

Мср Лука Петровић, асистент
Правног факултета Универзитета у Крагујевцу
ORCID: 0000-0003-1045-9555

Прегледни научни рад
УДК: 342.843:004
DOI: 10.46793/XXIMajsko.203P

ИЗБОРНИ ПРОЦЕСИ У ДИГИТАЛНОМ ДОБУ*

Резиме

Наредни корак у модернизацији традиционалне изборне процедуре разматра се у контексту употребе технолошко-информационих уређаја, интернета и дигиталних технологија као средстава којима би се обезбедила ефикасност и економичност процеса. Избори представљају врло осетљиво подручје с обзиром на то да је њихова основна сврха успостављање и легитимизација државне власти. До сада су се реализовали ослањајући се искључиво на активности људи као носилаца изборне администрације, али се у ери технолошког развоја појавила потреба да се одређени изборни кораци повере паметним уређајима како би се процедура поједноставила. Ипак, централна изборна фаза – фаза гласања – изазива највише неслагања по овом питању, те се с разлогом у многим стручним круговима води расправа о томе да ли електронско гласање може заменити традиционални начин изјашњавања бирача.

Аутор у раду анализира проблематику употребе интернета и технолошко-информационих уређаја у изборном поступку, уз осврт на предности и недостатке које ови модели доносе. Истраживање, поред тога, обухвата и друге фазе избора у којима се савремене технологије примењују. У разматрање се узимају и претходна, односно припремна фаза избора, која обухвата политичке кампање изборних такмаца, све више присутне на друштвеним мрежама, као и завршна фаза избора. Неизоставни део јесте питање заштите изборних права у дигиталном добу, односно анализа опасности које могу настати употребом савремених технологија.

Кључне речи: избори, електронско гласање, дигиталне технологије, изборна права, сајбер безбедност.

* Рад је резултат научноистраживачког рада аутора у оквиру Програма истраживања Правног факултета Универзитета у Крагујевцу за 2025. годину, који се финансира из средстава Министарства науке, технолошког развоја и иновација Републике Србије.

1. Уводна разматрања

Према дефиницији аутора Стивена Клифта, оснивача *E-Democracy* платформе која промовише дигиталну демократију и учешће грађана у политичким процесима, електронска, односно дигитална демократија подразумева употребу информационо-комуникационих технологија и стратегија од стране демократских актера друштва у политичким и управљачким процесима у локалним заједницама, затим држави и на међународној сцени. Под демократским актерима подразумевају се владе, изабрани званичници, медији, политичке организације и грађани (бирачи). Такође, електронска демократија подразумева веће и активније учешће грађана које омогућавају Интернет, мобилне комуникације и друге технологије у данашњој представничкој демократији.¹

Појам електронска демократија често се доводи у везу са појмом електронско управљање (*e-government, e-governance*), с обзиром на то да суштински оба концепта подразумевају коришћење информационо-комуникационе технологије. Ипак, велики број аутора који су се бавили датим питањем инсистира или на блажој, или на строжијој дистинкцији ових појмова. Тако се према једном становишту истиче да електронску демократију треба разликовати од електронског управљања, које се може сматрати само једним њеним сегментом, јер подразумева пребацивање активности владе на онлајн ниво са циљем повећања ефикасности њеног рада.² Са друге стране, постоје и схватања да се електронско управљање оријентише на што ефикасније пружање услуга грађанима, и да стога нема нужно везе са оним што се подразумева под елементима демократског процеса, осим у свом крајњем облику.³ Међутим, разлике у истакнутим становиштима губе на значају у практичном домену, јер механизми електронског управљања могу имати значајну улогу у имплементацији система електронског гласања, чиме би се заиста приближили ставу по коме је електронско управљање само један од сегмената електронске демократије.

Ипак, најважнију улогу у објашњавању појма електронске демократије свакако има концепт електронских избора (*e-elections, e-voting*). Избори представљају поступак путем кога грађани, односно бирачи, у модерним демократијама, бирају политичке субјекте којима ће поверити обављање политичке власти, док би модел електронских избора подразумевао укључивање информационо-комуникационих технологија у тај процес.

¹ Steven Clift's - Brief E-Democracy Definition, Publicus.net: <https://www.publicus.net/articles/edemresources.html> 01.04.2024.

² Вучковић, Ј., *Електронска демократија и електронско гласање*, Зборник радова: Усклађивање правног система Србије са стандардима ЕУ, књ. 9, Крагујевац, 2021 стр. 139.

³ Дамњановић, И., *Електронска демократија (E-democracy) као могућност демократизације*, Српска политичка мисао, год. 16. вол. 23, бр. 1/2009, стр. 87-88.

Успостављање таквог изборног модела представља врло сложено питање око кога ни у теорији, ни у пракси не постоји сагласност, као што је то, примера ради, случај са електронским управљањем.

Испитивање демократског потенцијала електронских избора представља веома комплексан истраживачки задатак који мора обухватити анализу могућности употребе информационо-комуникационих технологија кроз све изборне фазе. Изборни процес је, дакле, сложен и он се не ограничава само на радњу гласања, односно непосредног изјашњавања бирача. Појам избора у ширем смислу обухвата и претходну (припремну) фазу избора, као и тзв. завршну фазу, која према неким становиштима може трајати од објављивања резултата гласања па све до расподеле и потврђивања мандата изабраних представника.

2. Модел електронског гласања

О употреби технологије у изборном поступку почело се дискутовати још у XIX веку. Први случај употребе машина са полугом забележен је у Њујорку 1892. године. Иако су САД за проналазаче биле веома стимулативна средина, увођење машина у изборни поступак није било без правних контроверзи, те је њихова употреба у држави Масачусетс брзо означена као неуставна. Двадесети век, међутим, доноси драстичне промене у ширењу употребе машина за гласање. Пролиферација и даље усавшавање ових уређаја посебно се интензивирају након што су се седамдесетих година прошлог века у САД појавили *DRE* уређаји (*Direct Recording Electric*).⁴

Коришћење *DRE* уређаја значило је да се у процес укључују машине које мењају папирне гласачке листиће, па бирачи гласају притиском на дугме, посебну ручицу или додиром на екран *DRE* уређаја. Процес гласања се, међутим, одвија у контролисаном окружењу, односно не искључује се учешће изборне администрације на бирачком месту. Овај систем веома је скуп, рањив је на вирусе и могућности кварења и не оставља папирни траг, те због тога настаје простор за сумњу када је у питању фалсификовање резултата. Постоји теоретска могућност да би непоштен програмер могао да лажира (*DRE*) гласачки уређај тако да бирач верује да гласа за кандидата X, док компјутер региструје заправо глас за "кандидата Y". Бројање гласова такође може подлећи потенцијалном "заобилажењу".⁵

Гласање помоћу *DRE* уређаја изгледа тако што се бирач најпре идентификује на бирачком месту помоћу личног документа, након чега приступа машини за гласање. Машина мора бити постављена на таквом месту

⁴ Марковић, В., *Електронско гласање – тројански коњ или деус ех машина у савременим демократијама?*, Страни правни живот, вол. 67, бр. 3/2023, стр. 432. према: Stewart, C., *Voting Technologies*. Annual Review of Political Science, vol. 14, 2011, p. 357.

⁵ Димитријевић, П., *Право информационе технологије*, Ниш, 2014, стр. 201-215.

и на такав начин којим се обезбеђује тајност гласања. Приступом уређају отвара се интерфејс за гласање, односно бирачу се на екрану уређаја приказује гласачки листић са именима изборних кандидата или странака. Након што бирач донесе одлуку и направи избор, има прилику да на екрану уређаја изврши финалну проверу и евентуално коригује свој избор пре него што гласа. Након потврде гласања, глас бирача се бележи у електронску меморију уређаја и тиме се поступак гласања окончава. У неким системима као што је, примера ради: (*Voter Verified Paper Audit Trail – VVPAT*) систем, уређај истовремено штампа и папирну потврду гласања, коју бирач може видети кроз посебни стаклени део, али је не може и узети за себе јер иста служи за накнадну проверу резултата гласања.

Наредни корак у развоју концепта електронског гласања представља интернет гласање. Разлика између система интернет гласања и система директне електронске регистрације гласања огледа се у томе што се интернет гласање реализује углавном у неконтролисаном окружењу. У оквиру интернет (*online*) гласања, као гласања ван бирачког места, постоје извесне разлике у модалитетима. Тако, са једне стране, имамо такозвана *poll site* и *kiosk voting*, као облике интернет гласања код којих се гласање одвија на неком од бројних јавних места широм земље (нпр. тржни центри), а са друге стране постоји и тзв. *remote i-voting*, као најдоследнији модалитет интернет гласања, код којег бирач гласа преко било ког паметног уређаја и са било ког места на ком постоји интернет мрежа.⁶

Систем интернет гласања оправдава се аргументима да исто може утицати на већу излазност бирача, као и да омогућава гласање и оним бирачима који због велике удаљености од бирачког места не могу приступити гласању. Ипак, критике на рачун интернет гласања указују да овај систем може имати озбиљне недостатке. Тако се у расправи о овом моделу гласања најчешће укључује домен сајбер безбедности, односно оних опасности које су повезане са интернет (дигиталним) простором. Интернет као модел за спровођење избора има значајне инхерентне мане које се могу кретати од питања: како систем заштитити од потенцијалних напада хакера, затим како избећи породично гласање, па све до питања о тзв. приватизацији изборног процеса, с обзиром да програме и софтвере који се користе за реализацију електронских система гласања дизајнирају, производе и сервисирају углавном приватне компаније.

Примена електронских модалитета гласања није општеприхваћена. Ретки су примери оних држава које су се одлучиле да испробају електронске системе гласања, мада треба истаћи да се ради о „експерименталним” видовима електронског гласања. Конкретније речено, успостављање могућности електронског гласања у тим државама није искључило традиционални систем гласања, већ је електронски концепт уведен само као допунска могућност уз традиционални систем. Неке од држава које су испробале електронске системе

⁶ Марковић, В., *нав. чланак*, стр. 433.

брзо су од њих одустале, неке су их омогућиле само на локалном нивоу, а као пример државе у којој је такав систем доживео успех наводи се Естонија.

Естонија је прва и једина земља на свету у којој комплетно бирачко тело има могућност да гласа преко Интернета на свим изборима, укључујући и изборе за Европски парламент. Е-гласање је у овој земљи уведено 2005. године на локалним изборима, да би 2007. године Естонија била и прва земља у свету у којој се преко интернета гласало и на парламентарним изборима. Проценат бирача који користе интернет да гласају расте са сваким изборима. У марту 2020. године на општим изборима преко интернета је гласало 44 процената бирача. Систем гласања се одвија преко апликације на којој је потребно извршити идентификацију коришћењем одговарајућег пин-кода и личне карте, након чега се приступа „виртуалној гласачкој кабини“ у којој се могу видети изборне листе и изабрати жељени кандидати.⁷

Приликом осврта на изборну праксу Естоније треба нагласити да је ова држава имала веома повољне друштвене услове који су погодовали успостављању интернет система гласања. Бројни статистички подаци говоре о томе да је Естонија држава у којој је неписменост становништва потпуно искорењена, а број грађана који су високо образовани креће се и до 50 процената.⁸ Наведени подаци указују нам на то да питање „дигиталне писмености“ у Естонији не представља проблем који би могао спутавати функционисање интернет модела гласања, односно грађани имају једнаке могућности да гласају путем интернета, чиме се обезбеђује поштовање принципа једнакости, као једног од најважнијих принципа изборног права.

Нешто другачију изборну праксу затичемо на примеру СР Немачке. Упркос интересовању за успостављање електронског концепта гласања, Савезни уставни суд 2009. године донео је одлуку према којој коришћење електронских машина за гласање, без могућности ручног пребројавања гласа, није у складу са уставним принципима. Савезни Уставни суд СР Немачке је нагласио да принцип транспарентности и право на проверу резултата гласања морају бити доследно осигурани. Тиме је ова пресуда утицала на одустанак од употребе електронских машина за гласање на савезним изборима у Немачкој, јер се није могло гарантовати да ће изборни процес бити потпуно транспарентан и проверљив.⁹

Поред *DRE* уређаја и интернет модела гласања важно је поменути да постоји и трећи модел електронског гласања. Он се назива и „полueleктронски“ систем гласања и подразумева оптичко скенирање гласачких листића. Гласање се обавља употребом папирних гласачких листића

⁷ Вучковић, Ј., *нав. чланак*, стр.146.

⁸ OECD Index: <https://www.oecdbetterlifeindex.org/countries/estonia/>

⁹ Headnotes to the Judgment of the Second Senate of 30 June 2009, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/06/es20090630_2bve000208en.html

који се аутоматски скенирају и броје помоћу оптичког скенера. На овај начин обезбеђује се ефикасно и брзо бројање гласова и утврђивање резултата, али је и овај систем подложен техничким кваровима и манипулацијама.

Бројни недостаци који се као критика упућују електронским моделима гласања утицали су на то да се овај концепт посматра са великим подозрењем. Ипак, треба рећи да постоје и аргументи којима се он може оправдавати. Неминовно је да би употреба савремених дигиталних технологија у знатној мери могла олакшати изборни поступак. Овде се посебно има у виду радња пребројавања гласова која може бити врло сложена када су у питању бирачка места са великим бројем бирача. Такође, једна од предности електронског модела је економичност. Ангажовање људских ресурса који чине изборну администрацију изискује велике издатке из буџета. Употреба савремених технологија би на дугорочном плану резултирала смањењем трошкова за ангажовање лица у органима за спровођење избора. Одређени модели електронског гласања, као што је интернет гласање, поседују потенцијал да повољно утичу на излазност бирача јер је овај модел погодан за оне бираче који се због удаљености од бирачког места одлучују за изборну апстиненцију. Електронско гласање заиста би могло представљати будући корак модернизације изборних система, који ће нажалост морати да сачека изнајлажење ваљаних технолошких решења којима би се недостаци који се за њега везују могли адекватно предупредити.

3. Политичка кампања у дигиталном окружењу

Претходна односно припремна фаза избора подразумева изборне радње које се предузимају почев од момента расписивања избора, па све до отварања бирачких места. Поред формалних изборних радњи које предузимају органи изборне администрације, припремна фаза обухвата и кампању изборних такмаца. О значају припремне изборне фазе говори и чињеница да је она често предмет интересовања посматрачких мисија, с обзиром да се закључци о транспарентности и регуларности избора не могу извести уколико би иста била занемарена. Предмет посматрања у овом ступњу је сам поступак кандидовања, али и целокупан ток политичке кампање учесника избора. За одржавање демократске атмосфере и поштених избора значајно је да сви изборни такмаци имају једнаке могућности за вођење кампање, једнак приступ медијима и такву почетну позицију која гарантује једнаке шансе за успех у изборној трци.¹⁰

Медији су у свим политичким кампањама најважнији канал за комуникацију са бирачима. Њихов утицај на формирање ставова јавног мњења је готово незаменљив, па је стога од суштинске важности да медији пласирају

¹⁰ Петровић, Л., *Грађанска контрола избора и заштита изборних права* УЗборник радова: Усклађивање правног система Србије са стандардима ЕУ, књ. 12, Крагујевац, 2024, стр. 325.

објективне, правовремене и истините информације. Ипак, поље политичког деловања обилује бројним примерима необјективног и политички пристрасног извештавања, чиме се угрожава право бирача на информисаност, без чега нема ни ваљаног остваривања изборног права.

Питање информисања бирачког тела постаје сложенија проблематика развојем интернета и друштвених мрежа који у последњој деценији представљају главни, а не алтернативни извор информисања. Интернет и друштвене мреже данас су неизоставни сегмент изборних процеса, јер су се показале као најдоминантније поље комуникације политичких субјеката и грађана (бирача). Коришћење друштвених мрежа омогућава политичким актерима да досегну до знатно већег броја бирача, да прилагоде поруке циљним групама и анимирају их на начине који раније нису били могући.

Основне предности интернет кампање су ефикасност у приступању бирачима, затим брзо ширење информација и политичких порука, уз минималне трошкове, као и усмерено односно таргетирано оглашавање. Таргетирано оглашавање нуди могућност политичким субјектима да, користећи се поставкама и алатима друштвених мрежа, усмере политичке поруке према одређеној категорији корисника, а сходно њиховим интересовањима, политичким ставовима, узрасту и сл. Са друге стране, најзначајније опасности интернет кампање представља могућност готово неконтролисаног ширења лажних вести, употребе *deepfake садржаја*, деловања лажних (тзв. бот) налога.

3.1. Утицај дезинформација на формирање изборне воље

Пропаганда и манипулација информацијама су пратили политику од најранијих времена. Током историје никада није постојало златно доба транспарентности. Неки рани записи, који датирају још из времена старог Рима, указују да у периоду када је Марко Антоније упознао и заволео Клеопатру, његов тадашњи политички непријатељ Октавијан је то искористио да покрене клеветничку кампању против њега, исписујући кратке и оштре паролe на новчићима, у стилу неких архаичних „твитова”.¹¹ У старом Риму натписи на новчићима служили су да се пренесе политичка порука, а Октавијан је грађанима Рима желео да поручи да је Марко Антоније својом везом са Клеопатром постао издајник римских вредности. Нимало другачији контекст немају ни савремене методе политичког деловања. Убрзан развој друштвених мрежа пружио је могућности политичким субјектима али и њиховим присталицама, да у „дигиталном простору” отпочну прави

¹¹ Груловић, Б., *Лажне вести и стварање панике у јавности*, Актуелности, Тематски број часописа са радовима презентованим на научно-стручном скупу: Медији, образовање и култура у пандемији, бр 39/2021, стр. 62.

политички али и психолошки рат, користећи се дезинформацијама и лажним вестима.

Један такав случај десио се током председничких избора у САД 2016. године. Као председнички кандидати истакли су се актуелни амерички председник Доналд Трамп и кандидаткиња Демократске странке Хилари Клинтон. Избори су протекли у светлу опште поларизације друштва, а пресудни утицај на формирање ставова јавног мњења имале су друштвене мреже. Међутим, током председничке кампање, на готово свим друштвеним мрежама, деловао је огроман број лажних (бот) налога, као и лажних страница које су свакодневно шириле низ дезинформација и лажних вести. Ове вести углавном су биле усмерене на дискредитацију кандидаткиње Хилари Клинтон, па је тако америчка јавност имала прилике да чује да је Клинтонова умешана у педофилску мрежу чије је седиште у подруму пицерије у Вашингтону (тзв. афера „*Pizzagate*“) ¹², да снабдева наоружањем терористичке организације, као и да је изјавила да ће укинути Други амандман ¹³ на амерички Устав, који обезбеђује право на ношење оружја. Са друге стране, кандидат Републиканаца, према тврдњама корисника друштвених мрежа, уживао је чак званичну подршку поглавара Римокатоличке цркве, Папе Фрање ¹⁴. Све ове вести касније су се испоставиле као лажне, али се процењује да су исте имале утицаја на ставове бирача током председничке кампање.

Ипак, по окончању председничких избора, питање одговорности због ширења дезинформација готово да није ни постављано. Први разлог томе је чињеница да је Првим амандманом на Устав САД-а из 1791. године, слобода говора заштићена као апсолутно људско право. Амерички Конгрес, сходно томе, не може доносити никакав закон којим се ограничава слобода говора или штампе или право народа на мирне зборове и на упућивање петиције влади за исправљање неправди. ¹⁵ На савезном нивоу такође не постоји закон којим се прописују санкције за креирање и ширење лажних вести, а питање одговорности за ширење неистинитог садржаја могло би се једино поставити ако би се тиме позивало на насиље и намерно наносила штета другоме.

Други проблем је био идентификовање корисника друштвених мрежа који су спорне лажне садржаје пласирали или делили. Многи корисници су то чинили без намере да нанесу штету, верујући у истинитост лажних вести, те се зато ни не може поставити питање њихове одговорности. О одговорности би се могло говорити само ако би се открили аутори лажних садржаја, које је

¹² BBC News: <https://www.bbc.com/news/blogs-trending-38156985> (05.04.2025).

¹³ Портал Глас Америке: <https://www.glasamerike.net/a/tramp-klinton-drugi-amandman/3458585.html> (05.04.2025).

¹⁴ Портал Б92: https://www.b92.net/o/info/vas_komentar?nav_id=1207808 (05.04.2025).

¹⁵ Constitution of the United States, First Amendment: <https://constitution.congress.gov/constitution/amendment-1/>

било немогуће идентификовати. Овде посебно треба имати у виду и неке касније тврдње америчких безбедносних агенција да је у том периоду на друштвеним мрежама деловао велики број лажних, бот налога, који су се, између осталог, доводили у везу и са руским тајним службама.

Такође, важно је истаћи и суштинску разлику између две врсте лажних вести на основу степена обмане. У том смислу, можемо разликовати лажне вести у тзв. ужем смислу, које представљају све оне вести које су намерно као такве фабриковане, односно које су измишљене и немају потпору у реалности. Насупрот њима налазе се тзв. искривљене вести (*disorted news*), у којима су садржане информације које нису нужно нетачне, али које су презентоване и уоквирене на такав начин да може изгледати као да из њих произлазе неистинити закључци. И док су лажне вести у ужем смислу једноставније за детектовање, искривљене вести (*disorted news*) представљају софистициранију методу пропаганде за чије је разобличавање потребно уложити много више времена и истраживачког напора.¹⁶ Јасно је да утврђивање одговорности за објављивање искривљених вести може бити комплексно. Код искривљених вести је тешко утврдити намеру њиховог аутора, а понекад је готово немогуће са сигурношћу утврдити да ли се ради о искривљеним вестима или новинарској (ауторској) грешци.

Као одговор на проблем ширења лажних вести, поједине друштвене мреже су увеле мере попут обележавања садржаја, проверу чињеница, уклањање лажних налога. Иако се ради о мерама које су показале резултате у спречавању ширења неистинитих садржаја, чини се да оне саме по себи нису довољне, јер је проблем лажних вести структуралан и друштвени, а не само технолошки проблем. Почетком априла 2020. године, Твитер је саопштио да је уклонио 8.558 налога из Србије који су учествовали у координисаном промовисању једне политичке партије. Налози су према тврдњама ове платформе уклоњени јер су кршили политику друштвене мреже и подривали јавну расправу. У истој акцији брисања налога избрисани су и налози из Египта, Хондураса, Индонезије и Саудијске Арабије.¹⁷ Брисање налога, међутим, не представља дугорочно решење проблема. Суспензија налога на друштвеним мрежама не спречава трајно могућност отварања нових лажних налога. Проблем се може ублажити сарадњом и координисаном акцијом државе и субјеката који управљају друштвеним мрежама. Без поменуте сарадње, свако ангажовање државних органа, усмерено на откривање и санкционисање лица која су пласирала лажну вест, неће дати ваљане резултате.

¹⁶ Тодоровић, М., *Међународно право у сузбијању лажних вести: домети и алтернативе*, Савремене студије безбедности, бр, 1/2024, стр. 110.

¹⁷ BBC NEWS: <https://www.bbc.com/serbian/lat/srbija-52235903> (05.04.2025).

3.2. Манипулација стварношћу – утицај *deepfake* технологије на изборни процес

Нешто комплекснију форму лажних вести представљају дипфејкови (*deepfake*). Термин (*deepfake*) настаје комбинацијом термина „дубоко учење“ (*deep learning*) и „лажно“ (*fake*). Дипфејкови су хиперреалистични видео снимци који су дигитално измењени тако да приказују људе како говоре и раде ствари које се у стварности никада нису догодиле. Дипфејкови се ослањају на неуронске мреже које анализирају велике скупове података како би научиле да имитирају нечије фацијалне изразе, маниризме, глас и интонацију... Дипфејкови су постали јавни феномен 2017. године, када је један од корисника платформе *Reddit*¹⁸ објавио снимке познатих личности у компромитијућим сексуалним ситуацијама. Они су тешки за детекцију, јер користе стварне снимке, могу изгледати готово аутентично и оптимизовани су да се брзо шире на свим друштвеним мрежама. Због тога, многи гледаоци дипфејкова аутоматски претпостављају да је видео који гледају аутентичан.¹⁹ Постоји и могућност да се ови садржаји приказују у реалном времену, тако да могу изгледати као неупитно истинити.

Колико ова технологија може бити опасна, не само у сфери политичког већ и шире, говори нам пример из 2022. године, када се у раној фази руске инвазије на Украјину, појавио *deepfake* видео у коме украјински председник Володимир Зеленски наводно позива украјинску војску да положи оружје и капитулира пред Русијом. Овај снимак емитован је истог дана и на телевизији „Украина 24“, након хакерског упада у сигнал те телевизијске станице. Узевши у обзир наведени пример, сматрамо да није немогућа ситуација у којој би, рецимо, садржај који дискредитује председничког или другог изборног кандидата био пласиран у току самог изборног дана.

Deepfake технологија све чешће проналази своју употребу у домену политике, а посебно у сврху вођења политичких кампања. Коришћење *deepfake*-а није забрањено само по себи, али уколико је циљ садржаја ширење лажних вести, дезинформација и дискредитација других политичких субјеката, употреба ове технологије доводи нас на терен озбиљних опасности. Свесне последица које ова технологија може изазвати, многе државе света донеле су прописе којима уређују или ограничавају њену употребу.

Америчка савезна држава Калифорнија донела је неколико прописа којима се ограничава употреба *deepfake* садржаја у току избора. Законима се обавезују велике онлајн платформе да уклоне или означе обмањујуће и дигитално

¹⁸ Reddit је онлајн платформа и заједница која функционише као комбинација форума и друштвене мреже. Основан је 2005. године, а корисници (тзв. *Redditors*) на њему могу објављивати разне садржаје.

¹⁹ Westerlund, M., *The Emergence of Deepfake Technology: A Review*, Technology Innovation Management Review, Vol. 9, Issue 11, November 2019, p. 40.

измењене садржаје повезане са изборима. Постојећи закон, до 1. јануара 2027, забрањује било ком лицу да дистрибуира материјално обмањујући аудио или визуелни материјал кандидата за изборну функцију са намером да се повреди углед кандидата или да се обмане гласач да гласа за или против тог кандидата, у року од 60 дана од избора. Један од закона је добио и врло симболичан назив: „Закон о одбрани демократије од дубоких лажних обмана”.²⁰ Сличну законодавну праксу затичемо и у савезној држави Тексас.

Међу првим државама које су уредиле ово питање налази се Кина. 2022. године, Кинеска администрација за сајбер простор издала је посебан акт познат као: „Одредбе о администрацији дубоке синтезе информационих услуга заснованих на Интернету“. Одредбама је прописано да ниједна организација или појединац не сме да користи услуге дубоке синтезе (*deepfake*) за ангажовање у активностима забрањеним законима и административним прописима, као што су оне које угрожавају националну безбедност и интересе, нарушавају национални имиџ, нарушавају јавне интересе, нарушавају економски и друштвени поредак и нарушавају легитимна права и интересе других.²¹ Европска унија такође је уредила ово питање 2024. године, и то Уредбом о утврђивању усаглашених правила о вештачкој интелигенцији (*Artificial Intelligence Act*).²² Уредбом је прописана обавеза свих субјеката који користе системе вештачке интелигенције (AI), за генерисање или манипулисање сликовним, аудио или видео садржајем (*deepfake*), да открију, односно јасно етикетирају, да је садржај вештачки генерисан или изманипулисан. Изузетак од утврђеног правила су садржаји који се користе у уметничке или забавне сврхе, али само ако не представљају ризик да ће деловати манипулативно.

Употреба савремених технологија у предизборним кампањама омогућила је ефикаснију комуникацију између политичких субјеката и бирача, посебно младих који су често склонији бирачкој апстиненцији. Међутим, поред ових предности, употреба технологија доноси и значајне ризике, као што су лажне вести, *deepfake* садржаји и манипулације путем бот налога. Ови методи могу утицати на изборну одлуку бирача и угрожавају основна људска права, нарочито изборно право. Како се ради о проблему глобалног карактера, решавање ових питања захтева усмерење на глобалном нивоу. Правовремено увођење адекватних регулаторних механизма и међународна сарадња имаће

²⁰ AB-2655 Defending Democracy from Deepfake Deception Act of 2024, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2655

²¹ China Justice Observer, https://www.chinajusticeobserver.com/a/chinese-government-to-regulate-deepfake-technology?utm_source=chatgpt.com

²² Regulation (EU) 2024/1689 of the European parliament and of the council of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

кључну улогу у спречавању злоупотреба посредством дигиталних технологија и очувању демократских вредности. Уважавајући изазове дигиталног доба, ОЕБС је већ издао бројне документе и препоруке о употреби савремених технологија. ОЕБС игра значајну улогу у развоју стандарда и препорука које доприносе безбедности, транспарентности и правичности изборних поступака. У будућности, јачање сарадње између држава, организација и стручњака из различитих области попут технологије, права и политикологије, биће од суштинског значаја за очување интегритета изборних процеса и заштиту људских права у дигиталном добу.

4. Заштита изборних права у дигиталном добу

Разматрање о предностима и недостацима електронске демократије немогуће је заокружити без анализе изазова који се намећу као препрека у остваривању и заштити изборног права грађана. Употреба информационо-комуникационих технологија се на први поглед чини веома практичним решењем на путу модернизације традиционалног изборног поступка, али она подразумева и значајне ризике који су се за сада показали као тешко отклоњиви. Електронске моделе избора карактеришу мане које могу угрозити, не само регуларност процедуре и тајност гласања, већ и принципе општег и једнаког изборног права и слободних (фер) избора.

Први велики проблем са којим се у том домену суочавамо односи се на питање дигиталне писмености. Дигитална писменост подразумева поседовање способности, могућности, знања и вештина за коришћење дигиталних алата и технологија. Прелазак на електронске моделе гласања дакле не би био могућ уколико сви бирачи не би били кадри и способни да гласају употребом машина или путем интернета. Бирачи који не поседују таква знања и вештине би могли бити искључени из изборног поступка, што је супротно принципима општости и једнакости бирачког права. Такође, у систему електронског гласања отвара се могућност да бирачи који се не разумеју у дигиталне технологије направе грешке приликом одабира кандидата или да одустану од гласања. Дигитална писменост представља врло важан друштвени предуслов за реализацију електронских система гласања, те зато државе које се суочавају са овим проблемом би е-гласање могле остварити једино у комбинацији са традиционалним моделом гласања, тј. као допунску могућност.

Као опција за превазилажење проблема дигиталне писмености, наметнуло се и питање учешћа помагача за оне бираче који не поседују адекватне вештине и знања за руковање дигиталним технологијама. Ипак, учешће посматрача представља изузетак којим се нарушава принцип тајности гласања, али само у ситуацији када бирач због одређеног хендикепа није у могућности да самостално гласа без помоћи другог лица. Учешће помагача као одговор на проблем дигиталне писмености значио би учесталу примену изузетка од правила, чиме би и принцип тајности био озбиљно угрожен, а појавио би се

простор за злоупотребе. Намеће се такође могућност тзв. породичног гласања, јер када дигитално вешт члан једне породице гласа уместо оних који то нису, оправдано се можемо запитати: да ли ће заиста приликом гласања помагач одабрати ону опцију за коју бирач жели да гласа?

Други проблем у вези са електронским моделима гласања односи се на оне инхерентне недостатке који прате дигиталне системе. Уређаји за гласање и интернет платформе не остављају папирни траг, што аутоматски спречава могућност ручне провере резултата. Ипак, треба истаћи да неки системи, попут *VVPAT-a (Verification Voter Paper Audit Trail)*, поседују могућност штампања папирне потврде, која може бити важан корак у осигуравању транспарентности. Међутим, гласови се чувају и бележе у посебним меморијама уређаја или софтверима који су подложни не само техничким недостацима и кварењу, већ и нападу хакера. Ова опасност је посебно изражена код модела интернет гласања, а пример великог хакерског (*cyber*) напада догодио се 2007. године након сукоба између Русије и Естоније, што је владе широм света натерало да преиспитају сигурност својих интернет мрежа.²³

Још један велики изазов представља искључивање могућности посматрања изборног процеса при интернет гласању, што значи да је грађанско посматрање избора могуће само ако се користе уређаји за гласање на физичким бирачким местима. На овај начин, избори не могу бити потпуно транспарентни ако нису под непосредним надзором независних посматрача. Електронско гласање такође поставља велики изазов за судове и друге државне органе који су надлежни за заштиту изборних права и решавање изборних спорова. Пошто судије често немају адекватна техничка или информатичка знања, у случају спора због повреде изборног права било би неопходно ангажовање стручњака из области информационих технологија, као и из области сајбер безбедности, како би се на прави начин разматрали овакви спорни случајеви.

Трећи проблем у домену савремених избора односи се на утицај друштвених мрежа на формирање изборне воље грађана. Појаве попут лажних и искривљених вести, лажних налога и *deepfake* садржаја поседују потенцијал да манипулативно утичу на бираче који своје политичке ставове граде верујући да су поруке које су им пласиране истините. Једина правична могућност за кориговање последица избора одржаних у „неслободној атмосфери” огледала би се у понављању изборног процеса, ипак у пракси не постоји пример у коме је изборни поступак поништен и поновљен искључиво због медијско-пропагандних утицаја. Неспорна је чињеница да је њихов домет тешко измерити, као и да је још теже утврдити да ли би исход избора био другачији уколико би такво деловање било искључено.

Савремени изборни процес не може се вредновати само кроз правну призму, односно формално-процедурално слеђење закона. Демократски капацитет избора мора се мерити и кроз друштвене услове који омогућавају да

²³ Вучковић, Ј., *нав. чланак*, стр.147.

бирачи слободно формирају и изразе своју изборну вољу. Слободни избори представљају темељ демократског поретка и претпоставку ваљаног остваривања изборног права. Они подразумевају, између осталог, равноправан приступ информацијама, објективно информисање, транспарентност поступка и слободу медија. Како на то указују и сви релевантни међународни документи попут Универзалне декларације о људским правима²⁴, затим Међународног пакта о грађанским и политичким правима²⁵, Европске конвенције о људским правима²⁶ и Кодекса добре праксе у изборним питањима Венецијанске комисије²⁷, слободни избори могу постојати само ако се изборна воља бирача гради без спољних притисака и системских и пропагандних манипулација. У том контексту, озбиљно и стратешко деловање у дигиталном окружењу, које укључује превенцију злоупотреба технологије, од пресудне је важности за очување стварног демократског легитимитета изборног процеса. Уколико се злоупотребе не предупредe, дигитална демократија може се свести на пуко „срицање” демократије – испразну изборну форму без стварне демократске суштине.

5. Закључак

Иако употреба информационо-комуникационих технологија омогућава брже и ефикасније спровођење изборних процедура, она такође доноси ризике који могу угрозити регуларност избора и остваривање изборног права, посебно када су у питању инклузивност и сигурност гласачких система. Проблеми као што су недостатак дигиталне писмености код знатног дела бирачке популације и ризик од злоупотреба у сајбер простору, захтевају пажљиво и системско решавање. Да би се у будућности осигурао прави дигитални демократски процес, неопходно је применити мултидисциплинарни приступ у развоју, али и имплементацији електронских избора. Поред тога, политичке кампање у дигиталном добу које све више зависе од друштвених мрежа и интернета омогућиле су брзу, лаку и масовну дистрибуцију информација, али истовремено отвориле простор за манипулацију путем лажних вести и дезинформација. Ово може угрозити транспарентност избора и слободу бирача да формирају своју изборну вољу без непримерених медијско-пропагандних

²⁴ Универзална декларација о правима човека је декларација усвојена од стране Генералне скупштине Уједињених нација (A/RES/217, 10. децембра 1948. године, у Паризу) чл. 21.

²⁵ Међународни пакт о грађанским и политичким правима, <https://minljmpdd.gov.rs/sektori/ljudska-prava/medjunarodni-ugovori/medjunarodni-pakt-o-gradjanskim-i-politickim-pravima-iccp/>

²⁶ Конвенција за заштиту људских права и основних слобода (Рим, 1950), Протокол 1, чл. 3.

²⁷ Видети: Venice Commission., Interpretative declaration of the code of good practice in electoral matters as concerns digital technologies and artificial intelligence. (Venice, 6-7 December 2024).

утицаја. Стога је кључно да се *de lege ferenda* обезбеде услови који гарантују заштиту бирача од манипулативних утицаја који се све чешће као претња појављују и брзо шире у дигиталном свету. Заштита би се могла успоставити и путем увођења одговорности за ауторе лажних вести, као и за друштвене мреже које не предузимају активности да спрече и уклоне обмањујуће садржаје.

*Luka Petrović, LL.M., Assistant
Faculty of Law, University of Kragujevac*

ELECTORAL PROCESSES IN THE DIGITAL AGE

Summary

The next step in modernizing the traditional electoral procedure is being considered in the context of using technological and informational devices, the internet, and digital technologies as tools for ensuring the efficiency and cost-effectiveness of the process. Elections represent a highly sensitive area, given that their primary purpose is to establish and legitimize state authority. Until now, they have been carried out relying solely on the activities of people as the bearers of electoral administration. However, in the era of technological development, the need has emerged to entrust certain electoral steps to smart devices in order to simplify the procedure. Nevertheless, the central electoral phase – the voting phase – raises the most disagreement on this issue, and for good reason, a debate is ongoing in many expert circles about whether electronic voting can replace the traditional method of voter expression.

In this paper, the author analyzes the issue of using the internet and technological-informational devices in the electoral process, with a focus on the advantages and disadvantages these models bring. The research also includes other phases of the election in which modern technologies are applied. The analysis takes into consideration the preliminary or preparatory phase of elections, which includes political campaigns of the candidates, increasingly present on social networks, as well as the final phase of elections. An integral part of the discussion is the question of the protection of electoral rights in the digital age, including the analysis of potential risks that may arise from the use of modern technologies.

Key words: *elections, electronic voting, digital technologies, electoral rights, cybersecurity.*

Литература

- Вучковић, Ј., *Електронска демократија и електронско гласање*, Зборник радова: Усклађивање правног система Србије са стандардима ЕУ, књ. 9, Крагујевац, 2021.
- Груловић, Б., *Лажне вести и стварање панике у јавности*, Актуелности, Тематски број часописа са радовима презентованим на научно-стручном скупу: Медији, образовање и култура у пандемији, бр 39/2021.
- Дамњановић, И., *Електронска демократија (E-democracy) као могућност демократизације*, Српска политичка мисао, год. 16, вол. 23, бр. 1/2009. Димитријевић, П., *Право информационе технологије*, Ниш, 2014.
- Марковић, В., *Електронско гласање – тројански коњ или деус ех маџина у савременим демократијама?*, Страни правни живот, вол. 67, бр. 3/2023.
- Петровић, Л., *Грађанска контрола избора и заштита изборних права*, Зборник радова: Усклађивање правног система Србије са стандардима ЕУ, књ. 12, Крагујевац, 2024.
- Stewart, C., *Voting Technologies*, Annual Review of Political Science, vol. 14/2011.
- Тодоровић, М., *Међународно право у сузбијању лажних вести: донети и алтернативе*, Савремене студије безбедности, бр, 1/2024,.
- Westerlund, M., *The Emergence of Deepfake Technology: A Review*, Technology Innovation Management Review, Vol. 9, Issue 11, November 2019.
- Универзална декларација о правима човека је декларација усвојена од стране Генералне скупштине Уједињених нација (A/RES/217, 10. децембра 1948).
- Међународни пакт о грађанским и политичким правима.
- Конвенција за заштиту људских права и основних слобода (Рим, 1950.) Протокол 1.
- Venice Commission., *Interpretative declaration of the code of good practice in electoral matters as concerns digital technologies and artificial intelligence*. (Venice, 6-7 December 2024).
- Regulation (EU) 2024/1689 of the European parliament and of the council of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)
- AB-2655 Defending Democracy from Deepfake Deception Act of 2024, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2655
- Constitution of the United States, First Amendment, <https://constitution.congress.gov/constitution/amendment-1/>
- Steven Clift's - Brief E-Democracy Definition, Publicus.net
- China Justice Observer, https://www.chinajusticeobserver.com/a/chinese-government-to-regulate-deepfake-technology?utm_source=chatgpt.com
- OECD Index: <https://www.oecdbetterlifeindex.org/countries/estonia/>
- BBC News: <https://www.bbc.com/news/blogs-trending-38156985>
- Портал Глас Америке: <https://www.glasamerike.net/a/tramp-klinton-drugi-amandman/3458585.html>
- Портал Б92: https://www.b92.net/o/info/vas_komentar?nav_id=1207808
- BBC NEWS: <https://www.bbc.com/serbian/lat/srbija-52235903>