky aspekty života vrátane volieb je skutočnosť, ktorú nemožno spochybniť. Táto správa nie je robená so zámerom posúdiť ich pozitívne a negatívne aspekty, ale je zameraná na riešenie výziev, ktoré predstavujú v oblasti volieb. Preto sa bude sústreďovať najmä na problémy, ktoré tieto inovácie vyvolávajú a na ich možné riešenia, a nie na ich výhody.

20. Predkladaná správa nezamýšľa poskytnúť konkrétne a univerzálne riešenia na všetky problémy, ktoré používanie internetu a sociálnych médií môže vyvolať vo volebnom procese. Osobitosti každého štátu a každej demokracie by to spravili nemožným.¹⁴ Namiesto toho je jej cieľom identifikovať najrelevantnejšie právne problémy spôsobené používaním týchto technológií, popísať ich logiku a parametrov možného riešenia, pomenovať doteraz identifikované chyby a navrhnúť všeobecný súbor zásad a smerníc, ktoré môžu pomôcť demokracii prispôbiť seba a svoju právnu reguláciu realite nových technológií. V tomto zmysle sa záver tejto práce podobá skôr na mapu k existujúcim a budúcim zásadám regulácie a spolupráce, a nie príručke na riešenie všetkých problémov.

21. Táto správa je doplnkom k predchádzajúcim dokumentom Rady Európy k tejto téme, najmä správe Rady Európy z roku 2017 o „Informačnom zmätku“¹⁵ (správa o informačnom zmätku 2017) a k „Štúdiu o používaní internetu vo volebnej kampani“ (volebná štúdia 2017).¹⁶

III. Nové technológie a informácie

22. V online spoločnosti sú informácie primárnou komoditou nielen pre ekonomickú produkciu, ale aj pre sociálnu interakciu a riadenie. Vplyv internetu na realitu je univerzálny a ovplyvňuje aj tých, ktorí technológie nikdy nevyužívali. Priamo ovplyvňuje verejnú mienku, kdekoľvek sa ľudia nachádzajú, a mení spôsob, ako sa ľudia správajú a myslia vo svete okolo nich. Dáva možnosť vyjadriť sa každému, kto má o to záujem, a umožňuje im prispievať do verejnej diskusie, či už pozitívne alebo negatívne. Otvára cestu „subjektom PR“, aby sa ponáhľali na fórum vždy vtedy, keď je v stávke veľa a pokúsili sa ovplyvniť vývoj udalostí.

¹⁴ Príklady rôznych kritérií na riešenie podobných problémov nájdete v referenčnom dokumente CDL-AD(2019)016.

¹⁵ Správa Rady Európy, DGI(2017)09.

¹⁶ Štúdia Rady Európy, DGI(2017)11.

Do tejto rovnice virtuálneho a fyzického niekedy zasiahne aj fikcia.¹⁷ Verejné osoby môžu zistiť, že nimi stvárané fiktívne postavy sú oveľa vplyvnejšími „aktérmi“ ako ich fyzické ja.¹⁸ Humor môže mať podobný účinok: používatelia internetu môžu budovať rôzne predstavy, napríklad vytváraním fiktívnych satirických účtov verejných osôb, čo priamo ovplyvňuje imidž dotknutých osôb a môže občas zmiatť verejnosť a masmédiá.¹⁹

23. Informácie sú zdieľané najmä prostredníctvom obrázkov, ktoré sa na rozdiel od slov spracúvajú automaticky: človek riskuje, že sa zmení na pasívneho prijímateľa ponoreného do farieb, tvarov, sekvencií a šumu na pozadí, a pri absencii písanej kultúry a verbálneho jazyka sa stane neschopným transformovať informácie do vedomostí a obrázky do úsudkov a nápadov. Riskuje postupné znižovanie kapacity abstrahovania. *Homo sapiens*²⁰ sa stále viac mení na *homo videns*: tvor, ktorý sa pozerá, ale nerozmýšľa, ktorý vidí ale nerozumie. Obrázky sú doplnené o písaný text, či už pozitívny alebo negatívny, ktorý je taktiež konvertovaný do obrázku a, ako iné informácie, je spracovaný okamžite, miesto toho, aby sa o ňom premýšľalo.²¹

24. Ak je informácia redukovaná na jednoduché stimuly, ktoré ovplyvňujú prijímateľa,²² človek reaguje skôr na presvedčenie, a nie na informácie. Význam obrázku vedie tiež ku ťažkostiam s vysvetlením komplexných konceptov, ktoré si vyžadujú určitý stupeň abstrakcie. Stimuly, na ktoré ľudia reagujú, sú takmer výlučne audiovizuálne, pričom predpokladajú o nich, že sú pravdivé, a reagujú len na obrázky, ktoré sú schopné vyvolať reakciu. Citový obsah v nepotvrdených správach sa stáva oveľa dôležitejší ako skutočný, a tak provokuje emocionálne reakcie, zvyčajne nenávisť alebo ohováranie. Stále viac to využívajú PR agentúry platené politickými aktérmi na mobilizáciu v oblasti, kde sa presadili nenávisť a ohováranie.

25. Fenomén nazvaný „fake news“ (falošné správy)²³ upútal všeobecnú pozornosť na začiatku prezidentských volieb v USA v roku 2016. „Fake news“ zahŕňa rôzne odlišné

¹⁷ Jasný príklad zrútenia hranice medzi fikciou a realitou možno pozorovať v komunikačnej stratégii DAESH. Vedomým napodobňovaním videohier a trhákov vyvolávajú pozornosť, vytvárajú poľudštený obraz teroristu a odosobnený obraz obetí: Lesaca, Javier. Masívna zbraň. Península, Atalaya, 2017. Naopak, tradičné médiá nereflektujú dôsledky ich barbarstva v celej krutosti.

¹⁸ Podpora Kevina Spaceyho alebo jeho stelesnenie prezidenta Spojených štátov amerických v seriáli House of Cards vyvolala veľa kontroverzií. Prípád zápasníka Hulka Hogana sa dostal pred severoamerické súdy a nakoniec dosiahol priaznivý rozsudok na základe rozdielu medzi činmi fiktívnej postavy v ringu a mimo neho a osobou, ktorá ju stelesňovala.

¹⁹ Na rôznych platformách sociálnych médií sú falošné účty rozšírené a bez ohľadu na to, či upozorňujú na svoju parodickú povahu alebo nie, vytvárajú stereotyp postavy, ktorú napodobňujú, využívajúc humor. Niektorí z nich majú v konečnom dôsledku väčšiu sledovanosť ako skutočné účty osoby, ktorú parodujú. V španielskej politike sú pozoruhodnými príkladmi @EspeonzaAguirre a @NanianoRajoy.

²⁰ Sartori, Giovanni. *Homovideos*, Taurus, 1989

²¹ V tejto súvislosti je dôležité prehodnotiť slávnu frázu E. M. Fostera, ktorá hovorila, že „*Knihy sú fakty, ktoré treba čítať (čo je nepríjemné, pretože to trvá dlho); je to jediný spôsob, ako zistiť, čo obsahujú. Niektoré divoké kmene ich jedia, ale na Západe je čítanie jedinou známou technikou.*“

²² Schwartz, Tony. *La respuesta emocional*. Ed. Liderazgo democrático 2. Quito, 2001. p. 37.

²³ Správa Rady Európy o informačnom zmätku z roku 2017 sa zámerne zdržiava používania termínu „falošné správy“ z toho dôvodu, že je neadekvátny na zachytenie zložitosti informačného znečistenia a je čoraz viac spolitizovaný.

javy, najčastejšie kombinuje prvky tradičného spravodajstva s prvkami, ktoré nepatria do tradičnej žurnalistiky.²⁴ Falošné správy sú charakteristické pre kolaps tradičných spravodajstiev (hoci dezinformácie alebo senzácie nie sú novým fenoménom) a prevládajúci chaos v komunikácii na sociálnych médiách. Toto je nová verzia starého boja o definíciu pravdy, politických a finančných síl, ktoré vedú propagandistické vojny, využívajúc *falošné správy* ako hlavnú zbraň.

26. Masová distribúcia obrázkov rozhodne prispela k úspechu falošných správ tým, že dala informáciám zdanie neomylnosti. Komunikácia sa nakoniec zmení na predstavenie odmeňujúce jednoduché koncepty, zavádzajúce titulky, čokoľvek čo priťahuje pozornosť čitateľa (*click bait*), hoci môže skončiť až zjednodušene. Forma kraluje nad obsahom a obrázky nad myšlienkami; hľadajú sa jednoduché odpovede, ktoré rozdeľujú svet na čierne a biele, áno a nie a v ktorom nie sú žiadne nuansy. Stručnosť, dôležitosť obrázka a jednoduché zdieľanie obsahu typické pre sociálne siete, to všetko podporuje šírenie techník, ktoré skresľujú realitu.

27. Dnešné očakávanie neustálych aktualizácií a dokonca predpovedí²⁵ vedie k tomu, že sa informácie vyvíjajú hneď, ako vzniknú, bez toho, aby boli kontrolované alebo sa nad nimi zamyslelo. Táto dynamika odmeňuje rýchlosť, a nie kvalitu, čím vytvára informačné cykly, ktoré často netrvajú ani dvadsaťštyri hodín, a vyčerpávajú informácie skôr, než sú nasledujúci deň zverejnené v tlačенých médiách. Nekonečná úložná kapacita a jej dostupnosť znamenajú, že vyjadrenia môžu byť v priebehu niekoľkých sekúnd oživené z príslušnej webovej stránky mesiace, ba dokonca aj roky neskôr. Odhalené rozpory tiež podliehajú masovému šíreniu a niekedy, ak sú postavené mimo kontext, môžu byť predmetom „*fake news*“.

28. Tisícky analýz, dát a názorov o každej udalosti sa chaoticky hromadia na sociálnych sieťach a sú šírené takmer nekonečnou kapilaritou prostredníctvom rôznych koncových staníc, ku ktorým sú ľudia pripojení. Preťaženie informáciami bráni komunikácii, pretože niektoré fakty môžu ostať bez povšimnutia v tieni jednoduchších a pútavejších skutočností. Postup opravy chybných informácií nie je dostatočným prostriedkom na opravu týchto chýb.

29. Jednotlivci si vytvárajú svoje vlastné informačné ekosystémy alebo osobný svet, ktorý je tvorený informáciami, ktoré odkazujú samy na seba, nevyžadujú si konzistenciu s predchádzajúcimi textami, dokonca ani s realitou. Dôsledkom je silne skreslené vnímanie tých, ktorí nezdediajú rovnaký informačný ekosystém. Nové a rozmanité zdroje informácií umožňujú potvrdenie jednotlivých myšlienok, a tak posilňujú konfirmačné skreslenie, v ktorom sa pozornosť a dôveryhodnosť pripisujú informáciám, ktoré pomáhajú posilniť vlastné presvedčenie. Algoritmus využívaný nástrojmi osobnej komunikácie a inými sociálnymi sieťami zistí preferencie používateľa, znázorňuje ich častejšie, a tak posilňuje vedomosti a podporu podobných tém. Napriek obrovskému množstvu dostupných informácií je väčšina buď nedostupná, alebo k nim majú prístup tí, ktorí sú už presvedčení o ich

²⁴ Mourao, R. R. a Robertson, C. T. Falošné správy ako diskurzívna integrácia: Analýza stránok, ktoré zverejňujú nepravdivé, zavádzajúce, hyperpartizánske a senzáčné informácie, publikované online: 13. januára 2019.

²⁵ V Španielsku, najmä na Wikipédii, súčasný trend zahŕňa upozornenie na smrť ľudí, ktorí sú v skutočnosti zdraví. Napríklad zdravotná sestra, ktorá sa nakazila ebolou, bola spopolnená a potom zázračne opäť ožila.

nedôveryhodnosti. Neželané alebo nevítané fakty sa dajú ignorovať v prospech personalizovaných príbehov. Informácie a ich opravy sú vyberané s cieľom dokázať, že určitý názor je správny a že iné názory sú zlé.²⁶ K tomu môže dôjsť aj s overenými informáciami, pretože sú zdieľané oveľa viac, ak posilňujú predchádzajúce myšlienky, než keď ich spochybňujú.²⁷

30. Sociálne prostredie tiež určuje, ako sa informácie prijímajú, najmä keď umožňujú ľuďom identifikovať sa so skupinou a skryť to, čo môže poškodiť alebo odporovať názoru skupiny. Napríklad efekt rozbehnutého vlaku je založený na potrebe niekam patriť a hanbe byť odlišný. Ľudia preto veria názoru väčšiny, čím sa vytvára komora ozveny (*echo chamber*), kde sa názory navzájom posilňujú.

31. Konfirmačné skreslenie spôsobuje fragmentáciu medzi informačnými bublinami²⁸ paralelných informačných svetov, čo sťažuje existenciu spoločného priestoru na diskusiu. Všeobecná verejná sféra je v súčasnosti zredukovaná na malé, vysoko mobilizované navzájom od seba izolované bloky. Selektívna, takmer personalizovaná komunikácia, ktorá je uľahčená technológiami a sociálnymi sieťami, vytvára na seba odkazujúce mikro komunity, v rámci ktorých nemožnosť spoznať iných a vcítiť sa do ich kože podnecuje radikálnejšie názory a nedostatok dialógu, čo bráni empatii.²⁹ Tie dva elementy spoločne podporujú polarizáciu a vytváranie jednotného systému hodnôt, aspoň v rámci uzavretej skupiny, ktoré nakoniec umlčia a vylúčia disidentov. Odlišné informačné ekosystémy pri vzájomnej interakcii často narazia do seba, čo samo osebe živí polarizáciu, keďže kredibilita každého radikálneho názoru klesá v závislosti od názoru protistrany, na čo reaguje opätovným potvrdením radikálnych názorov.³⁰

32. Technológie ovplyvňujú nielen spôsob šírenia informácií, ale ovplyvňujú celý komunikačný proces zhromažďovania, uchovávanía, organizovania a šírenia informácií. Občania nie sú len prijímateľmi informácií, ale stávajú sa vplyvnými hráčmi v procese komunikácie. Ak chýbajú tradičné strážiace a regulačné subjekty, vytvárajú si vlastné zdroje informácií. V dôsledku toho množstva a diverzity informácií médiá strácajú svoj referenčný charakter a autoritu. Zmätok zdrojov a chyby, ktorých sa dopustili tradičné médiá z dôvodu spomínanej bezprostrednosti informačného procesu, urýchlili stratu ich dôveryhodnosti.³¹ V tomto ohľade sa jednotlivci a médiá často ocitajú na jednej lodi. Vytvárajú sa osobné

²⁶ Sunstein, C., Scala, A., Quattrociocchi, W. Echo Chambers on Facebook. 2016. Dostupné na: <<https://ssrn.com/abstract=2795110>> (pozreté 25/01/2018).

²⁷ Shin, Jieun, Thorson, Kjerstin. Partisan Selective Sharing: The Biased Diffusion of Fact-Checking Messages on Social Media. Journal of Communication. Vol 67, 2017. Dostupné na: <<http://onlinelibrary.wiley.com/doi/10.1111/jcom.12284/full>> (pozreté 25/01/2018).

²⁸ Parisier, Eli. The filter bubble. The Penguin Press. New York. 2011.

²⁹ Sunstein, C. R. The law of group polarization. Journal of political philosophy 10, 175 – 195 (2002).

³⁰ <<https://www.buzzfeed.com/charliewarzel/2017-year-the-internet-destroyed-shared-reality>> (pozreté 25/01/2018)

³¹ Prezident Trump využil niektoré z týchto skutočných alebo zdanlivých zlyhaní na udelenie cien falošným správam <https://www.elconfidencial.com/mundo/2018-01-18/trump-fake-news-awards-noticias-falsas-premios_1508101> (pozreté 25/1/2018). Príklad možno vidieť aj tu: <<https://theintercept.com/2017/12/09/the-u-s-media-yesterday-suffered-its-most-humiliating-debacle-in-ages-now-refuses-all-transparency-over-what-happened>> (pozreté 25/01/2018).

informačné priestory, v ktorých občania nachádzajú útočisko; tvárou v tvár záplave obsahu majú zredukovaný, zvládnuteľný, spoľahlivý a bezpečný informačný svet, v ktorom dominujú vzťahy s tými, ktorí sú im najbližšie v osobnom a pracovnom živote, ako aj z hľadiska ideologických názorov.

33. Zdieľaním informácií sa občania stávajú protagonistami komunikácie, spochybňujúc tak pridanú hodnotu masmédií. Občania internet čoraz viac využívajú ako zdroj informácií³² a nerozlišujú medzi originálnymi, vierohodnejšími zdrojmi informácií a zvyškom obsahu od rodiny a priateľov.³³ Až 79 % vidí rodinu a priateľov ako vierohodný zdroj informácií, po nich nasledujú názory vedeckých odborníkov (72 %), zamestnancov podnikov (60 %) a podnikov, ktorých služby využívajú (59 %). Informácie od novinárov (49 %), CEO (43 %), známych osobností (42 %) a celebrit (29 %) sú na konci zoznamu.³⁴

34. Dôležitosť, ktorú medziľudská komunikácia prostredníctvom sociálnych médií získava, viedla k masovému vytváraniu botov, anonymných, automatizovaných a niekedy falošných účtov, ktoré online vystupujú ako jednotlivci, a k zvýšeniu masívneho šírenia špecifických informácií zameraných na vytváranie prúdov verejnej mienky, akceptovanie alebo odmietanie ľudí a myšlienok umelým spôsobom.³⁵ Vyvolávaním dojmu, že majú širokú podporu, tieto funkcie vytvárajú efekt rozbehnutého vlaku a ostatní akceptujú myšlienky zdieľané touto zdanlivou väčšinou. Vytvára to davové (stádové) správanie, čím jednotlivci zanedbávajú svoju osobnú zodpovednosť a podrobujú sa vôli kolektívu; imitujú sa navzájom a popierajú odchýlky. Dezinformácie, najmä ak sa nachádzajú v masmédiách, sú pokladané za „vieru“, nespochybniteľný základ, ktorého popieranie znamená riziko vylúčenia.

IV. Vplyv sociálnych médií a internetu na demokraciu a volebné procesy

35. Internet dal ľuďom bezprecedentný prístup k informáciám o voľbách a umožnil im vyjadriť svoje názory, komunikovať s kandidátmi a byť aktívnou súčasťou volebnej kampane.³⁶ Najmä sociálne médiá predstavujú prevládajúce fórum pre politickú diskusiu a ako také sú zdrojom politických informácií.³⁷ Štúdie ukazujú, že narastajúci informačný tok podporovaný sociálnymi sieťami posilňuje kritické myslenie občanov voči ich vládam³⁸ a že je silná pozitívna korelácia (0.71) medzi používaním internetu a sociálnych sietí na jednej

³² 46 % občanov Európskej únie sledovalo v roku 2016 spravodajstvo na sociálnych sieťach: Správa Reuters Institute Digital News Report 2016, dostupná na:

<<http://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/Digital%2520News%2520Report%25202016.pdf>> (pozreté 25/01/2018).

³³ Podľa správy Inštitútu Reuters pre štúdium žurnalistiky na Oxfordskej univerzite „*Videl som novinky na Facebooku*“ v roku 2017 viac ako polovica Britov získavala informácie zo sociálnych sietí. A z tejto polovice si viac ako 50 % nepamätá správny zdroj informácií.

³⁴ Edelman Trust Barometer 2016.

³⁵ <<http://agendapublica.elperiodico.com/desde-rusia-bots/>>

³⁶ Volebná štúdia Rady Európy 2017, s. 7.

³⁷ Democracy Reporting International 2017.

³⁸ Gainous et al. 2016.

strane a podporou demokracie ako žiaducej formy vlády na strane druhej.³⁹ Veľa autorov okrem toho tvrdí, že rozšírené používanie internetu a sociálnych sietí poskytuje presnejšie vedomosti o záujmoch občanov a uľahčuje organizáciu veľkých spoločenských hnutí.⁴⁰

36. Napriek tomu, aj keď „*má internet moc stať sa nástrojom demokracie... jeho potenciál v tomto ohľade je ohrozený...[pretože] rovnaké technológie, ktoré uľahčujú diskusiu, vytvárajú možnosti pre cenzúru, monitorovanie online zvyklostí a jemné formovanie a manipulovanie chovania*“⁴¹, čím ohrozujú autenticitu volebného práva, rovnosť volebnej súťaže a v konečnom dôsledku schopnosť pretaviť *vôľu ľudu* do inštitucionálneho zastúpenia a vládnych rozhodnutí.⁴² Je potrebné poznamenať, že akýkoľvek neprimeraný vplyv na pravosť a slobodu volebného práva môže ovplyvniť nielen pretavenie vôle ľudu do konkrétnych činov, ale aj ochranu menšín, rovnováhu medzi ľudskými právami a možnosť vyvodit' zodpovednosť u politických strán a volených funkcionárov. Hoci tieto hrozby existovali už v aj v minulosti, vďaka sofistikovanejším metódam uľahčeným digitálnymi technológiami došlo k ich zvýšeniu.

37. Neustály a paralelný informačný tok cez viaceré platformy v skutočnom čase predstavuje veľkú výzvu pre monitorovanie správania a zdrojov počas politickej kampane. Roztrúsené a anonymné vytváranie obsahu silno bráni identifikácii a pripísaniu zodpovednosti za protiprávne konanie na internete. Zvýšené využívanie *botov* a *trollov* na vedenie diskusií na sociálnych sieťach, ako aj masívne šírenie falošných informácií vážne znižujú rovnosť vo volebnej súťaži a umožňujú externým subjektom manipulovať s diskusiou a volebnými preferenciami.⁴³ Algoritmy, ktorými sa riadia vyhľadávače a sociálne médiá, môžu navyše podporovať čiastočné a niekedy aj iluzórne chápanie politiky a demokracie.⁴⁴

38. Vplyv digitálneho prostredia na voľby bol zdôraznený kontroverziami po referende o britskom brexite a prezidentských voľbách v USA v roku 2016. Obmedzili sa pravidlá a regulácia platenej reklamy; osobné údaje voličov sa zbierali a spracovali na volebné účely bez ich súhlasu a právneho základu; politická komunikácia smerovala na neregulované sociálne médiá bez pravidiel spravodlivého mediálneho pokrytia. Tieto aspekty spochybnili ustanovené inštitúcie a zásady regulácie volebnej komunikácie, akými sú sloboda združovania, obmedzenie výdavkov a regulácia politickej reklamy⁴⁵, a oslabili schopnosť súčasných regulatívnych režimov zachovať rovnaké podmienky vo volebnej komunikácii. Digitálne prostredie predstavovalo hrozbu pre voľby a vytváralo potenciál pre vznik korupcie.

39. Reorganizácia komunikácie na internete a nové spôsoby prenosu politických odkazov voličom umožnili, aby sa nepravdivé a/alebo škodlivé informácie „*šírili medzi potenciálnymi*

³⁹ Basco 2018.

⁴⁰ Castells 2011; Metaxas and Mustafaraj 2012; Cohen et al. 2012; Európska únia 2015.

⁴¹ Laidlaw 2015, s. 1.

⁴² Porov. Volebná štúdia Rady Európy 2017, s. 7 – 9. Pozri tiež Tambini 2018, s. 265 – 293.

⁴³ Quintana 2016; Fidler 2017.

⁴⁴ Van Dijck 2013; McChesney 2013.

⁴⁵ Volebná štúdia Rady Európy 2017, s. 13.

voličmi v bezprecedentnom rozsahu bez akéhokoľvek dohľadu alebo vyvrátenia“.⁴⁶ To viedlo do určitej miery k *informačnému zmätku*, ktorý môže mať tieto tri rôzne formy:

- nepravdivé informácie (*mis-information*), teda zdieľanie nepravdivých informácií, ale bez úmyslu spôsobiť tým ujmu;
- zavádzajúce informácie (*dis-information*), teda vedomé šírenie nepravdivých informácií s úmyslom uškodiť; a
- škodlivé informácie (*mal-information*), teda autentické informácie šírené s úmyslom spôsobiť ujmu, často zverejnením informácií, ktoré majú zostať súkromné.⁴⁷

40. V určitých prípadoch boli *strategicky* šírené nepravdivé informácie s cieľom *ovplyvniť výsledky volieb*. Je zdokumentované, že *kybernetickými skupinami* na internete sú často *vládne, vojenské alebo politické stránicke tímy odhodlané manipulovať s verejnou mienkou* prostredníctvom sociálnych médií. Organizovaná *manipulácia cez sociálne siete* sa prvýkrát objavila v roku 2010, a do roku 2017 existujú podrobnosti o takých organizáciách v 28 krajinách.⁴⁸

41. Nielen sociálne médiá, ale aj vyhľadávače môžu manipulovať informáciami, či už úmyselne alebo neúmyselne, a tak skresľovať výsledky volieb v prospech konkrétneho politického názoru. Nedávne výskumy ukazujú, že manipulácia týchto poskytovateľov výsledkami vyhľadania môže vytvoriť takzvaný *efekt manipulácie s vyhľadávačmi*, ktorý môže v niektorých demografických skupinách posunúť volebné preferencie nerozhodnutých voličov o 20 alebo dokonca viac percent.⁴⁹

42. Ide o prípady, v ktorých štátne agentúry nasadili na šírenie vládnych názorov a kritiky na sociálnych sieťach tímy „*tvorcov názorov*“, alebo o prípad spoločnosti Cambridge Analytica, ktorá je vyšetrovaná pre údajné získanie a použitie súkromných dát 50 miliónov používateľov Facebooku v prezidentských voľbách v roku 2017 v USA a referende o britskom brexite.⁵⁰ Na rozdiel od priamych spôsobov cenzúry, ako je blokovanie webových stránok alebo zatýkanie kvôli aktivite na internete, manipulácia s online obsahom je ťažko zistiteľná a ešte ťažšie poraziteľná vzhľadom na jej rozšírenú povahu a veľký počet ľudí a botov zamestnaných na tento účel.

43. Keďže ciele správy sa nedostávajú k verejnosti, ale len ku vybraným skupinám alebo jednotlivcom, a nie sú podrobené žiadnemu dohľadu ani novinárskej kontrole, politickí kandidáti a strany môžu dávať rôzne prísľuby rôznym ľuďom, pričom svoje politické ciele delia na samostatné, nie vždy nevyhnutne zlučiteľné ciele. Výskumy ukazujú zvýšenie

⁴⁶ Volebná štúdia Rady Európy 2017, s. 15.

⁴⁷ Správa Rady Európy o informačnom zmätku 2017.

⁴⁸ Bradshaw & Howard, 2017. Pozri aj správu Freedom House 2017, podľa ktorej manipulačné a dezinformačné taktiky zohrali v priebehu roka dôležitú úlohu vo voľbách v najmenej 17 ďalších krajinách. Podľa organizácie Communications Security Establishment (CSE) kanadskej vlády len v roku 2017 bol demokratický proces 13 % krajín, v ktorých sa konali federálne voľby, napadnutý hackerskými útokmi, počítačovou kriminalitou a dokonca aj verejným alebo súkromným politickým subjektom s úmyslom manipulovať s informáciami, ovplyvniť verejnú mienku alebo dokonca destabilizovať demokratické inštitúcie.

⁴⁹ Epstein & Robertson, 2015.

⁵⁰ McCauley, P. and Schecter, A., 2018, BBC, 2018.

digitálnu kampaň v oblasti takzvaných „rozdeľujúcich“ tém, teda tých, ktoré sú veľmi kontroverzné alebo majú schopnosť mobilizovať voličov (prísluhovalecká politika, sociálne otázky, manželstvo osôb rovnakého pohlavia a pod.). Cílené správy sa snažia optimalizovať zdroje na volebnú kampaň, a preto sa vo veľkej miere zameriavajú na nestálych alebo nerozhodnutých voličov. Tí, na ktorých tieto správy nie sú zamerané, sú pripravení o celé spektrum politických vyhlásení, čo zase vytvára nerovnosť medzi voličmi, ktorí sa nemôžu rozhodovať na základe rovnakých informácií.

44. Štáty a súkromní aktéri po celom svete môžu využívať digitálne technológie na porušovanie ľudských práv a dokonca ako vojenské nástroje útoku na krajiny a ich inštitúcie prostredníctvom malwarov, ransomwarov, spywarov a iných sofistikovaných programov.⁵¹ Označuje sa to ako „kybernetická vojna“ a v minulosti sa úspešne využívala na zničenie štátnych projektov a systémov, napríklad útok Stuxnet na jadrovú elektrárňu Natanz (Irán).⁵²

45. Kybernetické nástroje sú okrem ich dostupnosti, prepracovanosti a prítlačivosti pre verejnosť vsadené do prostredia bez hraníc. To, čo bolo legálne vytvorené podľa vnútroštátneho práva, možno dnes ilegálne premiestniť do inej jurisdikcie a *vice versa*. S narastajúcim využívaním *cloud computingu* sa online informácie ešte viac roztrieštili, a preto je mimoriadne ťažké identifikovať ich pôvod a autorstvo. Počítačová kriminalita a kybernetické hrozby pôsobia mimo hraníc akejkoľvek vnútroštátnej jurisdikcie. Táto situácia prináša viaceré ťažkosti pre vyšetrovanie a trestné stíhanie; preto je snaha pristúpiť k tomuto fenoménu z nadnárodnej perspektívy.⁵³

46. Dnes sme svedkami súčasného šírenia informácií a informačného znečistenia (*information pollution*) na globálnej úrovni. Internetové služby obohatili a diverzifikovali zdroje spravodajstva, čím uľahčili prístup jednotlivcov k informáciám a ich rozhodovanie o najdôležitejších otázkach demokracie, najmä o voľbe zákonodarcu. Nová éra informačného zmätku však súčasne narušuje komunikačný ekosystém do takej miery, v ktorej už vážne zaťažuje rozhodovanie voličov, ktorí sú podvádzaní, manipulovaní a zasypaní nepravdivými informáciami, ktoré sú vytvárané s úmyslom ovplyvniť ich hlasovanie. Také prostredie by mohlo narušiť výkon práva na slobodné voľby a vážne ohroziť fungovanie demokratických režimov.

47. Digitálne technológie zmenili spôsob, akým spoločnosti pretavia vôľu ľudí do volieb a zastúpenia, a do veľkej miery zmenili politickú kampaň. Hoci internet podporuje niektoré aspekty demokratickej súťaže, taktiež ich brzdí. Celosvetová prítomnosť digitálnych technológií presunula éru demokratickej diskusie do virtuálneho sveta, čo vyvolalo veľa otázok o ich vplyve na účasť voličov a potrebe skúmať a regulovať spoločenské správanie online. Okrem toho je potrebné zabezpečiť adekvátnu ochranu pred kybernetickou vojnou.

⁵¹ Quintana 2016.

⁵² Quintana 2016; Mecinas Montiel 2016, p. 404, 418 – 419.

⁵³ Davara 2003; Salt 2017 p. 520 – 521.

V. Relevantné európske a medzinárodné štandardy a nástroje

48. Uvedené javy zasahujú do viacerých základných práv chránených na európskej a univerzálnej úrovni niekoľkými medzinárodnými listinami a dohovormi, akými sú napríklad Všeobecná deklarácia ľudských práv, Medzinárodný pakt o občianskych a politických právach, Americká deklarácia práv a povinnosti človeka, Americký dohovor o ľudských právach, Charta základných práv Európskej únie a Európsky dohovor o ľudských právach (ďalej len „EDLP“).

A. Právo na slobodné voľby a sloboda prejavu

1. Základné princípy

49. Podľa EDLP, ako ho interpretuje Európsky súd pre ľudské práva (ďalej aj „ESLP“), majú členské štáty Rady Európy povinnosť zabezpečiť práva a slobody pre každého, kto patrí do ich jurisdikcie. Právo na slobodné voľby zakotvené v čl. 3 dodatkového protokolu k EDLP nie je len objektívnym a zásadným princípom každej demokratickej spoločnosti, ale aj základným individuálnym právom, na ktoré sa môže každý občan spoľahnúť a ktoré najúčinnejšie podporuje „skutočnú demokraciu“.⁵⁴

50. Právo na slobodné voľby zahŕňa právo voliť a právo byť volený.⁵⁵ Okrem toho to pre členské štáty znamená aj pozitívny záväzok zabezpečiť podmienky, za ktorých si ľudia môžu slobodne vytvárať a vyjadrovať svoje názory a vyberať si svojich zástupcov. Tento záväzok je mimoriadne dôležitý vzhľadom na (ne)narušený komunikačný kontext volieb. Právo na slobodné voľby stanovuje, že členské štáty „sa zaväzujú organizovať slobodné voľby v primeraných intervaloch tajným hlasovaním za podmienok, ktoré zabezpečia slobodné vyjadrenie názoru ľudí pri voľbe zákonodarného zboru“, čo naznačuje, že právo na slobodné voľby a sloboda prejavu sú navzájom nevyhnutnými predpokladmi.⁵⁶ Túto interpretáciu potvrdil aj ESLP, keď uviedol, že „slobodné voľby a sloboda prejavu, najmä sloboda politickej diskusie, spoločne tvoria základ akéhokoľvek demokratického systému“.⁵⁷

51. Európsky súd pre ľudské práva ďalej uviedol, že obe práva sú navzájom prepojené a pôsobia tak, aby sa navzájom posilňovali, pričom sloboda prejavu je jednou z podmienok potrebných na zabezpečenie slobodných volieb. Aby boli práva zaručené čl. 3 dodatkového protokolu účinné, ochrana sa vzťahuje aj na predvolebnú kampaň. Z tohto dôvodu je v období pred voľbami obzvlášť dôležité, aby sa názory a informácie všetkých druhov mohli voľne

⁵⁴ Thorgeirsdóttir, Herdis (2005), Žurnalistika hodná tohto označenia: Kladná strana článku 10 EDLP, Kluwer Law International. Lécuyer, 2014. Pozri Mathieu-Mohin a Clerfayt proti Belgicku, sťažnosť č. 9267/81 (ESLP, 2. marca 1987); Ždanoka proti Lotyšsku, sťažnosť č. 58278/00 (ESLP, 16. marca 2006). Pozri tiež ESLP, 2018, „Príručka k článku 3 dodatkového protokolu k Dohovoru o ochrane ľudských právach a základných slobôd – Právo na slobodné voľby“, dostupné na:

<https://www.echr.coe.int/Documents/Guide_Art_3_Protocol_1_ENG.pdf>.

⁵⁵ Mathieu-Mohin a Clerfayt proti Belgicku; Ždanoka proti Lotyšsku.

⁵⁶ Plaizier, 2018.

⁵⁷ Bowman proti Spojenému kráľovstvu, sťažnosť č. 24839/94 (ESLP z 19. februára 1998), ods. 42.

široť.⁵⁸ Podľa EŠLP majú členské štáty pozitívny záväzok zabezpečiť efektívnu slobodu prejavu: EŠLP požaduje vytvoriť priaznivé prostredie pre účasť všetkých dotknutých osôb na verejnej diskusii, ktorá im umožní bez obáv vyjadrovať svoje názory a nápady. Štát sa musí nielen zdržať akéhokoľvek zasahovania do slobody prejavu jednotlivca, ale musí mať aj pozitívny záväzok chrániť jeho právo na slobodu prejavu pred útokmi vrátane útokov zo strany súkromných osôb.⁵⁹

52. Európsky súd pre ľudské práva uznal, že za určitých okolností môžu byť práva podľa čl. 10 EŠLP a čl. 3 dodatkového protokolu v rozpore a že v období pred voľbami alebo počas nich možno považovať za nevyhnutné zaviesť určité obmedzenia slobody prejavu, ktoré by inak neboli prijateľné, aby sa tak zabezpečilo „slobodné vyjadrenie názoru ľudí pri voľbe zákonodarného zboru“. ⁶⁰ Uznal, že pri hľadaní rovnováhy medzi týmito dvoma právami majú členské štáty priestor na voľnú úvahu, ako ho spravidla majú v súvislosti s organizáciou ich volebných systémov. Súčasne zdôraznil, že akékoľvek obmedzenia slobody prejavu musia byť úmerné legitímnemu cieľu, ktorý sledujú, a potrebné v demokratickej spoločnosti. Uviedol napríklad, že čl. 10 EŠLP ako taký nezakazuje diskusiu ani šírenie získaných informácií, aj keď existuje silné podozrenie, že tieto informácie nemusia byť pravdivé.⁶¹ Na druhej strane je potrebné upozorniť na rozhodnutie EŠLP týkajúce sa práva mimovládnej organizácie na vytváranie politických reklám v rozhlase a televízii, v ktorej sa vyvážilo právo sťažujúcej sa mimovládnej organizácie na šírenie informácií a myšlienok všeobecného záujmu, ktoré je verejnosť oprávnená dostávať, s vôľou orgánov chrániť demokratickú diskusiu a volebný proces pred deformáciou silnými finančnými skupinami s ľahším prístupom k vplyvným médiám.⁶² EŠLP uznal, že tieto skupiny by mohli získať konkurenčné výhody v oblasti platenej reklamy a obmedziť tak slobodnú a pluralistickú diskusiu, ktorej konečným garantom je štát. V dôsledku toho je na udržanie slobodnej a pluralistickej diskusie potrebné vziať do úvahy riziko nerovnováhy medzi politickými silami v politickej súťaži.

53. Práva podľa čl. 3 dodatkového protokolu nie sú ani absolútne: existuje priestor pre „predpokladané obmedzenia“⁶³ a členským štátom treba v tejto oblasti poskytnúť širokú mieru voľnej úvahy. Pri skúmaní súladu s čl. 3 dodatkového protokolu sa EŠLP zameral predovšetkým na dve kritériá: či došlo k svojvôli alebo disproporcionalite a či obmedzenie zasahovalo do slobodného vyjadrovania názoru ľudí.⁶⁴

⁵⁸ Bowman proti Spojenému kráľovstvu, sťažnosť č. 24839/94 (EŠLP, 19. februára 1998); Orlovskaya Iskra proti Rusku, sťažnosť č. 42911/08 (EŠLP, 21. februára 2017). Počas európskych volieb v roku 2019 povolil Facebook politické reklamy pre Európsky parlament v celej EÚ: <<https://www.politico.eu/article/facebook-allows-eu-wide-political-ads-for-european-parlament/>>; <<https://techcrunch.com/2019/04/26/facebook-says-its-open-to-advertising-u-turn-for-the-eu-elections-enabling-cross-border-campaigns/?renderMode=ie11>>.

⁵⁹ Dink proti Turecku, sťažnosť č. 2668/07, 6102/08, 30079/08, 7072/09 a 7124/09 (EŠLP, 14. septembra 2010).

⁶⁰ Bowman proti Spojenému kráľovstvu, sťažnosť č. 24839/94 (EŠLP, 19. februára 1998); Orlovskaya Iskra proti Rusku, sťažnosť č. 42911/08 (EŠLP, 21. februára 2017).

⁶¹ Salov proti Ukrajine, sťažnosť č. 655118/01 (EŠLP, 6. septembra 2005).

⁶² Animal Defenders International proti Spojenému kráľovstvu, sťažnosť č. 48876/08 (EŠLP, 2013).

⁶³ Článok 3 nie je obmedzený konkrétnym zoznamom „legitímnych cieľov“, ako sú tie vymenované v čl. 8 až 11 EŠLP, a EŠLP neuplatňuje tradičné testy „nevyhnutnosti“ alebo „naliehavej spoločenskej potreby“, ktoré sa používajú v kontexte čl. 8 až 11 EŠLP.

⁶⁴ Mathieu-Mohin a Clerfayt proti Belgicku; Ždanoka proti Lotyšsku.

54. Európsky súd pre ľudské práva uznal právo fyzických osôb na prístup na internet, pretože vo svojom rozsudku proti hromadnému blokovaniu online obsahu uviedol, že *„internet sa v súčasnosti stal jedným z hlavných spôsobov uplatňovania práva na slobodu prejavu a informácií, pretože poskytuje základné nástroje účasti na aktivitách a diskusiách týkajúcich sa politických otázok a otázok všeobecného záujmu“*.⁶⁵ Uvádza sa v ňom, že čl. 10 EDLP zaručuje slobodu prejavu, prijímania a šírenia informácií a myšlienok bez ohľadu na hranice. Blokovanie prístupu na webové stránky hostiteľa a webové stránky tretích strán okrem webových stránok, ktorých sa týka konanie, spôsobuje, že mnohé informácie sú neprístupné, a tým sa obmedzujú práva používateľov internetu. Európsky súd pre ľudské práva ďalej objasnil, že obmedzenie prístupu k zdroju informácií je zlučiteľné s dohovorom iba vtedy, ak existuje prísny právny rámec, ktorý poskytuje záruku súdneho preskúmania s cieľom zabrániť možnému zneužívaniu.

55. Európsky súd pre ľudské práva navyše uznal, že *«vzhľadom na dôležitú úlohu, ktorú internet zohráva pri zlepšovaní prístupu verejnosti k spravodajstvu a uľahčovaní šírenia informácií (pozri Delfi AS proti Estónsku [GC], ods. 133, 2015), funkciu bloggerov a používateľov sociálnych médií možno v súvislosti s ochranou čl. 10 prirovnať k „verejnému strážnemu psovi“*».⁶⁶ Táto ochrana sa môže rozšíriť na prístup k (verejne prístupným) informáciám, ak slúžia na uplatňovanie práva na slobodu prejavu: informácie, ku ktorým sa požaduje prístup, musia spĺňať test verejného záujmu. Ako však už bolo uvedené, čl. 10 EDLP nezaručuje neobmedzenú slobodu prejavu; obmedzenia môžu byť povolené napríklad s cieľom ochrany práva na súkromný život (čl. 8 EDLP), ak sú použité prostriedky primerané sledovanému cieľu.

56. Základné princípy týkajúce sa volieb sú ďalej vyjadrené v Kódexe dobrej praxe vo volebných veciach, ktorý prijala Benátska komisia v roku 2002.⁶⁷ Okrem iného zahŕňajú:

- rovnosť príležitostí pre strany a kandidátov;
- neutrálny prístup štátnych orgánov, pokiaľ ide o volebnú kampaň, mediálne krytie a verejné financovanie strán a kandidátov;
- rovnosť príležitostí môže byť skôr proporcionálna než striktná, a platí najmä pre „vysielenie v rádiu a televízii“;
- v súlade so slobodou prejavu by zákonné ustanovenia mali s ohľadom na volebnú kampaň zaistiť minimálny prístup k audiovizuálnym médiám v súkromnom vlastníctve a reklame pre všetkých kandidátov vo voľbách;
- financovanie kampane musí byť transparentné;
- rovnosť príležitostí môže viesť k obmedzeniu výdavkov politických strán, najmä na reklamu.

⁶⁵ Ahmet Yıldırım proti Turecku, sťažnosť č. 3111/10 (ESLP, 18. december 2012). Pozri tiež Cengiz a ďalší proti Turecku, sťažnosť č. 48226/10 a 14027/11 (ESLP, 1. decembra 2015).

⁶⁶ Magyar Helsinki Bizottság proti Maďarsku, sťažnosť č. 18030/11 (ESLP, 8. novembra 2016). Pozri tiež Animal Defenders International proti Spojenému kráľovstvu, sťažnosť č. 48876/08 (ECHR, 2013).

⁶⁷ CDL-AD(2002)023rev-cor. Pozri tiež Spoločné usmernenia pre prevenciu pred zneužívaním administratívnych zdrojov a reakciu naň počas volebných procesov (CDL-AD(2016)004), ktoré opätovne potvrdzujú princípy neutrality a rovnosti príležitostí týkajúce sa prístupu k verejnoprávnym médiám.

57. Používanie metód elektronického hlasovania spôsobuje konkrétne problémy so zreteľom na základné volebné princípy. Rada Európy je naďalej jedinou organizáciou, ktorá stanovila medzivládne štandardy v oblasti elektronického hlasovania. Odporúčanie Výboru ministrov Rec(2004)11, ktoré sa používa vo vnútroštátnej judikatúre aj nečlenských štátoch, a je využívané aj inými relevantnými medzinárodnými aktérmi, bolo nedávno aktualizované: nové odporúčanie – ktoré pozostáva z odporúčania CM/Rec(2017)5 o štandardoch pre elektronické hlasovanie, usmernení k implementácii ustanovení odporúčaní s konkrétnymi požiadavkami a dôvodovej správy – bolo navrhnuté ako vylepšenie dokumentu Rec(2004)11 a zaoberá sa najdôležitejšou časťou volebnej technológie, konkrétne elektronickým hlasovaním, teda použitím elektronických prostriedkov na odovzdanie a sčítanie hlasov. Do tejto kategórie patria systémy, ako sú hlasovacie zariadenia s priamym záznamom elektroniky (DRE), hlasovacie lístky, digitálne perá a internetové hlasovacie systémy. Cieľom odporúčania je zabezpečiť, aby elektronické hlasovanie zaručovalo všeobecné, rovnaké, slobodné a tajné volebné právo, a obsahuje ustanovenia o organizačných požiadavkách, zodpovednosti, spoľahlivosti a zabezpečení systému.

58. V tejto súvislosti sa upriamuje pozornosť aj na príslušné dokumenty Benátskej komisie. Kódex dobrej praxe vo volebných veciach jasne uvádza, že „*elektronické hlasovanie by sa malo používať iba vtedy, ak je bezpečné a spoľahlivé; voliči by predovšetkým mali mať možnosť získať potvrdenie svojich hlasov a v prípade potreby ich opraviť, pričom sa musí rešpektovať tajné volebné právo; systém musí byť transparentný*“.⁶⁸

2. Financovanie volebných kampaní

59. Existuje množstvo spoločne dohodnutých štandardov pre boj s korupciou pri financovaní politických strán a volebných kampaní (ktoré sa odporúčajú uplatňovať aj na subjekty súvisiace s politickými stranami, ako sú politické nadácie). Boli stanovené v odporúčaní Parlamentného zhromaždenia 1516(2001) o financovaní politických strán a následne v odporúčaní Výboru ministrov Rec(2003)4 o spoločných pravidlách boja proti korupcii pri financovaní politických strán a volebných kampaní. Štandardy, ktoré sa majú uplatňovať, zahŕňajú (a.) požiadavky na *primeranú rovnováhu* medzi verejným a súkromným financovaním politických strán; (b.) používanie *spravodlivých kritérií* na rozdeľovanie štátnych príspevkov stranám; (c.) zavedenie prísnych pravidiel týkajúcich sa súkromného darcovstva *vrátane zákazu alebo obmedzenia príspevkov* od zahraničných darcov, náboženských organizácií a obmedzenie korporácií a anonymných darov; (d.) *obmedzenia výdavkov strán* spojených s volebnými kampaňami; (e.) ustanovenia o *transparentnosti* darov a výdavkov politických strán; a (f.) zriadenie *nezávislého orgánu* a zmysluplných sankcií pre tých, ktorí porušujú pravidlá.

60. Podobne v usmerneniach k regulácii politických strán⁶⁹ Benátska komisia a OBSE/ODIHR stanovili, že regulácia volebných kampaní by mala

⁶⁸ Kódex dobrej praxe vo volebných záležitostiach, CDL-AD(2002)023rev-cor, oddiel I.3.2.IV.; pozri aj odseky 42 – 44 dôvodovej správy. Pozri tiež Správu Benátskej komisie o kompatibilite hlasovania na diaľku a elektronického hlasovania so štandardmi Rady Európy, CDL-AD(2004)12.

⁶⁹ CDL-AD(2010)024, s. 35, ods. 159.

- predchádzať nevhodnému vplyvu (a zaistiť nezávislosť strán) na politické rozhodnutia prostredníctvom peňažných darov;
- zaistiť transparentnosť výdavkov politických strán a
- zaistiť, aby všetky politické strany mali možnosť súťažiť v súlade s princípom rovnosti príležitostí.

61. Aby sa dosiahli tieto ciele, „*hlavnými spôsobmi, akými je regulovaná komunikácia kampane, sú volebné zákony vrátane obmedzení výdavkov a kontrol financovania kampane; dotácie na kampaňovú komunikáciu; moratória pred hlasovaním; regulácie médií, najmä licencie na vysielania; pravidiel politickej reklamy vrátane neustrannosti, dotácií a voľného vysielacieho času; a samoregulácie a novinárskej etiky*“.⁷⁰

62. Stanovili sa prísne štandardy s cieľom „*chrániť integritu volieb, zaistiť, aby boli slobodné a spravodlivé a aby sa zabránilo ich zneužitiu pre záujmy úzkej skupiny ľudí*“.⁷¹ Legislatívne opatrenia prijaté členskými štátmi a nariadenia však boli implementované so zameraním na voľby usporiadané offline.⁷² Preto sa ich použiteľnosť a účinnosť v časoch digitálnej politickej reklamy ukázala byť výrazne obmedzená. Ako už bolo spomenuté, v posledných rokoch museli politickí činitelia, vlády a občianska spoločnosť čeliť problému *presadzovania súčasných predpisov na internete*, pričom uplatniteľnosť existujúcej právnej úpravy volebnej kampane nie je výnimkou.

63. Legislatívne limity financovania kampane boli spochybnené novými formami digitálnej reklamy, ktoré sú vo svojej podstate menej transparentné ako ich analógoví predchodcovia, čím podkopávajú existujúce definície a obmedzenia založené na konkrétnych typoch médií. Zabezpečenie proti korupcii založené na metódach výpočtu výdavkov a kategóriách nahlasovania výdavkov na tradičných mediálnych kanáloch stratilo svoj význam, pretože politické kampane sa presunuli na internet. Výsledkom je, že aj absolútne limity výdavkov na vysielanie nadobúdajú čoraz menší význam, zatiaľ čo nariadenia o transparentnosti zamerané na informovanie občanov o sumách a metódach financovania kampane v digitálnom svete, ktorý nepozná hranice, sú ťažké, ak nie dokonca nemožné.⁷³

3. Politický prejav a medializácia volebných kampaní

64. Aj keď je „sloboda prejavu hybnou silou demokracie“, všetky právne systémy majú v súčasnosti stanovené pravidlá financovania politickej kampane, limity a povinnosť transparentnosti. V individuálnej sfére sa môže stať, že si prejav zaslúži ochranu bez ohľadu na obsah, ale to sa nevzťahuje na kampaň. Prevažná väčšina, ak nie dokonca všetky ústavné systémy stanovujú limity slobody prejavu počas volebnej kampane: napríklad obdobie moratória, ochranná zóna vo volebných miestnostiach (*cordon sanitaire*), pravidlá financovania kampane a povinnosť transparentnosti. Všetky obmedzenia kampane, dokonca aj tie, ktoré podporujú transparentnosť, treba v prvom rade chápať ako zásah, ktorý musí byť

⁷⁰ Volebná štúdia Rady Európy 2017, s. 9.

⁷¹ Volebná štúdia Rady Európy 2017, s. 9.

⁷² V tejto súvislosti je pri zmene rozsahu financovania volebných kampaní čoraz dôležitejšie využívanie kampaní hromadného financovania (*crowd funding*), najmä prostredníctvom internetu.

⁷³ Volebná štúdia Rady Európy 2017, s. 20 – 21.

v európskych systémoch odôvodnený testom nevyhnutnosti a proporcionality. Právna úprava zverejňovania politickej reklamy sa zdá byť právne možná a môže mať formu a) regulácie transparentnosti, a nie obsahu, b) regulácie politickej kampane, c) regulácie, ktorá je zameraná buď na voľby alebo na prieskum verejnej mienky, alebo je prepojená s mechanizmami financovania alebo je zameraná na identifikáciu pôvodu mimo politického prostredia. Napriek ťažkostiam pri definovaní určitých pojmov je zrejmé, že je možné navrhnúť režim uplatniteľný pre tradičnú tlač, vysielanie alebo plagátovú reklamu. Čo je však v digitálnej sfére publikácia a kto je vydavateľ? Kedy je správa „reklamou“, a nie individuálnym prejavom názoru, ktorý „sa stáva virálnym“?

65. Európsky súd pre ľudské práva jasne poukázal na zodpovednosť štátu za predchádzanie nerovnosti v mediálnom pokrytí počas volieb⁷⁴, online aj offline, pričom však existujú výrazné rozdiely v *vplyve* tradičných a nových médií.⁷⁵ Teraz je výzvou tieto rozdiely presne definovať – zistiť, či už došlo k „dostatočne závažnému presunu vplyvu“.⁷⁶ Kľúčovým pre odhad tohto „presunu“ je určiť, či sa má pozitívna zodpovednosť štátu za zabezpečenie rovnakého kontaktu s politickými stranami a kandidátmi aplikovať aj na nových sprostredkovateľov informácií a aký spôsobom.

66. Štandardy Rady Európy a iné nástroje v tejto oblasti sa snažia poskytnúť *komunikačný kontext vedúci ku uplatneniu práva na slobodné voľby*. Odrážajú pozitívne záväzky štátu na zaistenie toho, že občania dostávajú nevyhnutné a pravdivé informácie o politických stranách pre podporu ich demokratického rozhodnutia voliť svojich zástupcov.

67. Odporúčanie CM/Rec(2007)15⁷⁷ sa vzťahuje na širokú škálu médií bez ohľadu na prostriedky a technológie používané na šírenie ich obsahu a poskytuje usmernenia pre bezplatné a nezávislé mediálne pokrytie politických kampaní s vyššími štandardmi platnými pre verejnoprávne médiá. Odporúčanie obsahuje niekoľko usmernení zameraných na zabezpečenie zodpovedného, presného a spravodlivého pokrytia volebných kampaní; verejnoprávne médiá však nesú osobitnú zodpovednosť za pokrytie volieb „*spravodlivým, vyváženým a nestranným spôsobom bez diskriminácie konkrétnej politickej strany alebo kandidáta*“. Pokiaľ ide o celkové príležitosti politických strán a kandidátov osloviť voličov, odporúčanie ponecháva na rozhodnutí jednotlivých členských štátov, či povolia platenú politickú reklamu. Ak však strany majú možnosť nákupu reklamného priestoru na účely volebnej kampane, musia to byť schopné urobiť za rovnakých podmienok a platobných sadzieb.

68. Odporúčanie okrem toho stanovuje niekoľko všeobecných požiadaviek na zabezpečenie spravodlivých a transparentných kampaní; napríklad *právo na odpoveď* alebo rovnocenné opravné prostriedky, ktoré by mali byť k dispozícii kandidátom a/alebo politickým stranám, aby im umožnili účinne reagovať na akékoľvek vyhlásenia, ktoré by mohli vyvolať predsudky počas relatívne krátkeho trvania volebných kampaní. *Spôsoby šírenia prieskumov verejnej*

⁷⁴ Komunistická strana Ruska a iní proti Rusku, sťažnosť č. 29400/05 (ESLP, 19. júna 2012).

⁷⁵ Animal Defenders International proti Spojenému kráľovstvu, sťažnosť č. 48876/08 (ESLP, 22. apríla 2013).

⁷⁶ Ibidem, ods. 119.

⁷⁷ Odporúčanie CM/Rec(2007)15 Výboru ministrov členským štátom o opatreniach týkajúcich sa mediálneho pokrytia volebných kampaní.

mienky by mali poskytnúť verejnosti dostatočné informácie na posúdenie hodnoty týchto prieskumov, pričom potenciálny vplyv volebných oznamov tesne pred voľbami je zmiernený ustanoveniami, ktoré umožňujú členským štátom zväziť zákaz ich šírenia v deň predchádzajúci hlasovaniu („deň na premyslenie“). Odporúčanie okrem toho vysvetľuje *požiadavky na transparentnosť* plateného reklamného obsahu a *vlastníctvo* médií (tieto požiadavky sú podrobne uvedené v odporúčaní CM/Rec(2018)1)⁷⁸. Už uvedené usmernenia sa zameriavajú predovšetkým na lineárne vysielacie (súkromné a verejné) médiá s rozšírením o nelineárne audiovizuálne služby verejnoprávných médií. S posunom politickej kampane do online sociálnych médií za posledné desaťročie sa však ukazuje, že ich účinnosť sa znižuje.

69. Tento posun sa odráža aj v odporúčaní CM/Rec(2018)1, ktoré jasne poukazuje na potenciálne znepokojujúci vplyv, ktorý môže mať kontrola online platformy nad tokom, dostupnosťou, vyhľadateľnosťou a prístupnosťou informácií na *pluralitu médií*. Selektívne vystavovanie sa mediálnym obsahom, ktoré môže viesť k potenciálnej spoločenskej fragmentácii, sa považuje za jednu z veľkých obáv, najmä v čase volieb. Odporúčanie preto vyzýva štáty, aby splnili svoju pozitívnu zodpovednosť a vystupovali ako konečný garant mediálneho pluralizmu *zabezpečením plurality v celom rozsahu multimediálneho ekosystému*.

70. Tento výklad je posilnený odporúčaním CM/Rec(2018)2⁷⁹, ktoré sa zaoberá úlohami a zodpovednosťou internetových sprostredkovateľov vo vzťahu k ich používateľom a členským štátom, pričom náležite zohľadňuje ich rastúcu moc v oblasti komunikácie a šírenia informácií. Potenciálnu spoluzodpovednosť sprostredkovateľov za obsah, ktorý uskladňujú – ak nekonajú rýchlo a neobmedzia prístup k obsahu alebo službám hneď, ako sa dozvedia o ich nezákonnej povahe (v súlade so zásadami zákonnosti, nevyhnutnosti a proporcionality) – treba vnímať v tomto kontexte. Medzitým by sprostredkovatelia nemali mať žiadnu všeobecnú povinnosť monitorovať obsah, ku ktorému iba poskytujú prístup alebo ktorý prenášajú alebo uskladňujú. V tejto súvislosti sa upriamuje pozornosť aj na odporúčanie CM/Rec(2016)1, ktoré vyzýva členské štáty, aby pri vytváraní vnútroštátnych právnych rámcov zabezpečili zásadu neutrality siete s cieľom zaistiť ochranu práva na slobodu prejavu a prístupu k informáciám a právo na súkromie.⁸⁰

71. Výbor ministrov vo svojom vyhlásení Decl(13/02/2019)1 z 13. februára 2019⁸¹ o manipulačných schopnostiach algoritmickej procesov zdôraznil „*potrebu posúdiť regulačné rámce súvisiace s politickou komunikáciou a volebnými procesmi s cieľom zaistiť spravodlivosť a integritu volieb offline aj online v súlade so stanovenými zásadami. Predovšetkým by sa malo dbať na to, aby voliči mali prístup k porovnateľným informáciám v rámci celého politického spektra, aby si voliči boli vedomí nebezpečenstva politického redliningu, ku ktorému dochádza vtedy, keď sa politické kampane obmedzia na tých, ktorí sa*

⁷⁸ Odporúčanie CM/Rec(2018)1 o pluralite médií a transparentnosti vlastníctva médií.

⁷⁹ Odporúčanie CM/Rec(2018)2 o úlohách a zodpovednostiach internetových sprostredkovateľov.

⁸⁰ Odporúčanie CM/Rec(2016)1 o ochrane a podpore práva na slobodu prejavu a práva na súkromný život v súvislosti so sieťou.

⁸¹ Vyhlásenie Decl(13/02/2019)1 o manipulačných schopnostiach algoritmickej procesov, <https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b>.

dajú najľahšie ovplyvniť, a aby voliči boli účinne chránení pred nekalými praktikami a manipuláciou.“.

72. Parlamentné zhromaždenie vo svojej rezolúcii 2254(2019) o slobode médií ako podmienke demokratických volieb⁸² vyzvalo členské štáty, aby implementovali účinné stratégie na ochranu volebného procesu pred manipuláciou s informáciami a neprimeranou propagandou prostredníctvom sociálnych médií. Rezolúcia navrhla opatrenia, akými sú vývoj konkrétnych regulačných rámcov pre internetový obsah v čase volieb a zavedenie jednoznačnej právnej zodpovednosti spoločností sociálnych médií, ktoré zverejňujú nezákonný obsah škodlivý pre kandidátov – pričom sa vyhýba extrémnym opatreniam, ako je blokovanie celých webových stránok. Parlamentné zhromaždenie ďalej vyzvalo organizácie v mediálnom sektore, aby vyvinuli samoregulačné rámce s profesionálnymi a etickými normami na pokrytie predvolebných kampaní a internetových sprostredkovateľov, aby spolupracovali s občianskou spoločnosťou a organizáciami všetkých politických orientácií špecializujúcich sa na overovanie obsahu, aby sa zabezpečilo, že všetky informácie budú potvrdené dôveryhodným zdrojom tretej strany.

B. Právo na súkromie a ochrana osobných údajov

73. V čl. 8 dohovoru sa ustanovuje ochrana práva na súkromie. Na tomto základe ESLP vypracoval rozsiahlu judikatúru týkajúcu sa ochrany osobných údajov.⁸³

74. Dohovor Rady Európy o ochrane fyzických osôb pri automatizovanom spracovaní osobných údajov ETS č. 108 z roku 1981 stanovuje zásady a pravidlá spracovania osobných údajov, ako aj práva fyzických osôb. Dodatkový protokol k dohovoru z roku 2011 stanovuje normy pre zriadenie dozorných orgánov pre ochranu osobných údajov. Osobitnou pridanou hodnotou tohto právneho rámca v porovnaní so všeobecným nariadením Európskej únie o ochrane osobných údajov je to, že je otvorený pre ktorúkoľvek krajinu na svete a umožňuje, aby rôzne právne systémy boli „pod jednou strechou“, a tak harmonizovali rôzne právne režimy.⁸⁴

75. Dňa 10. októbra 2018 podpísalo 21 zmluvných strán dohovoru nový protokol modernizujúci tento dohovor (ďalej len modernizovaný dohovor). Článok 5 modernizovaného dohovoru posilňuje zásady ochrany osobných údajov tým, že vyžaduje, aby sa údaje spracúvali spravodlivo a transparentným spôsobom, zhromažďovali sa na explicitné, špecifikované a legitímne účely a nespracovávali sa spôsobom nezlučiteľným s týmito účelmi, pričom akékoľvek ďalšie spracúvanie na účely archivácie vo verejnom záujme vedeckého alebo historického výskumu alebo štatistické účely podlieha primeraným zárukám zlučiteľným s týmito účelmi. Modernizovaný dohovor okrem toho ustanovuje ďalšie zásady

⁸² Rezolúcia 2254 (2019) o slobode médií ako podmienka demokratických volieb, <<http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=25409&lang=en>>.

⁸³ Judikatúra ESLP týkajúca sa ochrany osobných údajov, dostupná na: <<https://rm.coe.int/case-law-on-data-protection/1680766992>>. Pozri aj ESLP, 2018, „Príručka k článku 8 Dohovoru o ochrane ľudských práv a základných slobôd – Právo na rešpektovanie súkromného a rodinného života“, dostupné na: <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>.

⁸⁴ Týka sa to tak mimoeurópskych krajín (Kaboverdy, Maurícius, Mexiko, Senegal, Tunisko a Uruguaj), ako aj európskych krajín (napr. Albánsko, Rusko, Srbsko, Turecko, Ukrajina).

a požiadavky, ako sú zámerná ochrana osobných údajov (*protection by design*), štandardné hodnotenie vplyvu na osobné údaje a súkromie, ako aj povinné oznamovanie porušenia ochrany osobných údajov prinajmenšom orgánom na ochranu osobných údajov. Zavádza dodatočné záruky, najmä so zreteľom na všadeprítomnosť informačných technológií pri spracovaní osobných údajov, a stanovuje nové kategórie osobných údajov za citlivé. Dodatočné záruky sa vzťahujú najmä na spracovanie citlivých údajov, ako sú politické názory. Modernizovaný dohovor obsahuje podrobnejšie ustanovenia o cezhraničnom toku osobných údajov, o dodatočných požiadavkách na kontrolné orgány v oblasti osobných údajov a o mechanizme nadväzujúcich opatrení.

76. Okrem toho existuje značný počet právnych nástrojov Rady Európy týkajúcich sa ochrany osobných údajov v rámci prevádzky sociálnych sietí.

77. Odporúčanie Výboru ministrov č. R(99)5 z roku 1999 o ochrane súkromia na internete obsahuje usmernenia na ochranu jednotlivcov v súvislosti so zberom a spracovaním osobných údajov vo vzťahu k digitálnym komunikačným systémom a internetovej telekomunikačnej sieti (*information highways*). V odporúčaní CM/Rec(2010)13 z roku 2010 o ochrane fyzických osôb pri automatizovanom spracúvaní osobných údajov v súvislosti s profilovaním sa stanovujú podmienky takéhoto spracúvania a uvádza sa v ňom podrobný zoznam informácií, ktoré je potrebné poskytnúť dotknutým osobám. Poznamenáva, že nedostatočná transparentnosť alebo dokonca „neviditeľnosť“ profilovania a nedostatočná presnosť, ktorá môže vyplývať z automatického uplatňovania vopred stanovených pravidiel vyvodzovania, môže predstavovať značné riziko pre práva a slobody jednotlivca. Hoci to bolo spočiatku vnímané ako technika používaná v obchodnom a marketingovom kontexte, nedávne udalosti ukazujú, že profilovanie sa uplatňuje aj vo volebných procesoch.

78. Rezolúcia ministrov spravodlivosti č. 3 z roku 2010 o ochrane osobných údajov a súkromí v 3. tisícročí MJU-30(2010)RESOL poukazuje na pravdepodobné dôsledky širokého využívania informačných a komunikačných technológií umožňujúcich pozorovanie, uchovávanie a analýzu väčšiny každodenných ľudských aktivít, a pokiaľ sa na celom svete účinne nepresadzujú prísne normy ochrany údajov, môže to u ľudí vyvolávať pocit, že sú pod dohľadom, a narušiť ich slobodné uplatňovanie ľudských práv a základných slobôd. Rezolúcia Parlamentného zhromaždenia 1843(2011) o ochrane súkromia a osobných údajov na internete a online médiách z roku 2011 zdôrazňuje, že ochrana práva na ochranu osobných údajov je nevyhnutným prvkom ľudského života a humánneho fungovania demokratickej spoločnosti a že jeho porušenie má vplyv na dôstojnosť, slobodu a bezpečnosť osoby.

79. Odporúčanie Výboru ministrov CM/Rec(2012)3 z roku 2012 o ochrane ľudských práv v súvislosti s vyhľadávacími nástrojmi uznáva výzvu, ktorú predstavuje skutočnosťou, že história vyhľadávania jednotlivca obsahuje stopy, ktoré môžu odhaliť vieru, záujmy, presvedčenie osoby, vzťahy alebo úmysly a mohli by okrem iného prezrádzať politické názory alebo náboženské alebo iné presvedčenie. Vyzýva na prijatie opatrení na presadzovanie zásad ochrany údajov, najmä obmedzenia účelu, minimalizácie osobných údajov a obmedzeného uchovávanía údajov, pričom dotknuté osoby musia byť informované o spracovaní a musia sa im poskytnúť všetky relevantné informácie.

80. Odporúčanie CM/Rec(2012)4 o ochrane ľudských práv v súvislosti so službami sociálnych sietí poukazuje na stále významnejšiu úlohu takýchto a iných služieb sociálnych médií, ktoré ponúkajú veľké možnosti na zvýšenie potenciálu účasti jednotlivcov na politickom, spoločenskom a kultúrnom živote. Odporúča opatrenia na zabezpečenie prostredia pre používateľov sociálnych sietí, ktoré im umožnia ďalšie uplatnenie ich práv a slobôd, na zvýšenie povedomia používateľov o možnom ohrození ich ľudských práv a o negatívnom dopade na práva iných ľudí pri využívaní týchto služieb, ako aj zvýšiť transparentnosť spracúvania údajov a zakázať nezákonné spracúvanie osobných údajov. Tieto opatrenia je možné vykonať prostredníctvom spolupráce s poskytovateľmi sociálnych sietí. V odporúčaní sa tiež zdôrazňuje, že používatelia by mali byť informovaní o tom, kde sa ich osobné údaje používajú v súvislosti s profilovaním.

81. Deklarácia Výboru ministrov z roku 2013 o rizikách pre základné práva vyplývajúce z digitálneho sledovania a iných technológií sledovania zdôrazňuje, že členské štáty nemajú len negatívnu povinnosť zdržať sa zasahovania do ľudských práv, ale aj pozitívnu zodpovednosť tieto práva aktívne chrániť, čo zahŕňa ochranu jednotlivcov pred konaním neštátnych organizácií. Všadeprítomné používanie rôznych zariadení a informácií zhromaždených prostredníctvom týchto zariadení umožňuje sledovanie a dohľad nad ľuďmi, čím sa odhaľujú chýlostivé a/alebo citlivé osobné informácie vrátane politických alebo náboženských preferencií, ktoré je možné zhromažďovať na poskytovanie ich podrobných a dôverných profilov.

82. Odporúčanie Výboru ministrov z roku 2014 CM/Rec(2014)6 predstavuje príručku o ľudských právach pre používateľov internetu a v roku 2017 Výbor pre dohovor ETS 108 prijal usmernenia pre ochranu jednotlivcov pri spracúvaní osobných údajov v oblasti *Big Data*. Výbor ministrov vo svojom vyhlásení Decl(13/02/2019)1 z 13. februára 2019 o manipulačných schopnostiach algoritmických procesov vyzval členské štáty, aby „*zvážili potrebu dodatočných ochranných rámcov pre údaje, ktoré idú nad rámec súčasného pojmu ochrany osobných údajov a súkromia a zaoberali sa významným dosahom cieleného využívania údajov na spoločnosť a na uplatňovanie ľudských práv v širšom zmysle*“.

83. Rada Európy vypracovala alebo zadala vypracovanie rôznych správ a štúdií v tejto oblasti vrátane Správy o „*používaní internetu a súvisiacich služieb, súkromnom živote a ochrane údajov: trendy a technológie, hrozby a dôsledky*“.⁸⁵ Táto správa vyzýva na potvrdenie a ochranu práva na anonymitu na internete, reguláciu a prísne obmedzenie vytvárania a používania profilovania vo všetkých oblastiach a na prijatie usmernení Rady Európy o obmedzeniach, ktoré sa majú aplikovať na sledovanie prostredníctvom technológie vrátane medzinárodného obchodu s týmito technológiami.

⁸⁵ Korff, 2013, na:

<<http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168067f7f4>>.

C. Ochrana pred počítačovou kriminalitou

84. Dohovor Rady Európy o počítačovej kriminalite ETS 185 z roku 2001 („Budapešťiansky dohovor“) rieši dva typy hrozieb pre volebnú demokraciu.⁸⁶ Po prvé, trestné činy proti dôvernosti, hodnovernosti a dostupnosti volebných počítačových údajov a systémov, ktoré predstavujú formy počítačovej kriminality ako nezákonný prístup k počítačovým systémom (čl. 2), nezákonné zachytávanie údajov (čl. 3), zasahovanie do údajov a systémov (čl. 4 a 5) a iné. Po druhé, dezinformačné systémy, pri ktorých sa porušujú pravidlá o ochrane osobných údajov, o financovaní politiky, o mediálnom pokrytí alebo vysielaní o voľbách, teda pravidlá na zabezpečenie slobodných, spravodlivých a hladkých volieb.

85. Zatiaľ čo druhý typ správania sám osebe nepredstavuje počítačovú kriminalitu, dôkazy o porušovaní takýchto pravidiel majú často formu elektronických dôkazov. Je preto nevyhnutné, aby štáty poskytli svojim orgánom činným v trestnom konaní potrebné právomoci na zabezpečenie takýchto dôkazov. Od zmluvných strán Budapešťianskeho dohovoru sa vyžaduje, aby tak urobili na základe čl. 16 až 21, ktoré sa týkajú procesnoprávných právomocí, akými sú urýchlené uchovanie uložených počítačových údajov, prehliadka a zaistenie počítačových systémov a údajov, zhromažďovanie prevádzkových údajov a iné.

86. Hlavným problémom je, že údaje, a teda aj elektronické dôkazy sú nestále a často ich uchovávajú poskytovatelia služieb v zahraničných jurisdikciách alebo sú uložené vo viacerých, presúvajúcich sa alebo neznámych jurisdikciách, teda „*nikde na serveroch v cloude*“.⁸⁷ Priradenie útoku alebo jednoducho identifikácia používateľa adresy internetového protokolu (IP) alebo vlastníka sociálnej siete alebo mailového účtu často nie je s primeraným úsilím možná. To je jeden z dôvodov, prečo sú počítačová kriminalita a iné kybernetické hrozby pre volebnú demokraciu stíhané len zriedka.

87. Zaistila sa efektívna medzinárodná spolupráca a spolupráca s poskytovateľmi služieb. Budapešťiansky dohovor vo svojej súčasnej podobe obsahuje podrobné ustanovenia o medzinárodnej spolupráci, ktoré kombinujú urýchlené dočasné opatrenia na zabezpečenie údajov (napr. čl. 29 o urýchlenom uchovávaní a čl. 35 o kontaktných miestach prevádzkovaných 24 hodín denne, 7 dní v týždni) s ustanoveniami o vzájomnej právnej pomoci. Tieto ustanovenia sa bežne využívajú pri vyšetrowaní počítačovej kriminality.

88. Tieto však dostatočne neriešia problém *cloud computingu* a súvisiace problémy jurisdikcie alebo skutočnosť, že poskytovatelia služieb v jednom štáte ponúkajú svoje služby v mnohých iných bez toho, aby boli právne alebo fyzicky prítomní alebo zodpovední v druhom štáte.

89. Z tohto dôvodu zmluvné strany Budapešťianskeho dohovoru začali rokovania o 2. dodatkovom protokole s cieľom umožniť ďalšie alternatívy posilnenej medzinárodnej

⁸⁶ Nasledujúce informácie sú založené na príspevku Alexandra Segera (výkonný tajomník, Výbor pre dohovor o počítačovej kriminalite, Rada Európy) na 15. európskej konferencii volebných riadiacich orgánov, Oslo, Nórsko, 19. – 20. apríla 2018.

⁸⁷ Podrobné základné informácie nájdete v správach, ktoré pripravila skupina Cloud Evidence Group v rámci Výboru pre dohovor o počítačovej kriminalite, <<https://www.coe.int/en/web/cybercrime/ceg>> (posledný prístup bol 30. septembra 2018).

spolupráce a prístupu k údajom na cloude. Zvažované riešenia zahŕňajú priamu spoluprácu s poskytovateľmi služieb so sídlom v iných zmluvných štátoch, rozšírenie vyhľadávania na počítače v iných jurisdikciách za obmedzených okolností alebo núdzovú vzájomnú pomoc. Očakáva sa, že rokovania potrvajú do konca roka 2019.⁸⁸

VI. Iné medzinárodné a vnútroštátne právne predpisy, judikatúra a iniciatívy⁸⁹

A. Medzinárodná úroveň

90. Na úrovni Organizácie Spojených národov bolo v Spoločnej deklarácii o slobode prejavu a internetu z 1. júna 2011⁹⁰ uvedené, že prístupy k regulácii vyvinuté pre iné komunikačné prostriedky (ako sú telefónne služby alebo vysielanie) sú veľmi odlišné od tých, ktoré sú potrebné pre internet, a takéto metódy musia byť preň špeciálne navrhnuté. Najnovšie spoločné vyhlásenie z 3. marca 2017 teraz zahŕňa „falošné správy“ (*fake news*), dezinformácie a propagandu a zdôrazňuje potrebu uprednostniť slobodu prejavu, pričom uvádza, že zákazy šírenia informácií založených na nejasných a nejednoznačných ideách vrátane „falošných správ“ alebo „neobjektívnych informácií“ sú nezlučiteľné s medzinárodnými normami pre obmedzenie slobody prejavu, ako je uvedené v §1 písm. a)⁹¹, a mali by sa zrušiť.

91. Rastúce povedomie o potrebe predchádzať falošným správam a obmedziť ich šírenie najmä počas volebných období vyvolalo iniciatívy siahajúce od výskumu, vzdelávania a spolupráce až po samoreguláciu a regulačné riešenia, a to aj na medzinárodnej úrovni. NATO zriadilo Stratcom Center of Excellence, *think-tank*, ktorý sa zameriava na vplyv informačnej dominancie na internet a kybernetickú obranu. V dôsledku spolupráce medzi EÚ a NATO v oblasti hybridných hrozieb bolo v roku 2017 zriadené Európske centrum kvality pre boj proti hybridným hrozbám.⁹²

92. Existuje niekoľko sietí ľudí, ktorí spolupracujú na overovaní online informácií, napríklad International Fact-Checking Network (IFCN) funguje ako útvar Poynterovho inštitútu, ktorý sa venuje združovaniu overovateľov faktov na celom svete. Bol vytvorený v roku 2015 na podporu a pozorovanie práce 64 organizácií na overovanie faktov z celého sveta.

⁸⁸ Pozri <<https://www.coe.int/en/web/cybercrime/t-cy-drafting-group>>.

⁸⁹ Táto správa neobsahuje vyčerpávajúci popis národného materiálu. Pozri tiež CDL-AD(2019)016.

⁹⁰ Vyhlásenie podpísané osobitným spravodajcom OSN pre slobodu názoru a prejavu, predstaviteľom OBSE pre slobodu médií, osobitným spravodajcom OAS pre slobodu prejavu a osobitným spravodajcom ACHPR pre slobodu prejavu a prístupu k informáciám 1. júna 2011.

⁹¹ Štáty môžu obmedziť právo na slobodu prejavu len v súlade s testom pre takéto obmedzenia podľa medzinárodného práva, konkrétne že sú ustanovené zákonom, slúžia jednému z legitímnych záujmov uznaných medzinárodným právom a sú nevyhnutné a primerané chrániť tento záujem.

⁹² Pozri tiež praktickú príručku na používanie sociálnych médií počas volieb, ktorú vypracoval Medzinárodný inštitút pre demokraciu a volebnú pomoc (International IDEA) v prospech volebných riadiacich orgánov: Seema Shah, „Guidelines for the Development of a Social Media Code of Conduct for Elections“, International IDEA, 2015. Príručka je dostupná na: <<https://www.idea.int/sites/default/files/publications/social-media-guide-for-electoral-management-bodies.pdf>>. Pozri: <<https://wayback.archive-it.org/12090/3/https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-%20online-disinformation%20>>.

B. Európska únia

93. V januári 2018 Európska komisia zriadila skupinu odborníkov na vysokej úrovni (HLEG), ktorá má poskytovať poradenstvo v oblasti politických iniciatív na boj proti „falošným správam“ a dezinformáciám, ktoré sa šíria online. Vo svojej záverečnej správe⁹³ HLEG odporučila viacerozmerný prístup založený na piatich pilieroch navrhnutých tak, aby:

- i) sa zvýšila transparentnosť správ online;
- ii) podporovala sa mediálna a informačná gramotnosť v boji proti dezinformáciám;
- iii) vyvinuli sa nástroje, ktoré umožnia používateľom a novinárom bojovať s dezinformáciami;
- iv) chránila sa diverzita a udržateľnosť európskeho ekosystému spravodajských médií a
- v) podporoval sa pokračujúci výskum o vplyve dezinformácií v Európe.

94. Na základe výsledkov HLEG vydala Európska komisia v apríli 2018 oznámenie, v ktorom načrtáva stratégiu Komisie na riešenie problému dezinformácií online.⁹⁴ Táto stratégia nepredpokladá regulačný zásah a jej hlavnými smermi sú: i) vypracovanie ambiciózneho samoregulačného kódexu postupov vedúcimi subjektmi na trhu (vrátane sociálnych sietí, inzerentov a iných subjektov z reklamného priemyslu); ii) posilnenie kapacity na overovanie a monitorovanie dezinformácií; iii) využívanie nových technológií (napr. umelá inteligencia) na boj proti dezinformáciám; iv) posilnenie volebných procesov a v) podpora vzdelávania a mediálnej gramotnosti.

95. Kódex postupov v oblasti dezinformácií bol prijatý v septembri 2018⁹⁵ s cieľom chrániť nadchádzajúce voľby do orgánov EÚ. Kódex je zameraný na:

- zabezpečenie transparentnosti sponzorovaného obsahu, najmä politickej reklamy, ako aj obmedzenie možností zacielenia politickej reklamy a zníženie príjmov pre poskytovateľov dezinformácií;
- umožnenie väčšej prehľadnosti o fungovaní algoritmov a overenia treťou stranou;
- uľahčenie objavovania a prístupu používateľom k rôznym spravodajským zdrojom reprezentujúcim iné názory;
- zavedenie opatrení na identifikáciu a zrušenie falošných účtov a na riešenie problému automatizovaných robotov;
- umožnenie nepretržitého monitorovania online dezinformácií overovateľmi faktov, výskumníkmi a verejnými orgánmi.

96. Európska komisia prostredníctvom rámcového programu pre výskum a inovácie Horizont 2020 podporila aj niekoľko inovačných činností zameraných na vývoj nových nástrojov a služieb na pomoc odborníkom a občanom pri overovaní online obsahu (textu, obrázka a videa). Európska únia okrem toho vytvorí nezávislú európsku sieť overovateľov faktov, ktorí budú vybraní z európskych členov IFCN. Sieť vyvinie pracovné metódy, zavedie najlepšie

⁹³ Pozri: <<https://wayback.archive-it.org/12090/3/https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-%20online-disinformation%20>>.

⁹⁴ Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov „Riešenie online dezinformácií: európsky prístup“, COM(2018)236 v konečnom znení. Dostupné na: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236>>.

⁹⁵ Dostupné na: <<https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>>.

postupy, aby sa dosiahlo čo najširšie pokrytie pre nápravu faktov. Komisia poskytne siete potrebné online nástroje, bezpečnú európsku online platformu pre dezinformácie, aby jej pomohla dosiahnuť stanovený cieľ. Prostredníctvom nástroja Connect Europe Facility (CEF) Komisia podporí aj zavedenie európskej platformy pre dezinformácie s cieľom zvýšiť kapacitu na odhaľovanie a analýzu dezinformačných kampaní v celej Európe.

97. V septembri 2018 vydala Európska komisia konkrétne odporúčania s cieľom chrániť európske demokratické procesy pred manipuláciou zo strany tretích krajín alebo súkromných záujmov a navrhla nové pravidlá pre siete volebnej spolupráce, online transparentnosť, ochranu pred kybernetickými incidentmi a kroky na boj proti dezinformačným kampaniam v kontexte volieb do Európskeho parlamentu.⁹⁶ V decembri 2018 bol prijatý Akčný plán boja proti dezinformáciám⁹⁷, ktorý je zameraný na budovanie kapacít a posilnenie spolupráce medzi členskými štátmi a inštitúciami EÚ na proaktívne riešenie hrozieb, ktoré dezinformácie predstavujú. Pozornosť sa upriamuje aj na stanovisko Európskeho dozorného úradníka pre ochranu údajov z marca 2018 o online manipulácii a osobných údajoch⁹⁸, v ktorom sa odporúča, aby sa dotiahli a presadzovali pravidlá ochrany údajov, aby sa regulačné orgány zamerali na kolektívnu diagnostiku problému a spolupracovali naprieč sektormi, aby sa podporovala samoregulácia a kódexy správania a aby jednotlivci boli oprávnení uplatňovať svoje práva vrátane kolektívneho konania.

98. Medzi už existujúcimi nariadeniami EÚ sa v súčasnom kontexte javia ako obzvlášť dôležité tieto:

- Všeobecné nariadenie o ochrane údajov (GDPR)⁹⁹, ktoré je priamo uplatniteľné v celej EÚ od 25. mája 2018. Jeho ustanovenia sú povinné a poskytujú jednotlivcom mnohé práva vrátane práv na transparentnú komunikáciu, vymazanie (právo byť zabudnutý) a prenosnosť údajov (t. j. prenos od jedného prevádzkovateľa údajov k druhému). Nariadenie ustanovuje všeobecný zákaz spracúvania osobných údajov „*odhaľujúcich rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie, prípadne členstvo v odborových organizáciách a spracúvanie genetických údajov, biometrických údajov na účely jednoznačnej identifikácie fyzickej osoby, údaje o zdraví alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby*“ s niektorými výnimkami, najmä ak „*je spracovanie nevyhnutné z dôvodov závažného verejného záujmu, na základe práva Únie alebo členského štátu, ktoré je primerané sledovanému cieľu, rešpektuje podstatu práva na ochranu údajov a ustanovuje vhodné a konkrétne opatrenia na ochranu základných práv a záujmov dotknutej osoby*“. Práva stanovené GDPR môžu vykonávať a

⁹⁶ Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov „Zabezpečenie slobodných a spravodlivých volieb do Európskeho parlamentu“, COM(2018)637 v konečnom znení. Dostupné na: <<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018DC0637>>.

⁹⁷ Pozri <<https://ec.europa.eu/digital-single-market/en/news/europe-protects-eu-steps-action-against-disinformation>>.

⁹⁸ Dostupné na: <https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf>.

⁹⁹ Dostupné na: <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=SK>>.

presadzovať nielen jednotlivci, ale aj organizácie konajúce v mene jednotlivcov. Na vyplnenie medzery v ochrane pred neadekvátnym spracúvaním osobných údajov mimo Európskej únie GDPR rozširuje právnu ochranu na spracúvanie osobných údajov dotknutých osôb Únie „bez ohľadu na to, kde sa spracúvanie uskutočňuje“. Kvôli tomu sa vzťahuje aj na subjekty zriadené mimo EÚ, ak ponúkajú tovar alebo služby jednotlivcom v Únii alebo ak sledujú ich online správanie. Nariadenie stanovuje prísne pravidlá pre prenos údajov mimo Európskej únie; spracovatelia údajov musia viesť záznamy o všetkých spracovateľských činnostiach. Sú zodpovední za prijatie všetkých potrebných opatrení, ktoré zaručia, že osobné údaje budú spracované zákonným, spravodlivým a transparentným spôsobom. Nariadenie GDPR tak má potenciál zabrániť neoprávnenému spracovaniu osobných údajov na volebné účely, ako v prípade Cambridge Analytica.¹⁰⁰

- Nariadenie (EÚ) 2015/2120, ktorým sa ustanovujú opatrenia týkajúce sa prístupu k otvorenému internetu¹⁰¹ platné od 30. apríla 2016, vytvára pre koncových používateľov v EÚ individuálne a vymáhateľné právo na prístup a šírenie internetového obsahu a služieb podľa vlastného výberu a zakotvuje princíp nediskriminačného riadenia internetového prenosu. Presadzovanie pravidiel otvoreného internetu v rámci EÚ je úlohou národných regulačných orgánov, ktoré by mali rešpektovať usmernenia prijaté Orgánom európskych úradov pre reguláciu elektronických komunikácií (BEREC) v roku 2016. Internetovým poskytovateľom služieb teda neprislúcha rozhodovať o úspechu alebo zlyhaní distribuovaných služieb a obsahu. Pravidlá zakotvujú v práve EÚ zásadu neutrality siete a snažia sa zabrániť blokovaníu, obmedzovaniu alebo diskriminácii online obsahu, aplikácií a služieb.¹⁰²
- Smernica Európskeho parlamentu a Rady 2000/31/EC¹⁰³ obsahuje výnimky zo zodpovednosti dostupné pre určitých poskytovateľov online služieb vrátane poskytovateľov „hostingových“ služieb pod podmienkou, že hneď ako sa o nich dozvedia, urýchlene odstránia alebo znemožnia prístup k nezákonným informáciám, ktoré uchovávajú. V tejto súvislosti treba poznamenať, že Európska komisia vo viacerých nedávnych tlačových správach zdôraznila potrebu, aby online platformy konali zodpovednejšie a zintenzívnili celoeurópske samoregulačné úsilie na odstránenie nezákonného obsahu; 1. marca 2018 prijala odporúčanie o opatreniach na účinný boj proti nezákonnému online obsahu¹⁰⁴, ktoré je zamerané na členské štáty a poskytovateľov hostingových služieb a ktorého cieľom je zvýšiť transparentnosť a presnosť mechanizmov oznamovania a konania.

C. Príklady na národnej úrovni

99. Viaceré štáty nedávno prijali alebo plánujú prijať legislatívu, ktorá reguluje online obsah a odporuje politicky nabitým dezinformáciám počas volieb. Nemecko konalo ako

¹⁰⁰ Informácie o implementácii GDPR v rôznych európskych krajinách nájdete na: <https://www.gdprtoday.org/gdpr-loopholes-facilitate-data-exploitation-by-political-parties/>.

¹⁰¹ Dostupné na: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2120>.

¹⁰² Dostupné na: <https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality>.

¹⁰³ Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=celex%3A32000L0031>.

¹⁰⁴ Dostupné na: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32018H0334>.

prvé¹⁰⁵ a zaviazalo internetových sprostredkovateľov (ako sú Facebook, Instagram, Twitter alebo YouTube), aby na základe sťažnosti bezodkladne odstránili akýkoľvek obsah, ktorý trestný kódex označuje za nezákonný; zjavne nezákonný obsah musí byť zablokovaný a vymazaný do 24 hodín. Trestné činy siahajú od nenávisných prejavov a ohovárania až po ohrozenie ústavného poriadku alebo národnej bezpečnosti a pod., ktoré môžu mať priamy vplyv na verejnú diskusiu a názor najmä v čase volieb (zákon je všeobecný, neupravuje osobitne volebnú kampaň). Zákon o presadzovaní práva na sieti, ktorý nadobudol účinnosť začiatkom roka 2018, upravuje pokuty až do výšky 50 miliónov eur, ktoré možno uplatniť aj v prípade, že trestný čin nebol spáchaný v Nemecku.

100. Francúzsky parlament v novembri 2018 prijal zákon na boj proti manipulácii s informáciami¹⁰⁶ počas volebného obdobia, ktorého cieľom je identifikovať a zastaviť úmyselne nepravdivé alebo zavádzajúce skutočnosti na online platforme v období troch mesiacov pred voľbami. Podľa nového zákona musia byť platformy transparentné: musia poskytnúť jasné, správne a transparentné informácie o svojej vlastnej identite a kvalite alebo identite a kvalite tretej strany, ktorá sponzoruje ich obsah; musia tiež zverejniť sumu, ktorú dostali výmenou za sponzorovanie obsahu. Prokurátor, každá osoba, ktorá ma záujem na predložení veci sudcovi na základe naliehavosti, ako aj politické strany alebo kandidáti môžu namietat' údaj, ktorý sa zdá byť zámerne nesprávnym alebo zavádzajúcim a je umelo a rozsiahle rozširovaný online; pojem umelého a rozsiahleho rozširovania bude záchytným bodom pre nepravdivé informácie. Sudca je povinný rozhodnúť o prípade tohto charakteru do 48 hodín, má právo blokovat' zverejnenie a prinútiť platformu zastaviť túto kampaň. Technickí sprostredkovatelia, ktorými sú osoby ponúkajúce prístup ku komunikačným službám, musia bezodkladne odstrániť akýkoľvek nezákonný obsah, na ktorý boli upozornení, a zaviesť ľahko dostupný a viditeľný mechanizmus, prostredníctvom ktorého ich budú osoby informovať o akýkoľvek falošných správach. Francúzsky úrad pre reguláciu vysielania má okrem toho právo odmietnuť podpísať dohovor s tretou krajinou, ak by aktivity tejto krajiny mohli vážne ohroziť život národa šírením falošných správ alebo porušovaním plurality názorových prúdov.¹⁰⁷

101. Rusko¹⁰⁸, Singapur¹⁰⁹ a Filipíny pri zvažovaní alebo prijímaní legislatívy

¹⁰⁵ Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) – Network Enforcement Act, <<https://germanlawarchive.iuscomp.org/?p=1245>>.

¹⁰⁶ Loi n° 2018 1202 relative à la lutte contre la manipulation de l'information, <<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037847559/>>.

¹⁰⁷ Francúzsky zákon bol predmetom ostrej kritiky, pozri napr. <<https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law>>. V prípade Nemecka pozri o. i. <<https://www.dw.com/en/germany-implements-new-internet-hate-speech-crackdown/a-41991590>> a <<https://www.economist.com/europe/2018/01/13/germany-is-silencing-hate-speech-but-cannot-define-it>>.

¹⁰⁸ Federálny zákon o informáciách, informačných technológiách a ochrane informácií (z 27. júla 2006, č. 149-FZ) bol prijatý 18. marca 2019. Postihuje šírenie „nespolahlivých spoločensky dôležitých informácií“, ktoré môžu ohroziť životy a verejnosť. Tento zákon umožňuje zablokovať webovú stránku obsahujúcu takéto informácie. V ten istý deň bol prijatý federálny zákon č. 30-FZ („zákon o nerešpektovaní“), ktorým sa k federálnemu zákonu o informáciách, informačných technológiách a ochrane informácií (z 27. júla 2006, č. 149-FZ) pridal článok 15-1-1. Postihuje prejav, ktorý „prejavuje neúctu k spoločnosti, štátu, oficiálnym štátnym symbolom... a orgánom štátnej moci“ a ktorý je vyjadrený „obscénnou formou“. Zákon o správnych

na odstránenie „nezákonného“ online obsahu priamo označili nemecký zákon za pozitívny príklad.¹¹⁰

102. Britská volebná komisia vyzvala na zvýšenie transparentnosti pre voličov v súvislosti s praxou digitálnych volebných kampaní. Vyдала odporúčania pre zodpovednosť digitálnych kampaní, výdaje za digitálne kampane, transparentnosť platieb za digitálne kampane a vynucovanie týchto pravidiel.¹¹¹

103. Zákon o čestných reklamách, ktorý bol predložený v Kongrese¹¹² USA v októbri 2017, predstavil pravidlá zverejňovania a vylúčenia zodpovednosti pre politickú reklamu online. Zatiaľ čo televízia a rádio sú už dávno povinné zverejňovať kupujúcich a obsah všetkých nákupov reklamy na ich staniciach, internetové spoločnosti túto povinnosť nemajú. Zákon o čestných reklamách by nariadil, aby internetové spoločnosti zverejnili identitu a obsah reklamy vzťahujúce sa na voľby a kampane. Konkrétne, došlo by k tomu na základe novelizácie desaťročia starého existujúceho zákona o financovaní kampane z roku 1971 pridaním frázy „platená internetová alebo platená digitálna komunikácia“ do zoznamu médií, ktoré podliehajú zákonu. Od každej webovej stránky, ktorá má aspoň 50 miliónov návštevníkov za mesiac (vrátane Facebook, Google a Twitter), by sa vyžadovalo, aby viedla verejný zoznam všetkých organizácií a osôb, ktoré minuli najmenej 500 dolárov na reklamu spojenú s voľbami. Výnimka sa udeľuje pre „spravodajstvo, komentáre a editoriály“, aby sa zabezpečilo, že požiadavky nebudú zaťažovať legitímne spravodajské reportáže a názorové články.

104. V niektorých krajinách boli vytvorené alebo sa kreujú špecializované jednotky na boj so šírením nepravdivých informácií, napríklad:

- a) Spojené kráľovstvo plánuje zriadiť národnú bezpečnostnú komunikačnú jednotku na boj proti dezinformačným „falošným správam“;
- b) v Českej republike je Centrum proti terorizmu a hybridným hrozbám (súčasť ministerstva vnútra) špecializovanou analytickou a komunikačnou jednotkou, ktorá monitoruje hrozby priamo súvisiace s vnútroštátnou bezpečnosťou, čo zahŕňa široké spektrum hrozieb a potenciálnych incidentov súvisiacich s terorizmom, útokmi na citlivé ciele, bezpečnostnými aspektmi migrácie, extrémizmom, verejnými zhromaždeniami, porušením verejného poriadku a rôznymi trestnými činmi, alebo aj dezinformačnými kampaňami spojenými s vnútornou bezpečnosťou. Vypracúva aj

deliktoch bol novelizovaný s cieľom zaviesť pokuty za publikácie obsahujúce „obscénnu neúctu“ a „falošné správy“.

¹⁰⁹ Pozri: <https://techcrunch.com/2019/05/09/singapore-fake-news-law/?renderMode=ie11&guccounter=1&guce_referrer_us=aHR0cHM6Ly90ZWNoY3J1bmNoLmNvbS8yMDE5LzA1LzA5L3NpbmdhcG9yZS1mYWtlLW5ld3MtbGF3Lw&guce_referrer_cs=oKT9smcHtaNhdWGcU8VGvg;https://mediawrites.law/fake-news-law-passed-in-singapore-protection-from-online-falsehoods-and-manipulation-act/>.

¹¹⁰ Pozri <<https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law>>.

¹¹¹ Pozri <https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Digital-campaigning-improving-transparency-for-voters.pdf>.

¹¹² <<https://www.congress.gov/bill/115th-congress/senate-bill/1989/text>>

návrhy na vecné a legislatívne riešenia, ktoré aj zavádza tam, kde je to možné, a šíri informácie a osvetu o danej problematike medzi laickou a odbornou verejnosťou.

105. V Brazílii sa podporuje spolupráca medzi volebnými orgánmi, akademikmi a odborníkmi z praxe s cieľom zistiť skutočný vplyv a účinnosť prijatých opatrení prostredníctvom Poradného zboru pre internet a voľby, ktorý radí volebnému súdu. Panama a Mexiko¹¹³ sú príkladmi krajín, v ktorých operátori a platformy spolupracujú s volebnými orgánmi s cieľom identifikovať hrozby a šíriť oficiálne informácie.

106. Overovanie faktov¹¹⁴, tzv. fact-checking, sa rozvíja vo viacerých krajinách¹¹⁵ a v niektorých z nich boli vytvorené siete overovateľov faktov; zaujímavým príkladom je „#Verificado18“ skupina novinárov, zástupcov občianskej spoločnosti a akademikov, ktorí sa snažili o odhalenie virálnych dezinformácií, overovanie tvrdení politikov a boj s nepravdivými informáciami pre federálny volebný proces v roku 2018 v Mexiku. Aj Španielsko počas posledných volieb zriadilo osobitnú jednotku na overovanie faktov.¹¹⁶

VII. Elektronické výzvy pre demokraciu a ľudské práva

107. Uskutočnenie demokratických volieb (teda samotná existencia demokracie) nie je možné bez rešpektovania ľudských práv, najmä slobody prejavu a tlače a slobody združovania a zhromažďovania na politické účely vrátane politických strán. Rešpektovanie týchto slobôd je absolútne nevyhnutné najmä počas volebnej kampane. Obmedzenie týchto základných slobôd musí byť v súlade s Európskym dohovorom o ochrane ľudských práv a vo všeobecnosti s požiadavkou, aby mali zákonný základ, boli vo všeobecnom záujme a rešpektovali princíp proporcionality. Právne predpisy by mali ustanoviť jasné pravidlá pre vyváženú konkurujúcu práv, ktoré by mali byť účinne implementované prostredníctvom volebného a všeobecného súdneho mechanizmu.

108. Používanie digitálnych technológií ovplyvňuje niekoľko osobitných predstáv o demokracii. Po prvé, nové informačné technológie, napríklad elektronické hlasovanie a vytváranie a aktualizácia voličských registrov, majú vplyv na *volebnú demokraciu*, ktorá sa chápe ako inštitucionálne činnosti a infraštruktúra, ktoré umožňujú konanie volieb a sú všeobecne známe v kontexte internetu ako „e-government“. Po druhé, internet a nové informačné technológie majú potenciál priniesť väčšiu transparentnosť a zodpovednosť, ako aj širšie a výkonnejšie formy politickej participácie, čím sa rozšíri dosah „verejnej sféry“; v tom zmysle majú vplyv na *deliberatívnu demokraciu*, ktorá sa uvádza v súvislosti s účasťou jednotlivcov na otvorenej diskusii vo viere, že to povedie k lepším rozhodnutiam v otázkach

¹¹³ INE (Instituto Nacional Electoral) z Mexika počas prípravy volieb v roku 2018 uzavrelo dohody o spolupráci s Facebookom, Twitterom a Google; pozri INE, Democracia en riesgo, Elecciones en tiempos de desinformación, Estrategia y acciones implementadas para enfrentar la desinformación deliberada en las elecciones mexicanas de 2018.

¹¹⁴ Cf. Lazer et al., 2018.

¹¹⁵ Pozri napr. dodatok k správe Rady Európy o informačnom zvätku za rok 2017, v ktorej sú uvedené európske iniciatívy na overovanie a odhaľovanie faktov. Pozri tiež <<https://reporterslab.org/fact-checking/>>.

¹¹⁶ <https://elpais.com/politica/2019/03/10/actualidad/1552243571_703630.html>

spoločného záujmu.¹¹⁷ Napokon, v rozsahu, akom tieto technológie podporujú proces, v ktorom sa veľké dezorganizované skupiny ľudí organizujú a konajú s cieľom riešiť špecifické sociálne, ekonomické alebo politické otázky, môžu ovplyvniť tzv. „kontrolujúcu demokraciu“ (*monitory democracy*) definovanú ako „verejná zodpovednosť a verejná kontrola osôb s rozhodovacou právomocou subjektmi, ktoré pôsobia v oblasti štátnych alebo medzištátnych inštitúcií alebo sú to takzvané mimovládne organizácie či organizácie občianskej spoločnosti, ako sú podniky, odbory, športové asociácie a charity“.¹¹⁸ V rozsahu, v akom schopnosť občanov zisťovať verejnú mienku a organizovať sa na politické účely závisí tak od informácií, ku ktorým majú prístup, ako aj od ich možnosti diskutovať a zhodnúť sa na spoločnom programe, je možné parametre kontrolujúcej demokracie považovať za začlenené do kategórie deliberatívnej demokracie.

A. Výzvy pre volebnú demokraciu

109. Ako už bolo uvedené, koncept „volebnej demokracie“ sa chápe ako inštitucionálne činnosti a infraštruktúra, ktoré umožňujú voľby. Od samotnej organizácie volieb cez vytvorenie a spravovanie voličských registrov až po zavedenie elektronických hlasovacích lístkov a hlasovanie cez internet volebný aspekt demokracie stanovuje materiálne a inštitucionálne podmienky nevyhnutné pre to, aby sa volebné právo premietlo do menovania zástupcov alebo schvaľovania zákonov a verejných politík. Správna údržba voličských registrov je kľúčová pre realizáciu princípu všeobecného volebného práva; prísne dodržiavanie postupov hlasovania a sčítavania hlasov je kľúčové pre realizáciu princípu slobodných volieb.

110. Na jednej strane dokáže používanie digitálnych technológií sprístupniť demokratické procesy všetkým občanom, avšak na druhej strane môže spôsobiť prekážky pre výkon a vývoj volebnej demokracie, čo bude mať za následok nové formy neprimeraného zásahu do práva voliť a práva byť volený (čl. 3 dodatkového protokolu k EDLP), slobody prejavu (čl. 10 EDLP) a práva na rešpektovanie súkromného života (čl. 8 EDLP).

111. Podľa Úradu pre zriadenie bezpečnosti komunikácie kanadskej vlády (CSE) „*protivníci na celom svete využívajú kybernetické vybavenia... proti voľbám... na potlačenie volebnej účasti, manipuláciu s výsledkami volieb a krádež informácií o voľbách... proti politickým stranám a politikom... na kybernetickú špionáž na účely nátlaku a manipulácie a na verejnú diskreditáciu jednotlivcov... a proti tradičným a sociálnym médiám... pre šírenie dezinformácií a propagandy a formovanie názorov voľčov*“.¹¹⁹ Okrem toho predpokladá, že

¹¹⁷ Laidlaw 2015, s. 10 – 11.

¹¹⁸ John Keane, *Život a smrť demokracie*, 2009. Definícia „monitorovej demokracie“ je uvedená na <<http://thelifeanddeathofdemocracy.org/glossary/monitorydemocracy/>>.

¹¹⁹ CSE 2017. Vo svete sme videli niekoľko príkladov týchto zásahov:

- „V júni 2016 americký štát Arizona takmer na týždeň odstavil svoj systém registrácie voľčov po tom, čo sa do systému pokúsili získať prístup protivníci. Nasledujúci mesiac štátna volebná agentúra v Illinois zrušila svoju webovú stránku na dva týždne po tom, čo objavila desaťtisíce záznamov voľčov (napr. mená, adresy a čísla vodičských preukazov), o ktorých bolo podozrenie, že si ich prezerali protivníci“ (Nakashima, ako uvádza CSE).
- „V reakcii na vnímanú slabosť softvéru v strojoch na tabuľovanie hlasov a na varovania, že voľby môžu byť terčom Ruska, Holandsko vo svojich posledných voľbách upravilo volebné postupy. Aby sa predišlo možnosti zasahovania protivníkov do volieb, všetky hlasy boli spočítané ručne“ (Escritt, ako ho uvádza CSE).

počas nasledujúcich rokov „je vysoko pravdepodobné, že kybernetické hrozby pre demokratické procesy celosvetovo narastú v počte aj premyslenosti“ z týchto dôvodov:¹²⁰

- „Mnohé účinné kybernetické vybavenia sú verejne dostupné, lacné a ľahko sa používajú.
- Rýchly nárast sociálnych médií spolu s poklesom dlhodobých autoritatívnych zdrojov informácií uľahčuje protivníkovi používať kybernetické vybavenie a iné metódy na zavádzanie dezinformácií a propagandy do médií a tak ovplyvňovať voličov.
- Volebné agentúry čoraz viac využívajú internet na vylepšenie služieb pre voličov. Ako sa tieto služby presúvajú do online priestoru, stávajú sa zraniteľnejšími voči kybernetickým hrozbám.
- Zabrániť kybernetickým hrozbám je výzvou, pretože je často ťažké ich včas zistiť, prisúdiť a reagovať na nich. V dôsledku toho sa rovnica nákladov a výnosov prikláňa na stranu tých, ktorí kybernetické vybavenia používajú, než tých, ktorí sa pred ich využívaním bránia.
- Napokon je tu dynamika úspechu, ktorá povzbudzuje protivníkov na opakovanie ich činnosti a inšpiruje k napodobňovaniu ich správania.“

112. Dohovor Rady Európy o počítačovej kriminalite ETS 185 z roku 2001 („Budapešťiansky dohovor“) a súčasná príprava druhého dodatkového protokolu ukazujú, že viaceré štáty pochopili tieto riziká.¹²¹

113. Z pohľadu počítačovej kriminality môžu hrozby pre volebnú demokraciu zahŕňať najmenej dva druhy zásahov. Jeden je útok proti dôvernosti, integrite a dostupnosti volebných počítačov a dát vrátane:

- ohrozenia voličských databáz a registračných systémov, napríklad prostredníctvom hackovania počítačových systémov alebo vymazaním, zmenou či pridaním údajov;

• „V decembri 2016 získali protivníci prístup na webovú stránku Ghanskej ústrednej volebnej komisie počas všeobecných volieb, keď sa spočítavali hlasy. Neznámy protivník tweetoval falošné výsledky, že úradujúci kandidát prehral voľby. Volebná komisia potom rozoslala svoje vlastné tweety, v ktorých tvrdila, že tieto výsledky sú nepravdivé. Hoci sa výsledok volieb nezmenil, tento incident poslúžil na vyvolanie zmätku v mysliach mnohých voličov“ (BBC News, ako uvádza CSE).

• „V posledných prezidentských voľbách v USA boli obe hlavné politické strany vystavené pokusom o počítačovú špiónaž zo strany Ruska. Ruskí agenti použili kybernetické schopnosti na získanie prístupu k mailom kľúčových politických zamestnancov pracujúcich na kampani Demokratickej strany. Emaily následne unikli, aby zahanbili kandidáta Demokratickej strany“ (ODNI, ako ho uvádza CSE).

• „Podľa správ médií sa francúzska spravodajská služba domnieva, že na ovplyvnenie prezidentských volieb boli použité siete botov na sociálnych sieťach (social botnets). Niektoré účty na sociálnych médiách, tie isté, ktoré boli aktívne počas minuloročných volieb v USA, propagovali nepravdivé a hanlivé informácie namierené proti vedúcemu kandidátovi. V posledných dňoch volieb sa jedna strana stala obeťou aj neoprávneného zverejnenia tisícok emailov súvisiacich s kampanou“ (Auchard, ako ho uvádza CSE).

• „Kybernetická vojna, kedysi prevažne hypotetická hrozba, sa stala dobre zdokumentovanou realitou a útoky cudzích štátov sú teraz skutočnou hrozbou pre národný online volebný systém. Ešte v máji 2014 sa útočníci spojili s Ruskom zamerali na volebnú infraštruktúru na Ukrajine a nakrátko odložili sčítanie hlasov“ (Springall et al. 2014).

¹²⁰ CSE 2017.

¹²¹ „Počítačová kriminalita vo volebnom procese: úloha Budapešťianskeho dohovoru“, <http://www.venice.coe.int/files/15EMB/Alexander_Seger.pptx>.

- manipulácie s volebnými prístrojmi pre ovplyvnenie výsledkov;
- zasahovania do fungujúceho systému (napríklad znefunkčnením internetových služieb či stránok počas volebného dňa);
- nezákonného prístupu do počítačov na účel krádeže, úpravy či rozšírenia citlivých informácií, ako napríklad krádež údajov o volebnej kampani na použitie pri informačných operáciách.

114. Takéto útoky zjavne predstavujú formy počítačovej kriminality, ako ju definuje Budapešťiansky dohovor o počítačovej kriminalite, napríklad nezákonný prístup do počítačového systému (čl. 2), nezákonné zachytenie údajov (čl. 3), zasahovanie do údajov a systému (čl. 4 a 5) a iné. V súčasnosti viac ako šesťdesiat zmluvných strán transponovalo tieto ustanovenia do svojich vnútroštátnych poriadkov.

115. Ako už bolo spomenuté, tieto útoky vedú k zásahom do viacerých základných práv garantovaných EDLP a inými medzinárodnými dohovormi o ľudských právach. Môžu byť vedené vládami, politickými stranami/kandidátmi, cudzími mocnosťami alebo súkromnými aktérmi. V tomto smere je potrebné zdôrazniť, že podľa EDLP majú štáty pozitívny záväzok zaistiť slobodné a bezpečné voľby a garantovať rešpektovanie okrem iného práva na súkromný život či slobody prejavu.

116. Druhý typ útoku zahŕňa (dez-)informačné operácie, ktoré síce nepredstavujú počítačovú kriminalitu, ale porušujú pravidlá ochrany osobných údajov, financovania politiky, mediálneho pokrytia či vysielania o voľbách, čiže pravidlá, ktoré majú zaistiť slobodné, spravodlivé a jasné voľby. Dôkazy svedčiace o porušení týchto pravidiel majú často elektronickú formu, čiže ide o dôkazy nachádzajúce sa v počítačových systémoch. Preto je podstatné, aby štáty poskytli svojim orgánom činným v trestnom konaní nevyhnutné právomoci na zaistenie takýchto dôkazov. Od zmluvných strán Budapešťianskeho dohovoru sa to vyžaduje na základe čl. 16 až 21.

117. Medzinárodné štandardy vskutku poukazujú na zodpovednosť štátov predchádzať nerovnosti v mediálnom pokrytí volebných kampaní a zaistiť informovanosť občanov o politických stranách, aby vedeli urobiť informovaný politický výber svojich zástupcov. Okrem povinnosti zabrániť nezákonnému zásahu do výkonu základných práv majú štáty taktiež pozitívny záväzok predchádzať tomu, aby došlo k porušeniam práv tretími stranami. Pre konkurujúce práva je potrebné zabezpečiť spravodlivú rovnováhu. Bežnými scenármi takýchto konfliktov sú nezákonné použitie údajov z voličského registra na volebné účely alebo nadmerné zverejňovanie osobných údajov kandidáta v zápale politickej kampane. Väčšina demokracií by prvý scenár považovala za jasné porušenie práva na súkromie a porušenie rovnosti volieb, a to napriek tomu, že politické strany majú právo na prístup k takýmto informáciám. Možno však tvrdiť, že povaha politickej diskusie by umožňovala rozšírené povolenie politického práva na prejav na úkor práva kandidáta na súkromie za podmienky, že tieto prejavy nepredstavujú jasné ohováranie. Súčasné demokracie sú na tieto scenáre zvyknuté a vytvorili pomerne bohatý súbor rozhodnutí a vnútroštátnej legislatívy v tejto veci.

118. Počas najmenej dvoch desaťročí viaceré krajiny experimentovali s internetovým hlasovaním s cieľom posilniť politické práva. Napríklad Švajčiarsko v roku 2000 spustilo

projekt „vote électronique“, aby otestovalo jeho spoľahlivosť. Krajina odvtedy uskutočnila viac ako 150 pokusov na federálnej úrovni a niektoré kantóny umožnili svojim občanom elektronické hlasovanie. Nórsko v roku 2008 taktiež spustilo testovanie internetového hlasovania a urobilo niekoľko pokusov počas miestnych volieb v roku 2011 a v parlamentných voľbách v roku 2013. V Kanade je internetové hlasovanie dostupné v niektorých provinciách (Ontario a Nové Škótsko) od roku 2003. Najúspešnejší experiment zrejme uskutočnilo Estónsko, kde diskusie o internetovom hlasovaní prebiehali od roku 2001, a od roku 2005 sa považuje za doplnkovú a právne záväznú formu hlasovania.¹²²

119. Bez ohľadu na úspech niektorých pokusov vyvolalo používanie internetu na odovzdávanie volebných hlasov niekoľko obáv o bezpečnosti. „*Estónsko bolo prvou krajinou na svete, ktoré použilo internetové hlasovanie celonárodne a v súčasnosti sa viac ako 30 % hlasov odovzdáva online*“, ale vedci z Univerzity v Michigene a Open Rights Group zistili, že „*estónsky systém elektronického hlasovania má vážne architektonické obmedzenia a procesné medzery, ktoré potenciálne ohrozujú integritu volieb*“ do tej miery, že „*útočníci by sa mohli zamerať na volebné servery alebo účty voličov, aby upravili výsledky volieb či podkopali legitimitu systému*“. Na základe svojich obáv dospeli k záveru, že „*raz, ak dôjde k zásadným pokrokom v počítačovej bezpečnosti, rizikový profil pre online hlasovanie môže byť priaznivejší, ale neveríme, že elektronické hlasovanie môže byť dnes bezpečné*“.¹²³

120. V tejto súvislosti je potrebné zdôrazniť, že cieľom dezinformácií a celoplošného digitálneho zasahovania do politickej diskusie nie je rozvrátiť samotný mechanizmus volieb, ale skôr podkopať dôveru verejnosti v proces a politický systém. Otvorenosť liberálnej demokracie je silnou stránkou, ale aj slabosťou. Digitálnym technológiám by sa nemalo dovoliť oslabiť dôveru verejnosti vo volebný systém, preto je potrebné uistiť verejnosť o bezpečnosti týchto technológií. Digitálne technológie by preto mali byť zavedené postupne a nemali by sa kombinovať s tradičnými postupmi. Inovácia nemôže ísť na úkor právnych požiadaviek vrátane bezpečnosti.

121. Tieto výzvy je potrebné riešiť s ohľadom na ich vzájomnú závislosť, čo znamená, že je potrebné uznať (1) nadnárodný charakter problému a (2) zásadnú úlohu, ktorú zohrávajú strážcovia digitálnych komunikačných systémov a internetovej telekomunikačnej siete (teda internetoví poskytovatelia služieb) pri vyšetrovaní a stíhaní počítačovej kriminality. Je potrebné posilniť medzinárodný právny rámec, aby sa vytvorili účinnejšie mechanizmy nadnárodnej spolupráce medzi národmi a súkromnými aktérmi a ak je to možné, zabezpečila sa väčšia jednotnosť vnútroštátnych právnych predpisov. Nakoniec sa zdá, že riešením je „*prispôbiť ústavný rámec moderných demokracií*“ novému elektronickému prostrediu, v ktorom sa darí počítačovej kriminalite a v ktorom vlády, korporácie a občania vzájomne reagujú a umožňujú existenciu demokracie“.¹²⁴

¹²² ACE Project 2018.

¹²³ Springall et al. 2014.

¹²⁴ Mecinas Montiel 2016, s. 427.

B. Výzvy pre deliberatívnu demokraciu

122. Princíp slobodného volebného práva je založený na slobode voličov formovať názory. Táto sloboda, ktorá sa sčasti prekrýva s rovnosťou volebných príležitostí, si vyžaduje, aby štát a verejné orgány vo všeobecnosti rešpektovali svoju povinnosť nestrannosti, najmä tam, kde sa využívajú masmédiá, plagáty, právo demonštrovať na verejných priestranstvách a ide o financovanie strán a kandidátov.¹²⁵ Sloboda vytvoriť si názor zahŕňa právo byť správne informovaný pred prijatím rozhodnutia, právo na súkromné online vyhľadávanie a právo na dôvernú komunikáciu na internete. Monitorovanie online aktivity ľudí bez ich súhlasu na účely pochopenia a využívania ich správania podkopáva tieto práva.

123. Technológia mení spôsob manažovania volebných kampaní. Internet je mocnou platformou pre politické strany na prezentovanie ich programu voličom a mobilizovanie väčšej základne pre podporu ich cieľov. Náklady na komunikáciu s voličmi prostredníctvom tohto média môžu byť podstatne nižšie vďaka dostupnosti bezplatných blogov, platforiem na zdieľanie videí a sociálnym médiám. Malé politické strany s limitovanými zdrojmi, ale najmä nezávislí kandidáti môžu profitovať z tohto typu komunikácie.

124. Zmeny v produkcii a konzumácii obsahu, ktorý sa týka volieb, však môže predstavovať výzvy pre uznávané inštitúcie a princípy regulácie volebnej komunikácie, ako sú sloboda združovania, limity výdavkov a regulácia politickej reklamy. Podkopávajú schopnosť súčasnej právnej regulácie udržiavať rovnaké podmienky volebnej komunikácie medzi novými a etablovanými, medzi bohatými a chudobnými, medzi kampaniami podnikov a občianskej spoločnosti. Noví sprostredkovatelia a platformy teraz zastávajú dôležité pozície strážcov, ktoré kedysi zastávali novinári, ale neprijali ešte etické záväzky médií. Predstavuje to hrozbu pre voľby a potenciál pre vznik korupčných praktík. Volebná štúdia Rady Európy z roku 2017 identifikuje obavy vo vzťahu k spravodlivosti volebného procesu, napríklad nedostatočná transparentnosť vedenia kampaní, výdavkov, správ a algoritmy používané na digitálne reklamy, obrovské zásahy do súkromia, nedostatok žurnalistického filtrovania a overovania si faktov v politických oznamoch, zvýšenie počtu dezinformácií a medzery v regulácii volebných kampaní (t. j. nemožnosť presadzovať moratórium), čo vedie k záveru, že *„súčasná právna úprava už nepostačuje na zachovanie rovnakej úrovne politickej súťaže a na obmedzenie úlohy peňazí vo voľbách“*.¹²⁶

125. Tradičná volebná kampaň je spochybňovaná novými formami komunikačných kanálov, ktoré nielenže pomáhajú šíreniu správ za nízke náklady, ale využívajú rôzne marketingové techniky, ktoré na konkrétnu skupinu voličov pôsobia priaznivejšie. Mechanizmy ako používanie personalizovaných reklám a správ, ktoré sa dajú využiť vo všetkých oblastiach marketingu, sú v súčasnosti využívané v oblasti volieb, čím poskytujú niektorým aktérom,

¹²⁵ Benátska komisia, Kódex dobrej praxe vo volebných záležitostiach, dôvodová správa, Slobodné voľby.

¹²⁶ Volebná štúdia Rady Európy z roku 2017; Pozri tiež správu z roku 2018 o „*Dezinformačných a volebných kampaniach*“ (Doublet, 2018, CDDG(2018)11), v ktorej sa navrhuje, aby Rada Európy pripravila široký akčný program v tejto oblasti. Odporúča napríklad definovať dĺžku volebných kampaní, aby sa predišlo riziku veľkých digitálnych kampaní pred obdobím volebnej kampane; vyžadovať digitálne stopy, aby sa vedelo, kto stojí za online platformami; získať informácie o výdavkoch vynaložených na digitálne volebné kampane prostredníctvom online platforiem; zákaz financovania digitálnych volebných výdavkov zahraničnou fyzickou alebo právnickou osobou.

ktorý majú prístup k týmto mechanizmom, netransparentnú výhodu. Volebné správy sa tak stali čoraz viac personalizovanými. Tí, ktorí vytvárajú kampane, nemusia myslieť na väčšinu voličov, ktorí sú už rozhodnutí o svojom hlase. Môžu sa sústrediť na malé skupiny voličov, ktorí svoje názory menia. Nové techniky kampane poskytujú možnosť maskovať personalizované oznamy za všeobecné, politicky neutrálne oznamy. Takýto skrytý vplyv je podporovaný používaním sociálnych platforiem nielen pre ich algoritmy na spracovanie údajov, ale najmä preto, že poskytujú možnosť priamo sa zacieliť na špecifickú skupinu osôb s personalizovanými reklamami a správami, zatiaľ čo zacielené osoby nevedia identifikovať personalizáciu. Pomocou technológií sa techniky volebných kampaní presunuli k evolučnému konceptu prístupu jeden na jedného; Joseph Pine to nazýva „*masové prispôsobenie*“.¹²⁷ Na rozdiel od tradičných masmédií, ktoré v zásade deklarujú svoje politické zafarbenie, ktoré je ich čitateľom známe, internetoví poskytovatelia nemajú deklarovанú politickú príslušnosť, takže pri absencii jasného náznaku, že nimi poskytované informácie sú v skutočnosti stránickou politickou reklamou, môžu byť používatelia pod domnienkou, že sú tieto informácie politicky neutrálne.

126. Rob Epstein preskúmal manipuláciu s volebnými preferenciami, konkrétnejšie vplyv optimalizácie vyhľadávačov (najmä Google kvôli jeho prevahe) na preferencie hlasovania [označované ako efekt manipulácie prostredníctvom vyhľadávačov (*Search Engine Manipulation Effect, SEME*)].¹²⁸ Podľa štúdie z roku 2015 majú vyššie umiestnené položky vo výsledku vyhľadávania spojené s webovými stránkami, ktoré uprednostňujú jedného kandidáta, vplyv na názory nerozhodnutých voličov.¹²⁹ Dôkazy z piatich experimentov v dvoch krajinách naznačujú, že „(i) *neobjektívna optimalizácia môže presunúť volebné preferencie nerozhodnutých voličov o 20 % alebo viac, (ii) presun môže byť oveľa väčší u niektorých demografických skupín, a (iii) takéto optimalizácie môžu byť zamaskované tak, že ľudia netušia o manipulácii*“. Autori štúdie dospeli k záveru, že „*ak Google vo voľbách uprednostní jedného kandidáta, jeho vplyv na nerozhodnutých voličov môže pokojne rozhodnúť o výsledku volieb*“. Hoci výsledky štúdie by bolo potrebné potvrdiť ďalším výskumom, možno súhlasiť so záverom autorov, že je to „*oveľa znepokojivejšie, že obchod s optimalizáciou vyhľadávačov nie je regulovaný*“.

127. V tejto súvislosti je potrebné mať na pamäti, že optimalizácia vyhľadávačov je výsledkom komplexných algoritmov a nie sú nevyhnutne vytvorené na účel manipulovania, ale sú zamerané na poskytovanie najaktuálnejších, najrelevantnejších a najnovších výsledkov vyhľadávania; algoritmy sa však dajú manipulovať prostredníctvom rôznych webových stránok, ktoré sa snažia získať lepšie umiestnenie vo vyhľadávaní. V skutočnosti vidíme, že Google neustále vylepšuje algoritmy vyhľadávania, aby predišiel takýmto zásahom. V každom prípade, či je manipulácia úmyselná alebo nie, efekt manipulácie prostredníctvom vyhľadávačov má dva vážne dôsledky pre demokraciu: moc manipulovať preferenciami môžu využiť súkromní aj verejní aktéri na ovplyvnenie rovnosti volieb a skutočnosť, že používatelia vyhľadávačov si nie sú vedomí kritérií (kódovania) mechanizmu na umiestnenie

¹²⁷ PINE, B.J., II. (1993). *Masové prispôsobenie: Nová hranica hospodárskej súťaže*. Harvard Business School Press, Boston.

¹²⁸ Epstein 2016.

¹²⁹ Epstein a Robertson 2015.

vo výsledkoch vyhľadávania, čo bráni ich schopnosti robiť plne informované rozhodnutia, a teda uplatňovať slobodu prejavu.

128. Efekt manipulácie prostredníctvom vyhľadávačov nie je viazaný výlučne na online vyhľadávače. Sociálne médiá sa tiež riadia kódovaním, ktoré nie je zaujaté. Spoločnosti ako Facebook, Twitter alebo Instagram na rozdiel od tradičných médií nie sú orientované politicky; primárne ich motivuje komerčný zisk a štruktúry svojich kódov vytvárajú v súlade s týmito záujmami. Algoritmy, ktorými sa riadia sociálne médiá, podporujú čiastkové a niekedy iluzórne chápanie politiky a demokracie, pretože poskytujú neobjektívne informácie, ktoré odrážajú čiastkové záujmy a správanie ich užívateľov.¹³⁰

129. Spoločnosti, ktoré vlastnia sociálne médiá a vyhľadávače, môžu skutočne tvarovať spoločenské interakcie online nielen preto, že majú moc kódovať prostredie týchto interakcií, ale aj pre ich schopnosť profilovať a predvídať hodnoty a správanie ich používateľov. Tieto spoločnosti majú jednoduchý prístup k *«digitálnym záznamom o správaní, napríklad „páči sa mi“ na Facebooku, histórii vyhľadávania, dopytom na vyhľadávanie alebo histórii nákupov, ktoré možno použiť na automatické a presné predpovedanie radu vysoko citlivých osobných hodnôt vrátane: sexuálnej orientácie, etnickej príslušnosti, náboženských a politických názorov, povahových vlastností, inteligencie, šťastia, používania návykových látok, odlúčenia rodičov, veku a pohlavia»*.¹³¹ Títo developeri dokážu spracovať uvedené informácie na vytvorenie veľmi presných profilov svojich používateľov, predpovedať ich preferencie, a dokonca zacieliť na nich individualizovanými údajmi a reklamami s cieľom podporiť alebo odradiť ich od konkrétneho správania.¹³²

130. Spoločnosti ako Facebook a Google na jednej strane monetizujú informácie o svojich užívateľoch a predávajú ich na trhu. Kupujúci, na strane druhej, používajú tieto informácie so žiadnou alebo veľmi malou zodpovednosťou na ovplyvnenie spotrebiteľov a niekedy aj voličov prostredníctvom *„na mieru šitých reklám založených na osobných údajoch“*.¹³³ Presne toto bol prípad Cambridge Analytica. Súčasný biznis model mnohých webových stránok je ponúkať obsah výmenou za osobné údaje. Skutočnosť, že ľudia sa vzdávajú svojich osobných informácií výmenou za používanie služieb zadarmo, umožňuje rozsiahle zbieranie dát webovými stránkami, čo môže viesť k ich použitiu a zneužitiu viacerými subjektmi.

131. Ak to aj bola pravda, že používatelia sociálnych sietí musia výslovne prijať všeobecné podmienky ochrany osobných údajov stanovené spoločnosťami, ktoré vlastnia sociálne

¹³⁰ Van Dijck 2013; McChesney 2013.

¹³¹ Graepel et al. 2013.

¹³² Napríklad podľa účtu Roberta Epsteina (2016):

„...štúdia Roberta M. Bonda, teraz profesora politológie na Ohio State University a ďalších, publikovaná v časopise Nature v roku 2012, opísala eticky pochybný experiment, v ktorom v deň volieb v roku 2010 Facebook poslal pripomienky „chod' von a voľ“ viac ako 60 miliónom používateľov. Pripomenutia spôsobili, že hlasovalo asi 340 000 ľudí, ktorí by inak nemohli. Jonathan Zittrain, profesor medzinárodného práva na Harvardskej univerzite, píšuci v časopise New Republic v roku 2014, poukázal na to, že vzhľadom na obrovské množstvo informácií, ktoré zhromaždil o svojich používateľoch, môže Facebook jednoducho posielať takéto správy iba ľuďom, ktorí podporujú jednu konkrétnu stranu alebo kandidáta, a to by mohlo ľahko zvrátiť tesné voľby – pričom nikto nevie, že k tomu došlo. A keďže reklamy, podobne ako hodnotenia vo vyhľadávaní, sú efemérne, manipulácia volieb týmto spôsobom by nezanechala žiadnu papierovú stopu.“

¹³³ Christopher Wylie, ako ho cituje Guimón 2018.

médiá, majú len malú alebo žiadnu kontrolu nad tým, kto je oprávnený „kupovať“ ich osobné údaje alebo ako sa majú použiť. Táto situácia podkopáva základné právo na súkromie a ochranu osobných údajov, pretože ochromuje schopnosť užívateľa obmedzovať používanie svojich osobných údajov.¹³⁴ Ústavný súd Španielska vo svojom rozsudku č. 292/2000 stanovil, že „základné právo na ochranu osobných údajov... dáva nositeľovi tohto práva moc ukladať tretím stranám povinnosť uskutočniť nejaké správanie alebo sa ho zdržať, teda dáva jednotlivcom právomoc rozhodovať o svojich údajoch... pričom táto právomoc je zbytočná, ak nositeľ nevie o tom, ktoré informácie majú v rukách tretie strany, kto sú tretie strany a na čo sa jeho informácie použijú.“¹³⁵

132. Používanie a zneužívanie osobných údajov na volebné účely maskované ako sloboda podnikania môže predstavovať vážnu hrozbu pre slobodu a rovnosť volieb najmenej v troch smeroch: po prvé, súkromné subjekty by mohli použiť tieto údaje na priamy nenáležitý vplyv na volebnú súťaž; po druhé, internetové spoločnosti a sociálne médiá by, argumentujúc slobodou podnikania, mohli obmedziť prístup k týmto údajom v závislosti od ich politických preferencií; a po tretie, monetizácia osobných údajov predstavuje výzvu pre dohľad nad peniazmi v politickej kampani.

133. Riziko podkopania práva na súkromie, slobodných/rovných volieb a slobody prejavu a presvedčenia (a ako tvrdia niektorí experti, aj slobody myslenia) naznačuje potrebu regulovať komerčné práva internetových spoločností a sociálnych sietí. Úplný zákaz „monetizovania údajov“ by však bránil aj rozvoju internetu a následne prístupu k zjavne bezhraničnému zdroju politických informácií a demokratickej aktivity. Kým spoločnosť nenájde nové formy financovania internetu, prílišné obmedzenie monetizácie osobných údajov by mohlo obmedziť základné politické práva, ako sú sloboda prejavu a sloboda združovania a zhromažďovania. Paradoxom je, že rovnaké technológie, ktoré rozšírili možnosti prejavov, sú tie, ktoré takéto možnosti obmedzujú.¹³⁶

134. Právo na prístup k internetu je nevyhnutnou podmienkou na uplatnenie slobody prejavu, ktorá je nevyhnutnou podmienkou existencie demokratickej spoločnosti.¹³⁷ Avšak samotný

¹³⁴ Davara 2003, s. 43 – 44.

¹³⁵ Ako uvádza Davara 2003. Vlastný preklad.

¹³⁶ Slovanmi Laidlaw (2015, s. xi – xii): „Komunikačné technológie, ktoré umožňujú alebo znemožňujú účasť na online diskusii, sú v súkromnom vlastníctve... Preto sa nevyhnutne spoliehame na to, že tieto spoločnosti budú uplatňovať právo na slobodu prejavu online, a tak sa stanú strážcami nášho online zážitku... Naše spoliehanie sa na týchto strážcov pri uplatňovaní práva na slobodu prejavu malo dva účinky. Po prvé, títo strážcovia sa čoraz viac stávajú cieľom právnych opatrení navrhnutých s cieľom využiť ich schopnosť regulovať správanie tretích strán... Po druhé... regulácia prejavu v kybernetickom priestore bola do značnej miery ponechaná na samoreguláciu, podobne ako regulácia internetu bola vo všeobecnosti slabá... Výsledkom je systém súkromnej správy fungujúci popri zákone, bez akýchkoľvek záruk ľudských práv, ktoré sa bežne očakávajú od štátom riadených systémov, ako sú zásady zodpovednosti, predvídateľnosti, dostupnosti, transparentnosti a proporcionality.“

¹³⁷ Lingens proti Rakúsku, sťažnosť č. 9815/82 (EŠEP, 8. júla 1986): „sloboda prejavu, ako je garantovaná v čl.10 ods. 1 EDLP, predstavuje jeden zo základných základov demokratickej spoločnosti.“ Okrem toho v prípade Ahmet Yildirim proti Turecku (sťažnosť č. 3111/10, 18. decembra 2012) EŠEP rozhodol, že blokovanie internetu môže byť „v priamom rozpore so skutočným znením čl. 10 ods. 1 EDLP, podľa ktorého sú práva uvedené v tomto článku zabezpečené „bez ohľadu na hranice“.

Pozri tiež Laidlaw (2015, s. 19 – 21):

internet predstavuje rôzne hrozby pre demokraciu. Keďže sociálne médiá a internet nie sú (a nemali by byť) priestorom, ktorý sa nachádza mimo právnej regulácie¹³⁸, je naliehavo potrebné nájsť riešenia pre tieto konflikty práv, ktoré umožnia rozumnú ochranu súkromia, politických a komerčných práv.

135. Neexistencia alebo nedostatok právnej regulácie internetu a sociálnych médií spôsobili, že používatelia nemajú zákonný spôsob ochrany ich údajov, ale najmä ich slobody prejavu a demokratických práv. Na jednej strane je problematické, ak súkromné technologické spoločnosti cenzurujú obsah, ktorý oni považujú za „škodlivý“ bez toho, aby niesli zodpovednosť a ich opatrenia boli transparentné.

136. Na druhej strane, pozitívny záväzok štátu zabrániť nenáležitým zásahom tretích strán nesmie viesť k neprimeraným štátnym zásahom prostredníctvom nadmernej alebo prehnanej regulácie, ktorá môže viesť k podkopaniu rovnakých práv, ktoré sa snaží chrániť. Neodôvodnené štátne sledovanie súkromnej komunikácie a rôzne spôsoby, ktorými je možné používať online platformy na (či už úmyselné alebo neúmyselné) ovplyvnenie informačného toku, priamo obmedzuje slobodu prejavu, brzdí demokratický dialóg a porušuje princípy inštitucionálnej neutrality a volebnej rovnosti. Hoci je v tomto smere pochopiteľné, že v súčasnosti má mnoho štátov na programe legislatívne riešenie otázky „fake news“, môže to predstavovať hrozbu pre slobodu prejavu a informácií, berúc do úvahy, že expresívne prejavy sú chránené medzinárodnými dokumentmi v oblasti ľudských práv, napríklad čl. 10 EDP. Ak sa štátnym orgánom umožní zasahovať do verejnej diskusie, môžu to zneužiť na umlčanie disidentov a prostredníctvom obmedzenia kritiky spoločenských postojov zabrániť diskusii, ktorá spochybňuje hlavné myšlienkové prúdy. Benátska komisia zdôraznila, že „*masmédiá nie sú jedinou kategóriou, ktorá by mala nárok na vysokú mieru slobody prejavu. Osoby, ktoré ovplyvňujú informácie a myšlienky o verejných záujmoch a prispievajú do verejnej diskusie o týchto záležitostiach vrátane osôb, ktoré realizujú kampaň a volených zástupcov, by mali mať na účel poskytovať presné a spoľahlivé informácie vysokú úroveň slobody prejavu vrátane určitého stupňa prehánania a dokonca provokácie, kým konajú v dobrej viere a sú náležité opatrení.*“¹³⁹

137. Vykonávať filtrovanie, blokovanie a stiahnutie nezákonného obsahu na internete s cieľom bojovať proti zločinom z nenávisťi a proti národnej bezpečnosti, ako aj ochrániť duševné vlastníctvo a súkromie či práva na ochranu dobrého mena je nevyhnutné, ale

„Demokracia bola vždy stelesnená v komunikačných praktikách a sloboda prejavu bola súdmi dôsledne označená za ústrednú úlohu demokracie. Vo veci *Lingens v. Rakúsko* EDP slávne poznamenal, že sloboda prejavu je jedným zo základných základov demokratickej spoločnosti... Mnohé štáty, ako napríklad Estónsko, Fínsko, Francúzsko, Grécko a Španielsko, legislatívne uznali prístup na internet ako základné právo. V roku 2003 Výbor ministrov Rady Európy prijal Deklaráciu potvrdzujúcu dôležitosť slobody prejavu na internete. Od roku 2010 sme svedkami zmeny paradigmy v uznávaní ľudských práv v kybernetickom priestore na medzinárodnej úrovni. Prístup na internet ako základné právo bol schválený Organizáciou Spojených národov (OSN) v správe Franka La Ruea, osobitného spravodajcu pre presadzovanie a ochranu práva na slobodu presvedčenia a prejavu... Rada OSN pre ľudské práva ju v roku 2021 doplnila prijatím rezolúcie potvrdzujúcej slobodu internetu ako základné ľudské právo, najmä právo na slobodu prejavu.“

¹³⁸ Volebný tribunál Mexika, g.

¹³⁹ CDL-AD(2013)024, Stanovisko k právnej úprave Azerbajdžanskej republiky týkajúcej sa ochrany pred ohováraním, ods. 37.

chúlostivé, a možno to zneužiť do takej miery, že povedie k cenzúre a nezákonnému umlčaniu politických oponentov. Všetky takéto opatrenia musia byť v súlade so zákonom, ktorý zahŕňa presné a úzke vymedzenie súvisiacich trestných činov¹⁴⁰ a ktorý musí sledovať legitímne ciele vymenované v čl. 10 EDĽP. Musia sa dodržať kritériá nevyhnutnosti v demokratickej spoločnosti a primeranosti.¹⁴¹ Musí sa garantovať účinná súdna kontrola nezávislými a nestrannými súdmi.

138. V prípade falošných správ, ktorých väčšina nespadá do žiadnej kategórie, ktorú je možné trestne stíhať, je potrebné použiť alternatívne prostriedky, ako je overovanie faktov (ktoré síce nie je všeliakom, ale je čoraz pokročilejšie a efektívnejšie), programy mediálnej gramotnosti zamerané na vnímanie problému a rozoznanie falošného obsahu a investovanie do kvalitnej žurnalistiky.¹⁴² Štátne orgány budú pri tomto úsilí potrebovať spoluprácu občanov a internetových korporácií.

139. Zároveň je potrebné zdôrazniť, že akékoľvek opatrenia na riešenie informačného zmätku musia byť vytvorené s veľkou opatrnosťou, aby nenarušili „neutralitu siete“. Toto je základným princípom internetu, kde musia poskytovatelia internetových služieb zaobchádzať so všetkými online údajmi rovnako a poskytovať podmienky pre neobmedzený užívateľský prístup bez diskriminácie založenej na obsahu či pôvode. Ochrana demokratickej funkcie internetu pred monopolizáciou súkromnými spoločnosťami si vyžaduje rovnaké zaobchádzanie so všetkými odoslanými či prijatými údajmi bez rozdielu v poplatkoch alebo kvalite služieb.¹⁴³ Zrušenie politiky „neutrality siete“, na čom sa v decembri 2017 dohodla Federálna komisia pre komunikáciu USA¹⁴⁴, umožňuje internetovým poskytovateľom služieb blokovat' alebo obmedzovať (spomaliť) webové stránky a účtovať si za vyššiu rýchlosť sťahovania a nahrávania. Za týchto podmienok možno s online službami, aplikáciami a webovými stránkami zaobchádzať rozdielne z rôznych dôvodov, či už komerčných alebo ideologických, vrátane menej demokratických krajín, kde sú internetoví poskytovatelia služieb vo vlastníctve štátu alebo cenzurovaní a kde môžu byť štátne orgány v pokušení poskytnúť rýchlejšie prístupy provládnym médiám.

140. Hoci nadmerná alebo neadekvátne regulácia internetu môže byť kontraproduktívna a môže brániť dostupnosti a rozvoju internetu a následne aj slobode prejavu a samotnému demokratickému dialógu, problém informačného zmätku nemožno nechať bez pozornosti. Riziko narušenia práva na súkromie v dôsledku zneužitia osobných údajov a zničenie slobody

¹⁴⁰ Pozri napríklad Benátska komisia, Stanovisko k federálnemu zákonu Ruskej federácie o boji proti extrémistickej činnosti, CDL-AD(2012)016.

¹⁴¹ Pozri napríklad Benátska komisia, Stanovisko k zákonu č. 5651 Turecka o regulácii zverejňovania na internete a boji proti trestným činom spáchaným prostredníctvom takéhoto zverejňovania („internetový zákon“), CDL-AD-2016)011.

¹⁴² Porov. správa Rady Európy o informačnom zmätku 2017, ktorá ponúka viac ako 30 odporúčaní pre rôzne zainteresované strany.

¹⁴³ Z hľadiska ústavného práva aj medzinárodného práva ľudských práv je kľúčové brať do úvahy realitu vplyvných aktérov mimo volených orgánov, ktorí bránia realizácii základných práv. Pozri Thorgeirsdóttir, Herdis (2005), Žurnalistika hodná tohto označenia: pozitívna strana čl. 10 EDĽP, Kluwer Law International.

¹⁴⁴ Účinnosť nariadení o neutralite siete prijatých v roku 2015, ktoré sa snažili zastaviť internetových poskytovateľov služieb, aby uprednostňovali stránky a služby, ktoré im platili za zvýšenie rýchlosti prístupu k ich dátam, oficiálne vypršala v júni 2018.

prejavu a volebnej rovnosti spôsobené architektúrou internetu (t. j. efekt manipulácie prostredníctvom vyhľadávačov, epistemické bubliny, echo komory a falošné správy) spolu s nedostatkom regulácie, ktoré nenechali občanom žiadne právne nástroje na ochranu ich osobných a politických práv, sú situácie, ktoré si vyžadujú naliehavé konanie.

141. Toto konanie musí zahŕňať aj silné súkromné subjekty primárne motivované komerčnými záujmami, ktoré majú moc obmedzovať ľudské práva, zároveň však zachovávajú základnú platformu pre demokraciu a uznávajú túto svoju zodpovednosť.

VII. Závery

142. Uskutočnenie demokratických volieb (teda samotná existencia demokracie) nie je možné bez rešpektovania ľudských práv, najmä slobody prejavu a tlače a slobody združovania a zhromažďovania na politické účely vrátane politických strán. Rešpektovanie týchto slobôd je absolútne nevyhnutné najmä počas volebnej kampane. Obmedzenie týchto základných slobôd musí byť v súlade s Európskym dohovorom o ochrane ľudských práv a vo všeobecnosti s požiadavkou, aby mali zákonný základ, boli vo všeobecnom záujme a rešpektovali princíp proporcionality. Právne predpisy by mali ustanoviť jasné pravidlá pre vyváženie konkurujúcich práv, ktoré by mali byť účinne implementované prostredníctvom volebného a všeobecného súdneho mechanizmu.

143. Vzťah medzi demokraciou a digitálnymi technológiami je komplexný. Na jednej strane sa v niektorých demokraciách stali internet a sociálne médiá dominantnou platformou pre politickú interakciu, používanie týchto nástrojov posilnil kritický prístup občanov voči vláde a ich rozsiahle používanie podporuje organizovanie veľkých sociálnych hnutí a uľahčuje interakciu medzi občanmi a politickými stranami. Na druhej strane možno tieto nové nástroje použiť, a skutočne sa používajú, proti voľbám s cieľom potlačiť účasť vo voľbách, manipulovať s volebnými výsledkami a ukradnúť údaje o voličoch; proti politickým stranám a politikom na uskutočnenie počítačovej špionáže na účel nátlaku a manipulácie a na verejné diskreditovanie jednotlivcov; proti tradičným aj sociálnym médiám na šírenie dezinformácií, propagandy a formovanie názorov voličov. Nová digitálna sféra umožňuje nové formy kriminality a monetizácie dát, čo vážne ohrozuje právo na súkromie a modeluje spoločenské interakcie selektívnym (a niekedy strategickým) podávaním alebo skrývaním informácií pred používateľmi, čím podporuje čiastkové pochopenie reality a obmedzuje slobodu prejavu.

144. Internetové služby obohatili a diverzifikovali spravodajské zdroje, uľahčili prístup jednotlivcov k informáciám a k rozhodovaniu o najvážnejších otázkach v demokracii, najmä o voľbe ich zákonodarcu. Informačný zmätok (falošné, zavádzajúce a škodlivé informácie) však môže zároveň deformovať komunikačný ekosystém do tej miery, že voliči môžu byť v rozhodovaní vážne zaťažení zavádzajúcimi, manipulujúcimi a nepravdivými informáciami vytvorenými na ovplyvnenie ich hlasovania. Toto prostredie potenciálne podlamuje výkon práva na slobodné voľby a vytvára nebezpečenstvo pre fungovanie demokratického systému.

145. Malá skupina veľmi mocných súkromných aktérov, ktorí doslova vlastnia informačné toky, má svoje vlastné komerčné záujmy a práva, ktoré kolidujú s občianskymi a politickými právami a volebnými princípmi. Internetoví poskytovatelia prebrali na seba úlohu strážcu, ktorá pôvodne prislúchala tradičným médiám, ale bez toho, aby prijali etické záväzky médií.

Súkromné technologické spoločnosti tak cenzurujú obsah, ktorý považujú za „nebezpečný“ bez toho, aby mali právnu zodpovednosť a ich opatrenia boli transparentné. Je pravdou, že sociálne platformy nedávno prijali sériu opatrení na prevenciu pred falošnými správami a limitovanie ich šírenia v období volieb. Existuje koncept spoločenskej zodpovednosti korporátov, akási samoregulácia spoločností s prvotným cieľom „neškodiť“ a dodržiavať zásady právneho štátu a ľudské práva vrátane práva na náhradu pre svojich používateľov a zodpovednosti za svoje produkty (podľa obchodného práva, súťažného práva, práva životného prostredia a pod).¹⁴⁵ Deje sa to však na dobrovoľnom a neregulovanom základe bez uznaného právneho rámca založeného na princípoch právneho štátu.

146. Zatiaľ čo štáty majú pozitívny záväzok predchádzať nezákonnému zásahu do občianskych a politických práv tretích strán, nezákonný štátny zásah prostredníctvom prílišnej alebo neprimeranej právnej úpravy môže viesť k podlomeniu samotných práv, ktoré sa tým majú chrániť. Nezákonné štátne sledovanie súkromnej komunikácie a rôzne spôsoby, ktorými možno online platformy využívať (či už úmyselne alebo neúmyselne), ovplyvňujú informačný tok, priamo obmedzujú slobodu prejavu, bránia demokratickému dialógu a zasahujú do princípu inštitucionálnej neutrality a volebnej rovnosti. Ak sa štátnym orgánom umožní zasahovať do verejnej diskusie, môžu to zneužiť na umlčanie disidentov a prostredníctvom obmedzenia kritiky spoločenských postojov zabrániť diskusii, ktorá spochybňuje hlavné myšlienkové prúdy. Filtrovanie, blokovanie a stiahnutie nezákonného obsahu na internete s cieľom bojovať proti zločinom z nenávisťi a proti národnej bezpečnosti, ako aj ochrániť duševné vlastníctvo a súkromie či práva na ochranu dobrého mena musia byť v súlade so zákonom, ktorý obsahuje presné a úzke vymedzenie súvisiacich trestných činov, a musí sledovať legitímne ciele uvedené v čl. 10 EDLP. Kritériá nevyhnutnosti v demokratickej spoločnosti a proporcionality musia byť vždy rešpektované. Musí byť zaistená efektívna súdna kontrola nezávislými a nestrannými súdmi.

147. Pokiaľ ide o „falošné správy“, je potrebné použiť alternatívne prostriedky, ako sú overovanie faktov, programy mediálnej gramotnosti zamerané na vnímanie problému a rozoznanie falošného obsahu a investovanie do kvalitnej žurnalistiky.

148. Zároveň je potrebné zdôrazniť, že každé opatrenie na riešenie problému informačného zmätku musí byť vytvorené s veľkou opatrnosťou, aby nepodkopalo princíp „neutrality siete“. Internet by mal ostať otvorenou platformou.

149. Aby sme mohli čeliť týmto výzvam, je potrebné zabezpečiť niekoľko opatrení zo vzájomne závislého a globálneho hľadiska, najmä:

Čo sa týka volebnej demokracie:

- A. kriminalizovať kybernetické útoky proti dôvernosti, integrite a dostupnosti volebných počítačov a údajov v súlade s Budapešťanskou konvenciou o počítačovej kriminalite:

¹⁴⁵ Facebook, Google a Twitter sú signatármi Kódexu postupov proti dezinformáciám a zaviazali sa každý mesiac podávať správy o opatreniach prijatých pred voľbami do Európskeho parlamentu v máji 2019: pozri aprílové správy o implementácii Kódexu postupov, <<https://ec.europa.eu/digital-single-market/news-redirect/651264>>.

- B. poskytnúť orgánom činným v trestnom konaní potrebné právomoci na zabezpečenie elektronických dôkazov o porušení pravidiel pre ochranu osobných údajov, financovanie politiky, mediálne pokrytie alebo vysielanie volieb;
- C. pripraviť sa na riešenie mimoriadnych situácií a zaviesť organizáciu krízového manažmentu; národné riadiace orgány pre voľby by mali mať k dispozícii primerané zdroje a odbornú prípravu na prijímanie digitálnych technológií a riešenie súvisiacich rizík kybernetickej bezpečnosti;

Pokiaľ ide o deliberatívnu demokraciu:

- D. uznať (1) nadnárodnú povahu problému a (2) zásadnú úlohu, ktorú zohrávajú internetoví sprostredkovatelia (t. j. internetoví poskytovatelia služieb, vyhľadávače a spoločnosti sociálnych médií);
- E. posilniť medzinárodný rámec (1) na vytvorenie účinnejších mechanizmov nadnárodnej spolupráce medzi národmi a súkromnými aktérmi a, ak je to možné, (2) zabezpečiť väčšiu jednotnosť vnútroštátnych právnych predpisov;
- F. pracovať na regulačnom a súdnom modeli založenom na spoločnej zodpovednosti súkromných a verejných aktérov a na viacerých regulačných prístupoch a prístupoch k riešeniu konfliktov. Takýto model by mohol zahŕňať aspoň štyri stratégie, pričom všetky sú schopné ustavične sa prispôsobovať neustále sa meniacemu prostrediu internetu a komunikačných technológií:
 - podporovať ďalší výskum a spoluprácu medzi volebnými orgánmi, akademickými pracovníkmi a odborníkmi z praxe s cieľom posúdiť skutočný vplyv digitálnych technológií na volebné procesy a účinnosť prijatých opatrení;
 - podporovať vzdelávanie na posilnenie právnej a demokratickej kultúry medzi občanmi;
 - podporovať samoreguláciu, napríklad povinné prijatie etických kódexov a kódexov sociálnej zodpovednosti podnikov, medzi internetovými poskytovateľmi služieb, vyhľadávačmi a spoločnosťami sociálnych médií; a
 - poskytnúť nápravné mechanizmy v zákonoch, politikách a alternatívnych mechanizmoch riešenia konfliktov.

150. Na úrovni Rady Európy sa urobilo už veľa na uspokojenie už spomínaných výziev. Okrem iného Budapešťiansky dohovor poskytuje viacero nástrojov na prevenciu počítačovej kriminality (vrátane volebného procesu) a pre medzinárodnú spoluprácu zameranú na zaistenie elektronických dôkazov; čo je dôležité, súčasná práca na 2. dodatkovom protokole by mala umožniť ďalšie možnosti podpory medzinárodnej spolupráce a prístupu k dátam uloženým na internetových serveroch (*cloud*). Okrem toho existuje celý rad právnych noriem na ochranu súkromia a osobných údajov v kontexte sociálnych médií. Ako univerzálna dohoda o ochrane osobných údajov by mal slúžiť Modernizovaný dohovor o ochrane jednotlivcov s ohľadom na automatické spracovanie osobných údajov, ku ktorému sa môže pripojiť každá krajina na svete a ktorý stanovuje medzinárodné štandardy. Vyvinulo sa aj veľa právnych nástrojov na zaistenie slobodných volieb, najmä prostredníctvom regulácie financovania volebnej kampane a opatrení na prevenciu nerovnosti mediálneho pokrytia počas volieb na internete aj mimo neho.

151. Viaceré dokumenty Rady Európy naznačujú, že je priestor pre ďalšie vylepšenia. Konkrétne Správa o informačnom zmätku Rady Európy z roku 2017 navrhuje viaceré odporúčania pre vlády, ministerstvá školstva, organizácie médií, technologické spoločnosti a občiansku spoločnosť s cieľom vyriešiť výzvy, ktoré predstavuje narastajúci počet falošných, zavádzajúcich a škodlivých informácií a ich vplyv na demokratické procesy; štúdia Rady Európy z roku 2017 o voľbách dospela k záveru, že súčasný právny rámec už nepostačuje na udržanie rovnosti politickej súťaže a na obmedzenie úlohy peňazí vo voľbách, a navrhuje viacero opatrení na nápravu tejto situácie.

152. Vzhľadom na hlavný výsledok týchto dokumentov a štúdie, nedávny posun vo vplyve internetových kanálov na volebnú komunikáciu si vyžaduje opatrenia v týchto oblastiach:

- A. prehodnotenie pravidiel a regulácie politickej reklamy: pokiaľ ide o prístup k médiám (aktualizácia vysielacích kvót, limitov a kategórií reportáží, zavedenie nových opatrení na pokrytie internetových médií, platforiem a iných služieb, riešenie dôsledkov cielenia na malé skupiny) a o výdavky (rozšírenie rozsahu komunikačných kanálov, ktoré sú pokryté legislatívou, riešenie monitorovacích kapacít štátnych orgánov);
- B. právna zodpovednosť sprostredkovateľov z hľadiska transparentnosti a prístupu k údajom zvyšujúcim transparentnosť výdavkov, najmä na politickú reklamu. Internetový sprostredkovateľ by mali poskytnúť prístup k údajom o platenej politickej reklame, aby sa predišlo nezákonnému (cudziemu) zásahu do volieb a aby sa dali identifikovať kategórie cieľových skupín.
- C. kvalitná žurnalistika: posilnenie presnosti a spoľahlivosti spravodajstva, lepšie zapojenie publika, posilnenie verejnoprávných a lokálnych médií a posilnenie samoregulácie s dodatočným zameraním sa na transparentnosť online správ a ich šírenie;
- D. posilnenie postavenia voličov ku kritickému zhodnoteniu volebnej komunikácie zamerané na opatrenia na predchádzanie vystaveniu falošným, zavádzajúcim a škodlivým informáciám (s náležitým ohľadom na obmedzenia, ktoré majú iniciatívy na kontrolu faktov), úsilie o mediálnu gramotnosť (vrátane sociálnych médií) prostredníctvom vzdelávania a presadzovania;
- E. otvorený internet: zaistenie neutrality siete, zváženie zákonného posilnenia práv používateľov na otvorený internet a zaistenie, aby každé obmedzenie prístupu k internetovému obsahu bolo založené na presnej a predvídateľnej právnej úprave upravujúcej rozsah každého obmedzenia, a garancia súdneho dohľadu na prevenciu pred zneužitím;
- F. ochrana osobných údajov: potvrdenie a ochrana práva na anonymitu na internete, regulácia a prísne obmedzenie vytvárania a používania profilov vo všetkých druhoch rôznych kontextov. Okrem toho by Rada Európy mohla zvážiť prijatie usmernení o obmedzeniach, ktoré sa majú uplatňovať na technológie sledovania vrátane medzinárodného obchodu s takýmito technológiami; presadzovanie dohovoru 108 ako „zlatého globálneho štandardu“; a prípadne vypracovanie osobitného právneho

nástroja na riešenie vysokého rizika, ktoré pre ochranu osobných údajov predstavuje používanie digitálnych technológií v politických kampaniach a reklame.

153. Ako už bolo zdôraznené, bezhraničný charakter internetu a súkromné vlastníctvo informačných tokov spôsobuje, že súčasné výzvy pre demokraciu a volebné procesy sú mimoriadne zložité. Medzinárodná spolupráca a zapojenie príslušných súkromných subjektov sú preto nevyhnutné na to, aby bolo možné čeliť týmto výzvam a zabezpečiť právo na slobodné voľby a fungovanie demokracie v budúcnosti.

Z originálu:

Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), on Digital Technologies and Elections, adopted by the Council of Democratic Elections at its 65th meeting (Venice, 20 June 2019) and by the Venice Commission at its 119th Plenary Session (Venice, 21-22 June 2019)

Preložil:

Mgr. Andrea Nagyová, odbor zahraničných vzťahov a protokolu, Kancelária Ústavného súdu Slovenskej republiky